LEARN TO MASTER THE HANDS-ON LABS, ACE TECHNICAL QUESTIONS AND PASS THE CCNA

Cisco CCNA

In 60 days



PAUL BROWNING CCNP - FARAI TAFA CCIE - DANIEL GHEORGHE CCIE - DARIO BARINIC CCIE



UPDATED FOR THE BRAND NEW EXAMS:

- ✓200-120 CCNA (CCNAX)
- ✓100-101 ICND1 (CCENT)
- ✓200-101 ICND2

https://t.me/learningnets

CISCO CCNA
in 60 Days

Paul Browning (LLB Hons) CCNP, MCSE
Farai Tafa CCIE
Daniel Gheorghe CCIE
Dario Barinic CCIE

https://t.me/learningnets

This study guide and/or material is not sponsored by, endorsed by, or affiliated with Cisco Systems, Inc., Cisco®, Cisco Systems®, CCDA™, CCNA™, CCDP™, CCNP™, CCIE™, and CCSI™. The Cisco Systems logo and the CCIE logo are trademarks or registered trademarks of Cisco Systems, Inc., in the United States and certain other countries. All other trademarks are trademarks of their respective owners.

Copyright Notice

Copyright ©2014, Paul Browning, all rights reserved. No portion of this book may be reproduced mechanically, electronically, or by any other means, including photocopying, without written permission of the publisher.

ISBN: 978-0-9569892-9-1

Published by:

Reality Press Ltd.
Midsummer Court
314 Midsummer Blvd.
Milton Keynes
UK

MK9 2UB

help@reality-press.com

Legal Notice

The advice in this book is designed to help you achieve the standard of the Cisco Certified Network Associate (CCNA) exam, which is Cisco's foundation internetworking examination. A CCNA is able to carry out basic router and switch installations and troubleshooting. Before you carry out more complex operations, it is advisable to seek the advice of experts or Cisco Systems, Inc.

The practical scenarios in this book are meant to illustrate a technical point only and should be used only on your privately owned equipment, never on a live network.

https://t.me/learningnets

Table of Contents

Acknowledgements

Contributors

About the Authors

- Paul Browning
- Farai Tafa
- Daniel Gheorghe
- Dario Barinic

Preface

- Read This First!
- Extra Study Materials
- Getting Hands-on Time
- Does CCNA in 60 Days Work?

Introduction to the Second Edition

Free Stuff

FAQs

How the Programme Works

- Are You Ready?
- Exam Questions
- Your Study Plan
- Preparation Day

Day 1 – Networks, Cables, OSI, and TCP Models

- Day 1 Tasks
- Network Devices
  - *Common Network Devices*
  - *LAN and WAN Topologies*
- OSI and TCP Models
  - *The OSI Model*
  - *OSI Troubleshooting*
  - *The TCP/IP, or DoD, Model*
- TCP/IP
  - *Transmission Control Protocol (TCP)*

https://t.me/learningnets

Internet Protocol (IP)
User Datagram Protocol (UDP)
File Transfer Protocol (FTP)
Trivial File Transfer Protocol (TFTP)
Simple Mail Transfer Protocol (SMTP)
Hyper Text Transfer Protocol (HTTP)
Internet Control Message Protocol (ICMP)
Address Resolution Protocol (ARP)
Proxy ARP
Reverse Address Resolution Protocol (RARP)
Gratuitous Address Resolution Protocol (GARP)
Simple Network Management Protocol (SNMP)
Hyper Text Transfer Protocol Secure (HTTPS)

Cables and Media

LAN Cables
WAN Cables

Connecting to a Router

Router Modes
Configuring a Router

Day 1 Questions

OSI/TCP Model Questions
Cable Questions

Day 1 Answers

OSI/TCP Model Answers
Cable Answers

Day 1 Lab

IOS Command Navigation Lab

Day 2 – CSMA/CD, Switching, and VLANs

Day 2 Tasks

Switching Basics

Carrier Sense, Multiple Access with Collision Detection
Collision and Broadcast Domians
Auto-negotiation
Switching Frames

Switching Concepts

The Need for Switches
Ethernet Frames
Initial Switch Configuration

Virtual Local Area Networks (VLANs)

VLAN Marking
VLAN Membership
VLAN Links
Access Links
Trunking
Configuring VLANs
Basic Switching Troubleshooting
Common Switch Issues
VLAN Assignment Issues
Day 2 Questions
Day 2 Answers
Day 2 Lab
Switching Concepts Lab
Day 3 – Trunking, DTP, and Inter-VLAN Routing
Day 3 Tasks
Configuring and Verifying Trunk Links
Manual (Static) Trunk Configuration
Dynamic Trunking Protocol (DTP)
IEEE 802.1Q Native VLAN
Inter-VLAN Routing
VTP
Configuring VTP
VTP Modes
VTP Pruning
Configuration Revision Number
Basic VLAN Troubleshooting
Troubleshooting Trunking and VTP
Troubleshooting Inter-VLAN Routing
Day 3 Questions
Day 3 Answers
Day 3 Labs
VLAN and Trunking Lab
VTP Lab
Day 4 – Router and Switch Security
Day 4 Tasks
Protecting Physical Access
Console Access

Telnet Access
Protecting Enable Mode
Protecting User Access
Updating the IOS
Router Logging
Simple Network Management Protocol (SNMP)
Securing the Switch
Prevent Telnet Access
Enable SSH
Set an Enable Secret Password
Services
Change the Native VLAN
Change the Management VLAN
Turn Off CDP
Add a Banner Message
Set a VTP Password
Restrict VLAN Information
Error Disable Recovery
External Authentication Methods
Router Clock and NTP
Shut Down Unused Ports
Cisco Discovery Protocol (CDP)
Switch Port Security
CAM Table Overflow Attacks
MAC Spoofing Attacks
Port Security Secure Addresses
Port Security Actions
Configuring Port Security
Configuring Static Secure MAC Addresses
Verifying Static Secure MAC Address Configuration
Configuring Dynamic Secure MAC Addresses
Verifying Dynamic Secure MAC Addresses
Configuring Sticky Secure MAC Addresses
Configuring the Port Security Violation Action
Verifying the Port Security Violation Action
Day 4 Questions
Day 4 Answers
Day 4 Labs
Basic Router Security Lab
https://t.me/learningnets

Basic Switch Security Lab

Day 5 – IP Addressing

Day 5 Tasks

IP Addressing

IP Version 4
Binary
Hexadecimal
Converting Exercise

Address Classes

Subnet Mask Primer

Using IP Addresses

Private IP Addresses

Subnetting

Easy Subnetting
Classless Inter-Domain Routing
The Subnetting Secrets Chart

Route Summarisation

ZIP Codes
Route Summarisation Prerequisites
Applying Route Summarisation

Variable Length Subnet Masking

Using VLSM
Slicing Down Networks

Troubleshooting IP Addressing Issues

Troubleshooting Subnet Mask and Gateway Issues

Day 5 Questions

Day 5 Answers

Answers for the conversion exercises

Day 5 Lab

IP Addressing on Routers Lab
Binary Conversion and Subnetting Practice

Day 6 – Network Address Translation

Day 6 Tasks

NAT Basics

Configuring and Verifying NAT

Static NAT
Dynamic NAT or NAT Pool

https://t.me/learningnets

NAT Overload/Port Address Translation/One-Way NAT
Troubleshooting NAT
Day 6 Questions
Day 6 Answers
Day 6 Labs
Static NAT Lab
NAT Pool Lab
NAT Overload Lab
Day 7 – IPv6
Day 7 Tasks
History of IPv6
Fit for Purpose?
Why Migrate?
Hex Numbering
IPv6 Addressing
IPv6 Address Representation
The Preferred Form
Compressed Representation
IPv6 Addresses with an Embedded IPv4 Address
The Different IPv6 Address Types
Link-Local Addresses
Site-Local Addresses
Aggregate Global Unicast Addresses
Multicast Addresses
Anycast Addresses
Loopback Addresses
Unspecified Addresses
IPv6 Protocols and Mechanisms
ICMP for IPv6
IPv6 Stateful Autoconfiguration
IPv6 Stateless Autoconfiguration
Configuring Stateless DHCPv6
Enabling IPv6 Routing in Cisco IOS Software
IPv6 Compared to IPv4
Day 7 Questions
Day 7 Answers
Day 7 Lab
IPv6 Concepts Lab
https://t.me/learningnets

Hex Conversion and Subnetting Practice
Day 8 – Integrating IPv4 and IPv6 Network Environments
Day 8 Tasks
IPv4 and IPv6 Dual-Stack Implementations
Implementing Dual-Stack Support in Cisco IOS Software
Configuring Static IPv4 and IPv6 Host Addresses in Cisco IOS Software
Configuring IPv4 and IPv6 DNS Servers in Cisco IOS Software
Day 8 Questions
Day 8 Answers
Day 8 Labs
IPv4 – IPv6 Basic Integration Lab
IPv4 – IPv6 Tunnelling Lab
Day 9 – Access Control Lists
Day 9 Tasks
ACL Basics
Port Numbers
Access Control List Rules
ACL Rule 1 – Use only one ACL per interface per direction.
ACL Rule 2 – The lines are processed top-down.
ACL Rule 3 – There is an implicit "deny all" at the bottom of every ACL.
ACL Rule 4 – The router can't filter self-generated traffic.
ACL Rule 5 – You can't edit a live ACL.
ACL Rule 6 – Disable the ACL on the interface.
ACL Rule 7 – You can reuse the same ACL.
ACL Rule 8 – Keep them short!
ACL Rule 9 – Put your ACL as close to the source as possible.
Wildcard Masks
Configuring Access Control Lists
Standard ACLs
Extended ACLs
Named ACLs
Applying ACLs
ACL Sequence Numbers
Add an ACL Line
Remove an ACL Line
Resequence an ACL
ACL Logging

Using ACLs to Limit Telnet and SSH Access
Troubleshooting and Verifying ACLs
Verifying the ACL Statistics
Verifying the Permitted Networks
Verifing the ACL Interface and Direction
Day 9 Questions
Day 9 Answers
Day 9 Labs
Standard ACL Lab
Extended ACL Lab
Named ACL Lab
Day 10 – Routing Concepts
Day 10 Tasks
Basic Routing
Packet Forwarding
Internet Protocol Routing Fundamentals
Flat and Hierarchical Routing Algorithms
IP Addressing and Address Summarisation
Administrative Distance
Routing Metrics
Prefix Matching
Classful and Classless Protocols
Passive Interfaces
Routing Protocol Classes
Understanding Vectors
Distance Vector Routing Protocols
Link State Routing Protocols
The Objectives of Routing Protocols
Optimal Routing
Stability
Ease of Use
Flexibility
Rapid Convergence
Routing Problems Avoidance Mechanisms
Topology-Based (CEF) Switching
Cisco Express Forwarding (CEF)
The Adjacency Table
Accelerated and Distributed CEF
https://t.me/learningnets

Configuring Cisco Express Forwarding
Verifying That Routing Is Enabled
Verifying That the Routing Table Is Valid
Verifying the Correct Path Selection
Day 10 Questions
Day 10 Answers
Day 10 Lab
Routing Concepts Lab
Day 11 – Static Routing
Day 11 Tasks
Configuring Static Routes
Configuring Static IPv6 Routes
Troubleshooting Static Routes
Day 11 Questions
Day 11 Answers
Day 11 Lab
Static Routes Lab
Day 12 – OSPF Basics
Day 12 Tasks
Open Shortest Path First
OSPF Overview and Fundamentals
Link State Fundamentals
OSPF Fundamentals
OSPF Configuration
Enabling OSPF in Cisco IOS Software
Enabling OSPF Routing for Interfaces or Networks
OSPF Areas
OSPF Router ID
OSPF Passive Interfaces
Day 12 Questions
Day 12 Answers
Day 12 Lab
Basic OSPF Lab
Day 13 – OSPFv3
Day 13 Tasks
OSPF Version 3
https://t.me/learningnets

Cisco IOS Software OSPFv2 and OSPFv3 Configuration Differences
Configuring and Verifying OSPFv3 in Cisco IOS Software
Day 13 Questions
Day 13 Answers
Day 13 Lab
Basic OSPFv3 Lab
Day 14 – DHCP and DNS
Day 14 Tasks
DHCP Functionality
DHCP Operations
DHCP Reservations
DHCP Scopes
DHCP Leases
DHCP Options
Configuring DHCP
DHCP Servers on Cisco Routers
DHCP Clients on Cisco Routers
DHCP Packet Analysis
Troubleshooting DHCP Issues
DNS Operations
Configuring DNS
Troubleshooting DNS Issues
Day 14 Questions
Day 14 Answers
Day 14 Labs
DHCP on a Router Lab
DNS on a Router Lab
Day 15 – Layer 1 and Layer 2 Troubleshooting
Day 15 Tasks
Troubleshooting at the Physical Layer
Troubleshooting Link Status Using Light Emitting Diodes (LEDs)
Troubleshooting Cable Issues
Troubleshooting Module Issues
Using the Command Line Interface to Troubleshoot Link Issues
Troubleshooting VLANs and Trunking
Troubleshooting Dynamic VLAN Advertisements

Troubleshooting Loss of End-to-End Intra-VLAN Connectivity
Using the "show vlan" Command
Day 15 Questions
Day 15 Answers
Day 15 Labs
Layer 1 Troubleshooting Lab
Layer 2 Troubleshooting Lab
Day 16 – Review 1
Day 16 Tasks
Day 16 Exam
Day 16 Answers
Day 16 Lab 1 – Switch Configuration
Topology
Instructions
Day 16 Lab 2 – Switch Security
Topology
Day 17 – Review 2
Day 17 Tasks
Day 17 Exam
Day 17 Answers
Day 18 – Review 3
Day 18 Tasks
Day 18 Exam
Day 18 Answers
Day 18 Lab 1 – Static NAT
Topology
Instructions
Solution Hints and Commands
Day 18 Lab 2 – NAT Pool
Topology
Instructions
Solution Hints and Commands
Day 18 Lab 3 – NAT Overload
Topology
Instructions
Solution Hints and Commands

Day 19 – Review 4

Day 19 Tasks

Day 19 Exam

Day 19 Answers

Day 19 Lab – DHCP

Topology
Instructions
Solution Hints and Commands

Day 20 – Review 5

Day 20 Tasks

Day 20 Exam

Day 20 Answers

Day 20 Lab – Static Routes

Topology
Instructions
Solution Hints and Commands

Day 21 – Review 6

Day 21 Tasks

Day 21 Exam

Day 21 Answers

Day 22 – Review 7

Day 22 Tasks

Day 22 Exam

Day 22 Answers

Day 23 – Review 8

Day 23 Tasks

Day 23 Exam

Day 23 Answers

Day 23 Lab – Multi-technology

Topology
Instructions
Solution Hints and Commands

Day 24 – Review 9

Day 24 Tasks

Day 24 Exam

https://t.me/learningnets

Day 24 Answers
Day 25 – Review 10
Day 25 Tasks
Day 25 Exam
Day 25 Answers
Day 26 – Review 11
Day 26 Tasks
Day 26 Exam
Day 26 Answers
Day 27 – Review 12
Day 27 Tasks
Day 27 Exam
Day 28 – Review 13
Day 28 Tasks
Day 28 Exam
Day 28 Answers
Day 29 – Review 14
Day 29 Tasks
Day 29 Exam
Day 29 Answers
Day 30 – Exam Day
Day 31 – Spanning Tree Protocol
Day 31 Tasks
The Need for STP
IEEE 802.1D Configuration BPDUs
Spanning Tree Port States
Spanning Tree Blocking State
Spanning Tree Listening State
Spanning Tree Learning State
Spanning Tree Forwarding State
Spanning Tree Disabled State
Spanning Tree Bridge ID
Spanning Tree Root Bridge Election
https://t.me/learningnets

Spanning Tree Cost and Priority
Spanning Tree Port Cost
Spanning Tree Root and Designated Ports
Spanning Tree Root Port Election
Spanning Tree Designated Port Election
Cisco Spanning Tree Enhancements
Port Fast
BPDU Guard
BPDU Filter
Loop Guard
Root Guard
Uplink Fast
Backbone Fast
Incorrect Root Bridge
Incorrect Root Port
Incorrect Designated Port
Day 31 Questions
Day 31 Answers
Day 31 Lab
Spanning Tree Root Selection Lab
Day 32 – Rapid Spanning Tree Protocol
Day 32 Tasks
The Need for RSTP
RSTP with PVST+
RPVST+
Configuring RSTP
Day 32 Questions
Day 32 Answers
Day 32 Lab
RSTP Lab
Day 33 – EtherChannels and Link Aggregation Protocols
Day 33 Tasks
Understanding EtherChannels
Port Aggregation Protocol Overview
PAgP Port Modes
Auto Mode
Desirable Mode
https://t.me/learningnets

PAgP EtherChannel Protocol Packet Forwarding
Link Aggregation Control Protocol Overview
LACP Port Modes
LACP Active Mode
LACP Passive Mode
EtherChannel Load-Distribution Methods
EtherChannel Configuration Guidelines
Configuring and Verifying Layer 2 EtherChannels
Configuring and Verifying PAgP EtherChannels
Configuring and Verifying LACP EtherChannels
Day 33 Questions
Day 33 Answers
Day 33 Lab
EtherChannel Lab
Day 34 – First Hop Redundancy Protocols
Day 34 Tasks
Hot Standby Router Protocol
HSRP Version 1
HSRP Version 2
HSRP Version 1 and Version 2 Comparison
HSRP Primary Gateway Election
HSRP Messages
HSRP Preemption
HSRP Addressing
HSRP MD5 Authentication
HSRP Interface Tracking
HSRP Load Balancing
Configuring HSRP on the Gateway
Configuring HSRP Preemption
Configuring HSRP Interface Tracking
Configuring the HSRP Version
Virtual Router Redundancy Protocol
VRRP Multiple Virtual Router Support
VRRP Master Router Election
VRRP Preemption
VRRP Load Balancing
VRRP Versions
VRRP Advertisements
Configuring VRRP on the Gateway
https://t.me/learningnets

Configuring VRRP Interface Tracking
Debugging VRRP
Gateway Load Balancing Protocol
GLBP Operation
GLBP Virtual MAC Address Assignment
GLBP Redundancy
GLBP Load Preemption
GLBP Weighting
GLBP Load Sharing
GLBP Client Cache
Configuring GLBP on the Gateway
Day 34 Questions
Day 34 Answers
HSRP Lab
VRRP Lab
GLBP Lab
Day 35 Tasks
Router Memory and Files
Managing the IOS
Booting Options
Booting Process and POST
IOS Licensing
A New Model
License Activation
Day 35 Questions
Day 35 Answers
Day 35 Lab
Day 36 – EIGRP
Day 36 Tasks
Cisco EIGRP Overview and Fundamentals
EIGRP Configuration Fundamentals
EIGRP Messages
EIGRP Packet Header
Hello Packets
Acknowledgement Packets
Update Packets
Query Packets
Reply Packets
https://t.me/learningnets

Request Packets
EIGRP Neighbour Discovery and Maintenance
Dynamic Neighbour Discovery
Static Neighbour Discovery
EIGRP Hello and Hold Timers
EIGRP Neighbour Table
Reliable Transport Protocol
Metrics, DUAL, and the Topology Table
EIGRP Composite Metric Calculation
Using Interface Bandwidth to Influence EIGRP Metric Calculation
Using Interface Delay to Influence EIGRP Metric Calculation
The Diffusing Update Algorithm (DUAL)
The EIGRP Topology Table
Equal Cost and Unequal Cost Load Sharing
Default Routing Using EIGRP
Split Horizon in EIGRP Networks
EIGRP Route Summarisation
Understanding Passive Interfaces
Understanding the Use of the EIGRP Router ID
Day 36 Questions
Day 36 Answers
Day 36 Lab
EIGRP Lab
Day 37 – Troubleshooting EIGRP
Day 37 Tasks
Troubleshooting Neighbour Relationships
Troubleshooting Route Installation
Troubleshooting Route Advertisement
Debugging EIGRP Routing Issues
Day 37 Questions
Day 37 Answers
Day 37 Lab
Day 38 – EIGRP For IPv6
Day 38 Tasks
Cisco IOS Software EIGRPv4 and EIGRPv6 Configuration Differences
https://t.me/learningnets

Configuring and Verifying EIGRPv6 in Cisco IOS Software
Day 38 Questions
Day 38 Answers
Day 38 Lab
Day 39 – OSPF
Day 39 Tasks
Designated and Backup Designated Routers
Additional Router Types
OSPF Packet Types
OSPF Hello Packets
Database Description Packets
Link State Request Packets
Link State Update Packets
Link State Acknowledgement Packets
Establishing Adjacencies
OSPF LSAs and the Link State Database (LSDB)
Router Link State Advertisements (Type 1)
Network Link State Advertisements (Type 2)
Network Summary Link State Advertisements (Type 3)
ASBR Summary Link State Advertisements (Type 4)
AS External Link State Advertisements (Type 5)
OSPF Areas
Not-so-stubby Areas (NSSAs)
Totally Not-so-stubby Areas (TNSSAs)
Stub Areas
Totally Stubby Areas
Route Metrics and Best Route Selection
Calculating the OSPF Metric
Influencing OSPF Metric Calculation
OSPF Default Routing
Configuring OSPF
Troubleshooting OSPF
Troubleshooting Neighbour Relationships
Troubleshooting Route Advertisement
Debugging OSPF Routing Issues
Day 39 Questions
Day 39 Answers

Day 39 Lab
OSPF Lab
Day 40 – Syslog, SNMP, and Netflow
Day 40 Tasks
Logging
Simple Network Management Protocol
Cisco IOS NetFlow
Troubleshooting Utilising NetFlow Data
Day 40 Questions
Day 40 Answers
Day 40 Labs
Logging Lab
SNMP Lab
NetFlow Lab
Day 41 – Wide Area Networking
Day 41 Tasks
WAN Overview
WAN Categories
NBMA Technologies
WAN Components
WAN Protocols
Metro Ethernet
VSAT
T1/E1
T3/E3
ISDN
DSL
Cable
Cellular Networks
VPN Technologies
MPLS
Basic Serial Line Configuration
PPPoE
PPPoE Configuration
https://t.me/learningnets

PPPoE Verification and Troubleshooting
Troubleshooting WAN Connections
Day 41 Questions
Day 41 Answers
Day 41 Lab
PPPoE Lab
Day 42 – Frame Relay and PPP
Day 42 Tasks
Frame Relay Operations
Common Frame Relay Terms
Frame Relay Technology
Configuring Frame Relay
Troubleshooting Frame Relay
Frame Relay Errors
PPP Operations
Configuring PPP
PPP Authentication
Troubleshooting PPP
Day 42 Questions
Day 42 Answers
Day 42 Labs
HDLC Lab
Frame Relay Lab
Point-to-Point Protocol Lab
Day 43 – Review 1
Day 43 Tasks
Day 43 Exam
Day 43 Answers
Day 43 Lab – PPP and NAT
Topology
Instructions
Solution Hints and Commands
Day 44 – Review 2
Day 44 Tasks
Day 44 Lab – PPPoE
https://t.me/learningnets

Solution Hints and Commands
Day 45 – Review 3
Day 45 Tasks
Day 45 Exam
Day 45 Answers
Day 46 – Review 4
Day 46 Tasks
Day 46 Exam
Day 46 Answers
Day 46 Lab – VLANs and STP
Topology
Instructions
Solution Hints and Commands
Day 47 – Review 5
Day 47 Tasks
Day 47 Exam
Day 47 Answers
Day 47 Lab – EIGRP and ACL
Topology
Instructions
Solution Hints and Commands
Day 48 – Review 6
Day 48 Tasks
Day 48 Exam
Day 48 Answers
Day 48 Lab – OSPF
Topology
Instructions
Solution Hints and Commands
Day 49 – Review 7
Day 49 Tasks
Day 49 Exam
Day 49 Answers
Day 49 Lab – OSPF and ACL
Topology
https://t.me/learningnets

Solution Hints and Commands
Day 50 – Review 8
Day 50 Tasks
Day 50 Exam
Day 50 Answers
Day 50 Lab – EIGRP with PPP and ACL
Topology
Instructions
Solution Hints and Commands
Day 51 – Review 9
Day 51 Tasks
Day 51 Lab 1 – STP and VLANs
Instructions
Solution Hints and Commands
Day 51 Lab 2 – VLANs
Topology
Instructions
Solution Hints and Commands
Day 52 – Review 10
Day 52 Tasks
Day 52 Exam
Day 52 Lab – OSPF and Router Security
Topology
Instructions
Solution Hints and Commands
Day 53 – Review 11
Day 53 Tasks
Day 53 Exam
Day 53 Answers
Day 53 Lab – EIGRP and ACL
Topology
Instructions
Solution Hints and Commands
Day 54 – Review 12
Day 54 Tasks
Day 54 Exam
https://t.me/learningnets

Day 54 Answers
Day 54 Lab – OSPF and ACL
Topology
Instructions
Solution Hints and Commands
Day 55 – Review 13
Day 55 Tasks
Day 55 Exam
Day 55 Answers
Day 55 Lab – OSPF and NAT
Topology
Instructions
Solution Hints and Commands
Day 56 – Review 14
Day 56 Tasks
Day 56 Lab
Day 57 – Review 15
Day 57 Tasks
Day 57 Labs
Day 58 – Review 16
Day 58 Tasks
Day 59 – Review 17
Day 59 Tasks
Day 60 – Review 18
Day 60 Tasks

https://t.me/learningnets

Acknowledgements

Thanks to all my classroom students over the years, and to all the thousands of students who have joined www.howtonetwork.com www.in60days.com and www.in60days.net, for giving me regular feedback and ideas.

Contributors

Thanks to Tim Peel, CCNA, for his help in editing this book.

https://t.me/learningnets

About the Authors

Paul Browning

I worked in the police force in the UK from 1988 to 2000. I was always on active duty and spent time both as a detective and as a sergeant. I got involved in IT in 1995 when I bought my first computer and had to get a friend to help me sort out the autoexec.bat file to get DOS working. Then I had to fix something inside the computer when it broke. I sort of enjoyed that so I paid to go on an A+ PC assembly course.

I volunteered to teach e-mail in the police station when that came in, around 1995, and that was fun too. I left the police force to work on a helpdesk in 2000 but quickly grew tired of the monotony of fixing the same problems. I studied hard and in a few months passed my MCSE and CCNA exams. I got a job with Cisco Systems in the UK in late 2000, where I was on the WAN support team.

We were all made redundant in 2002 because the IT bubble had burst by then and I found myself out of work. Frightened and desperate, I offered to teach a Cisco course at a local IT training centre and, to my surprise, they agreed. I quickly had to write some notes and labs, which became a book I called *Cisco CCNA Simplified*. That book has now been replaced by the one you are reading now.



The book gave readers all the information they needed to pass the CCNA exam, as well as the ability to apply everything they had learned to the real world of Cisco networking. The book sold many thousands of copies all over the world, and eventually it turned into an online course at www.howtonetwork.com, which now offers video based IT certification training.

With the notes I had written, I started my own Cisco training company, which taught CCNA and CCNP boot camps in the UK for a few years. I sold the company to a friend in 2008 so I could work on online training, which gave me more time with my family.

Farai Tafa



Farai Tafa, CCIE 14811 RS/SP, is an internetwork engineer with over 10 years of experience in core IP routing, LAN and WAN switching, IP telephony, and wireless LAN implementation. He currently holds two Cisco CCIE certifications in the Routing and Switching and the Service Provider tracks. His other certifications include CCVP, JNCIA, JNCIS, and ITILv3 Foundation.

Farai lives in Dallas, Texas, with his wife and two daughters.

Daniel Gheorghe

https://t.me/learningnets

Daniel Gheorghe is a CCIE in Routing and Switching. He is currently preparing for his second CCIE certification (in Security) and he is developing his skills in system penetration testing. He also holds numerous certifications in networking and security, from Cisco and other vendors, including CCNA, CCDA, CCNA Security, CCNP, CCDP, CCIP, FCNSA, FCNSP, and CEH. He took an interest in IT at an early age and soon developed a passion for computer networking, which made him study hard in order to reach an expert level.



Daniel has worked for different Cisco Partners and System Integrators in Romania in system design, implementation, and troubleshooting for enterprise-level networks. He is also involved in several international freelance consulting projects in his areas of expertise. Daniel is a very dynamic person, and in his spare time he likes to travel and to participate in all kinds of sports.

Dario Barinic



Dario Barinic is a network expert (dual CCIE #25071 – Routing and Switching, and Service Provider) with a Master of Engineering degree and eight years of experience in the networking field. He also holds other certifications, such as Cisco CCNA and CCNP, HP AIS, ASE, MASE, and various Cisco specialisations.

Dario is specialised in the area of routing and switching (designing, implementing, troubleshooting, and operating service provider and large enterprise WAN and LAN networks). His major fields of interest are service provider/large enterprise networks (core routing and switching), network security, and passing on knowledge to enthusiastic individuals who are at the start of their networking career.

Dario works as a regional systems integrator for a Cisco Gold Partner in Zagreb, Croatia, where he lives. He is also involved in various international freelance consulting projects, primarily in the area of routing and switching.

https://t.me/learningnets

Preface

My name is Paul Browning and, along with Farai, Dario, and Daniel, my job is to get you through your CCNA (or ICND1 and ICND2) exam(s) in the next 60 days. Your job is to do what I tell you to do, when I tell you to do it. If you can do that, then in 60 days' time you will be a qualified Cisco CCNA engineer. If you skip days or try to play catch-up by doing two or three days' work when you have time, you will fail – badly. Trust me, I've been teaching a long time and I know what I'm talking about.

Do any of the following problems sound familiar to you?

"I just don't know where to start studying. I feel overwhelmed by the information."

"I've bought all the CBT-style videos and books, and have even been on a course, but I don't feel ready to take the exam and I don't know if I ever will."

"I've been studying for a long time now, but I haven't booked the exam yet because I just don't feel ready."

I hear these comments every day from Cisco students on forums and via e-mails to my office. I've come to realise that the problem isn't the lack of quality training materials; that used to be the case in the late '90s, but now there are too many training manuals. The problem isn't the lack of desire to pass the exam. The problem is a lack of two things which mean the difference between success and obscurity – a plan and structure.

This is why personal trainers do so well. We can all exercise every day, go for a run, do push ups, and eat healthy food, but having a trainer means you don't have to think about it. You just turn up and do what he tells you to do and you get the results (unless you cheat). This is where I come in – you turn up at the time you agree to each day and do what I ask you to do. Don't argue with me, don't complain, and don't make excuses as to why you can't do something. Just do it, as the Nike slogan goes.

Read This First!

I've learned a lot and have had some great feedback from the first version of this book, so I thought I'd add this bit to save you and me some time.

1. In order to pass the exam, you need both this book and access to either Packet Tracer/GNS3 or a live rack of Cisco equipment. Although I do own other training websites for IT certifications and I do refer to them sometimes, there is absolutely no need to join them in order to pass.
2. If Cisco make any exam changes after this book is printed, I will add notes/videos or exams to www.in60days.com/book-updates so you aren't disadvantaged in any way. Please do check the very last page of this book for your access codes.
3. You must dedicate two hours per day for 60 days in order to pass the exam. More is better if you can manage it. It's only for two months. I've done my best to balance the book out but some days will be longer than two hours whilst others will be shorter, so please do extra study to fill up the time if you finish a module early.

https://t.me/learningnets

4. I've added tons of resources to accompany this book at www.in60days.com. This will make it easier to keep you up to date on any changes. You can access them all by entering the code which is on the very last page of the book. To save space I've put all the cram guides, bonus labs, and study tools there also. Otherwise the book would be over 1000 pages!
5. This book has been prepared by myself, a CCIE, and two dual CCIEs but, being human, there still may be the odd error. Please come over to www.in60days.com where we will post any corrections and updates on the errata page.
6. The previous version of this book had around 150 pages of goodies at the back including cram guides, labs and other extras. To save space I've moved them all onto www.in60days.com. At the last page of this guide is your codeword. You will need to use this to get access to the bonus material for the book by way of proof of purchase.

Extra Study Materials

After ten years of working as an IT consultant and teaching Cisco, I've found that almost every student uses more than one resource. It makes sense, I suppose, as every resource differs. Recognising that you will probably do this, I wanted to mention that I do run other websites. I'm not selling them to you but if you are going to look around for supplemental stuff, then bear them in mind. Please also note that all you need to pass, as I said above, is this book and access to Packet Tracer, GNS3, or live Cisco equipment – that's all.

www.howtonetwork.com – unlimited video-streaming training for Cisco, Microsoft, Juniper, and much more. If you do decide to join, then please use the code "60book" for a BIG discount. Use this site if you want to study at your own pace and will be doing more than just the CCNA exam.

www.in60days.com – free site to accompany this book, with updates, quizzes, and other goodies.

www.subnetting.org – free site to drill your subnetting skills.

There are many other training vendors out there but because I'm self-taught, I can't really tell you what I think, so feel free to have a surf around.

Getting Hands-on Time

I mentioned Packet Tracer above, as well as GNS3. Here are your options for getting hands-on time.

Download the latest version of Packet Tracer (PT). This is a router and switch simulator created for Cisco Academy students. I've completed many of the labs and examples in this book using PT purely for convenience. Bear in mind that PT is not live equipment so it will never act in exactly the same way live equipment does. Some students become confused when they can't see certain commands or get the same results they would have gotten when using live equipment. I've had many frustrated students contact me trying to get labs working properly only for me to find out they were using PT. In my opinion, it's enough for CCNA-level study but not beyond that, and remember that for job interviews, you need to have some hands-on time

https://t.me/learningnets

using live equipment.

Next option is a router emulator. This is running actual Cisco IOS code on your computer. GNS3 is a free tool used by many thousands of Cisco engineers, from CCNA to CCIE, to create virtual networks for lab work. The major weakness of GNS3 is that it cannot emulate Cisco switches (this may change soon) because they use hardware to forward frames. You can prepare around 70% towards the exam using GNS3, but then you need to revert to either PT or live switches for lab work. This may change in the near future if Cisco agree to release some of their code to the public to allow students to study for exams.

I've created my version of GNS3 with a network topology created at www.howtonetwork.com/vRack. It's free.

Live equipment is another choice. You can buy reasonably priced racks bundled on eBay. You will need at least two 2960 switches and three or four routers in order to do all the labs. I've tried to keep it simple with the minimum amount of labs in this book. You will need to have the correct cables and interface cards, which is why many people turn to racks on eBay. Just double check the price because many racks can be overpriced.

Cisco do test you on 15.x IOS in the exam; however, at the moment, it is a tiny part of the syllabus so anything running 12.3 onwards will do everything you need. If you plan to take the CCNP exam, then you may prefer to choose higher-end models.

Your last option is renting remote racks. Cisco offer a rack rental service (although it's an emulator) which will cover all your CCNA needs and beyond. I may have a live rack on www.howtonetwork.com as you read this so please check. Another company is www.mindtechcom.com but they only offer CCIE rack rental; however, you do get a free hour when you register, and their switches are very useful for doing all the switching labs you need to work on.

Does CCNA in 60 Days Work?

My idea for the programme came whilst following a keep fit programme provided by a special forces soldier. He wrote a get fit guide where every day you ate certain foods at certain times and did prescribed workouts. The results for me were amazing. I put it down to not having to think; each day I did what he told me to do and I saw my body literally transform from flabby to fit.

It then struck me. If a step-by-step fitness programme (which is now all the rage) works for many tens of thousands of normal people, surely it would work for pretty much anything else – like learning guitar, speaking Spanish, or even passing Cisco exams. *Cisco CCNA in 60 Days* was born. The results have been astounding. I started to receive e-mails and forum posts every week from people who had been stuck, sometimes for years, and who were now passing their exams.

I'm not sure why I was surprised, but I had my critics of course. Most hid behind usernames and posted negative reviews on Amazon. When I read them I realised they hadn't actually read what I wrote or even followed the programme at all. They were looking for reasons to hate my programme. But it all boils down to this, I suppose: If you follow the 60-day programme, will it

https://t.me/learningnets

work for YOU?

Well, please don’t take my word for it. The programme has been around for over 12 months now, and here is a very small sample of the results.



https://t.me/learningnets





★★★★★ **CCNA Passed!**, December 21, 2012

By **R. Rios** (Lebanon, PA USA) - See all my reviews
REAL NAME

Amazon Verified Purchase (What's this?)

This review is from: Cisco CCNA in 60 Days (Kindle Edition)

What can I says? This really work! (of course... if you follow the instructions!). I passed my CCNA 12/14/12 and I love it! I was able to solved all exam Labs, etc. Also, may sure do a lot of labs and just practice, practice and practice. The subnetting table really work and save you a lot of time in the exam. Finally if you want pass your exam without "braindumb" this is your choice.

★★★★★ **Well written guide for getting your certification.**, April 7, 2013

By **Igor Zinovik** - See all my reviews

Amazon Verified Purchase (What's this?)

This review is from: Cisco CCNA in 60 Days (Paperback)

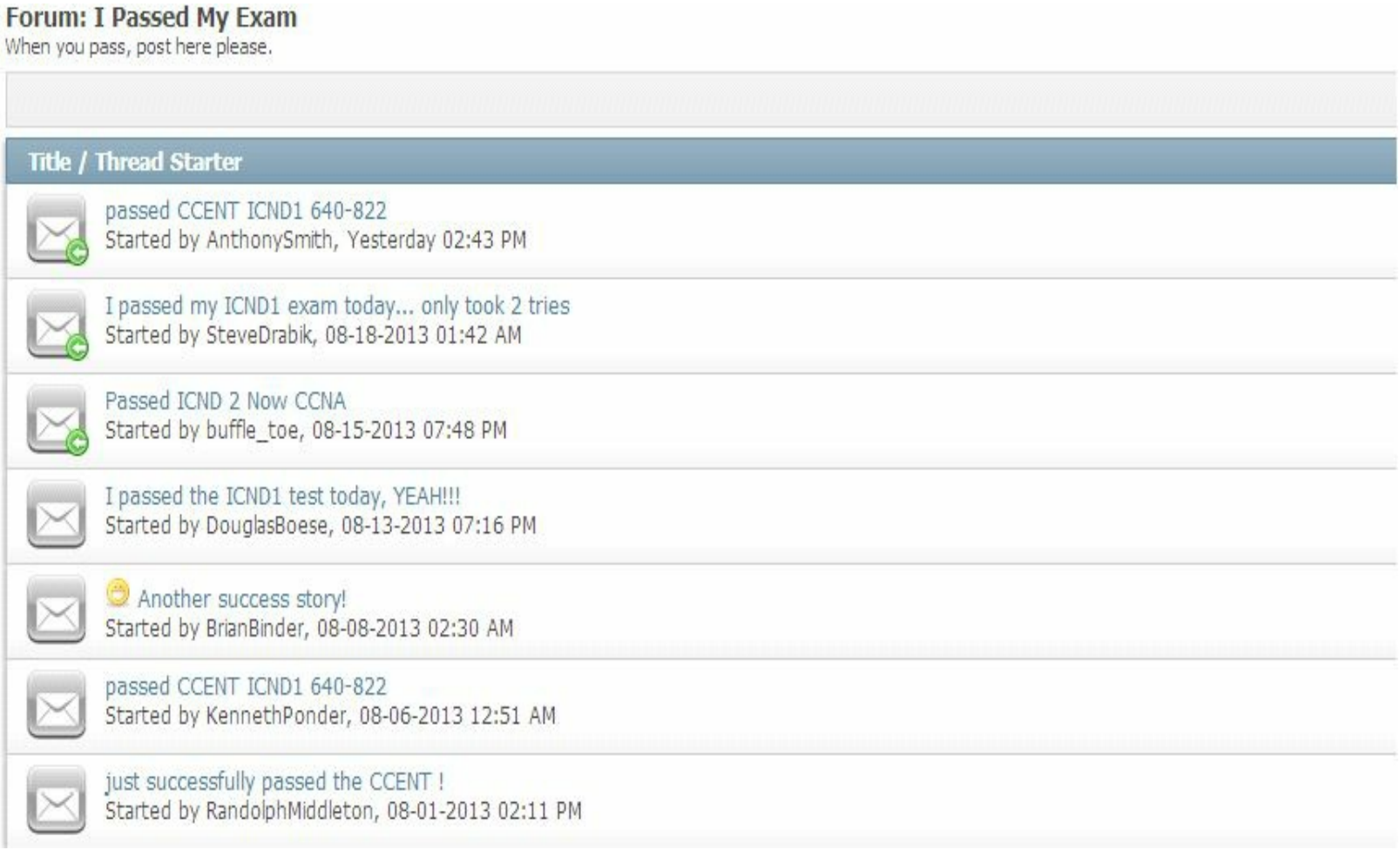
Material is well written and author emphasizes you to practice a lot. Motivation chapter is very inspiring.

This book really helped me to understand subnetting, supperneting, VLSM and route summarization.

I can write a lot of good words about Pauls book, but none of them can express value of this book.

When words are not enough, actions and results will speak themselves: I read this book and successfully passed my CCNA exam.

https://t.me/learningnets



Of course there are countless e-mails, phone messages, blog comments, and more forum posts which I can't fit in here but hopefully I've made my point.

https://t.me/learningnets

Introduction to the Second Edition

Cisco are a pretty clever company, especially when it comes to marketing and positioning their products and certifications. If they see a new technology they think will give them a market advantage, they buy the company. In order to support this equipment, they need well-trained and knowledgeable engineers. This is where you come in.

Cisco, for their part, endeavour to keep the perceived value of their certification programme at a high level. For this and other reasons, the certification process is regularly updated. The latest update, the Cisco CCNA Routing and Switching certification, has seen the most sweeping amount of changes since the exam started. Not only has the syllabus been updated to reflect new technologies, such as IPv6, but the level of difficulty has been dramatically increased as well. And I'm sure you have already noticed that it is no longer called the CCNA but the CCNA RS, which differentiates it from the other CCNA tracks. To confused matters, Cisco refer to the exam as the CCNAX.

It's also worth bearing in mind that Cisco now require you to have at least the ICND1 before taking any specialisation tracks, such as Voice or Security, but please do check the Cisco website for the latest news and updates – www.cisco.com/go/ccna. I am often asked about which exam you need to have in order to take the Security or Voice certs, or about pass marks, etc. It's always best to check directly with Cisco regarding these questions.

The exam updates are both good and bad news for you. Good that when you pass, you will be admired and respected by colleagues and employers, but bad in that you have a very difficult task ahead of you. You have a huge amount of information to digest and understand, as well as complex configuration tasks to configure and troubleshoot, with the clock ticking whilst under exam conditions.

In order to help you pass the new-style CCNA exam, I've completely rewritten this book. Some parts of the first edition have stayed because they teach you exactly what you need to know and they have been battle tested by thousands of students who came before you. Other parts have been improved or updated as a result of feedback. Entirely new sections have been added due to changes to the syllabus.

I've used several tools this time, including my personal experience in the exams, dual CCIE Farai Tafa's CCNP study guides, real-world experience, RFCs, and what I've learned since 2000, when I left the police force in the UK and started my career in Cisco networking. I've also hired CCIE Daniel Gheorghe and dual CCIE Dario Barinic, who have added sections, updated others, and trimmed other bits out. Bear in mind that all three CCIEs are full-time network architects I hired to improve this guide. None of them teach internetworking, they DO internetworking. Bear that in mind when you are checking out other books and training materials!

Free Stuff

Unlike Sybex and Cisco Press, Reality Press is a tiny publishing operation. In fact, to be honest, it's just me! I sit in my little office writing and working on my training websites and hire

https://t.me/learningnets

freelancers when I need them. In fact, here is me taking a break from editing this book:



I'm telling you this because I need a small favour from you.

I need your help to promote this book and get the word out by posting a positive review on Amazon. I do my best to give you great value-for-money and your review will really help. When you've done that, please fill in the form on www.in60days.com/reviews, attach a screenshot, and I'll send you access to a CCNA exam to help you prepare for the real thing.

https://t.me/learningnets

FAQs

Q. Is this book the same as your other CCNA book, *Cisco CCNA Simplified*?

A. Nope. I do have some of the text from that and some from my CCNP books in here, but most of it is new. I wanted to include other stuff and some more of my own comments and observations, so this book is an improvement on the others in many ways. I've retired *CCNA Simplified* now.

Q. I've done a few days now and no labs. Where are all the labs?

A. You can't do labs if you don't know the theory yet. You'll move from mostly theory to mostly labs as you get closer to the exams.

Q. Do I need to join www.in60days.net?

A. No. I designed this book to be a standalone resource. On the website, instead of text I do presentations on video and demonstrate all the labs, but in the book I do it all in text format with figures. If you have the money to spare and like lectures then feel free to join, but you don't need to. Otherwise, check out www.in60days.com, which complements this book.

Q. Does the book cover network foundations for beginners?

A. It used to but because the new exam subjects have added over 300 pages to this book, it's now impossible to fit in many of the basics. If you are a novice, I recommend reading a good Network+ book first.

Q. Why is some stuff in your cram guide but not in the theory?

A. Some stuff I just want to give you in the cram guide, but if I want to cover it in more detail, it will be in the book.

Q. Should I do the one-exam route or the two-exam route?

A. You can do either with this programme. At the 30-day mark, you can take the ICND1 exam, or you can continue on to the ICND2 module and at the end take the CCNA exam.

Q. Which is best?

A. There is no best. It is cheaper to take one exam and get it over with, but there is more to cover. The two-exam route gives you more breathing space and you get a qualification after the first exam. Personally, I'd take the two-exam route, as it lets you focus on less topics per exam.

Q. How much time do I need to study each day?

A. Set aside two hours per day. Bear in mind that the average person watches five hours of TV every day and more on weekends.

Q. What if I miss a day?

A. You'll want to avoid that at all costs. Find a time when you can study every day. If you have to miss a day, then just pick up where you left off the next day.

Q. What if I have a question?

https://t.me/learningnets

A. Feel free to post any questions you have on the forum at www.in60days.com.

Q. Can a person really pass in just 60 days? Cisco Academy teaches the CCNA course over two years.

A. They do, but it is usually only one evening per week for two hours, with 20 to 30 students per class. The poor results speak for themselves on that programme. My method is more intensive but it is also of very high quality.

Q. Do I need to buy anything else?

A. Not really. You need this book and some Cisco equipment. If you really want extra stuff, then please check out the links at the beginning of the book.

Q. I have more than two hours per day to spend on studying, so can I study more?

A. Sure. Study the same stuff again or do more labs. Don't study what you already know.

Q. What if I can't do two hours per day?

A. You will surely fail.

Q. Where are the troubleshooting labs?

A. They all are! You will no doubt make mistakes all the way through the labs and have to fix them in order to finish the lab. This is especially true with the challenge labs which have no solution provided.

https://t.me/learningnets

How the Programme Works

The 60-day study programme offers a combination of learning techniques, including reading, reviewing, cramming, testing, and hands-on labs. You will take in new information for the first few sessions and then start to review each module each day, as well as implement the lessons on live Cisco equipment. You will then begin to employ the theory to exam-style questions and eventually apply your knowledge in the real exam.

You need to factor in two hours of study per day spread amongst the theory, labs, exams, and review. I've also built in free sessions for you to choose what you want to study. You start off with mainly theory and then build up to mainly labs and exams, plus review. You will review every lesson the next day and then come back to it again on other review days, as well as in labs and exams. Take NAT, for example:

Day 6 – NAT
Day 6 – NAT labs
Day 18 – NAT review
Day 20 – NAT labs
Days 23 through 25 – Free study and NAT labs
All days – NAT in the cram guide

In addition, there are NAT challenge labs and you study NAT every day in the cram guide. The same goes for many other subjects. Minor subjects such as CSMA/CD I refer to twice, but that is all. There is little chance these will come up in the exam, so there is little incentive to remember them. There will be ample time to cover everything, as well as free study sessions where you can go over any weak areas. You should keep working on your weak areas until there are none left.

You'll start off with some preparation sessions, and please do not skip these. I can tell you for a fact that a person with a strong reason and desire to pass will always pass. A person who sort of, kind of likes the idea of passing the CCNA exam will soon give up when he sees the amount of work involved.

UPDATE: I've moved the motivational guide to www.in60days.com to save space.

The motivational guide will get you focused on the WHYs of wanting to pass. This will be the magnet which draws you towards your 60 daily study sessions and your final goal of becoming a Cisco CCNA engineer (and beyond, I hope).

This study guide is comprised of a mixture of content from several sources, including:

- Original notes and ideas exclusive to this guide
- Some notes from my CCNA study guide, *Cisco CCNA Simplified* (out of print)
- Farai Tafa's *CCNP Simplified* study guides
- Presentation notes from my in60days.net members-only programme
- Extra notes, labs and explanations

http://t.me/learningnets

- Notes and updates from CCIEs Dario and Daniel

If you have read any of the books above or have used the resources, some of the content may seem familiar in places. The difference is I've brought everything together and have broken it down into daily study sessions. Over 90% of the content in this guide is completely new and original. We'll dip into the CCNP notes now and again when I want to add some extra details for you, or sometimes you'll need to go a bit beyond the CCNA level for stuff to make sense; otherwise, more questions are left hanging in the air, and we don't want that, do we?

I have included some bonus labs on in60days.com, so if you want to test your hands-on skills further, then please follow those. If you're looking for some other review materials, please check out the free white papers section at www.in60days.com.

Are You Ready?

The subjects below are covered in the CCNA exam syllabus. Often, exams are themed whereby they drill you hard on one or two subjects whilst other subjects are left alone. It is the luck of the draw. This course is designed to leave no gaps in your knowledge at all.

I've split your study into ICND1 and ICND2. When you book your exam(s), the exam titles are 100-101 for ICND1 and 200-101 for ICND2. You can also take both exams at the same time in the 200-120 CCNAX composite exam. I would recommend that you take the two-exam route because you can concentrate on specific topics and there is less chance of becoming overwhelmed. The downside, of course, is having to pay for two exams, which is more expensive.

ICND1	ICND1	ICND1	ICND1	ICND1	ICND1
Switching	**IPv4/IPv6**		**IOS**	**TCP**	**Routing**
Security*	Addressing		Security*	DHCP*	Static*
Basic Config*	VLSM		NAT*	DNS	Dynamic*
Cables			ACLs	TCP/IP	OSPFv2/v3* Single-area
DTP/VLANs*	Subnetting		NTP	OSI	Inter-VLAN
CSMA/CD			CDP		Concepts
ICND2	**ICND2**	**ICND2**	**ICND2**	**ICND2**	**ICND2**
Switching	**IPv4**	**WAN**	**IOS**	**IP Services**	**Routing**
STP/RSTP*	IPv6	Frame Relay*	ACLs*	FHRP	OSPFv2/3* Multi-area
EtherChannel	NAT*	PPP*	VPN	SNMP	EIGRP*
Trunking*	Summarisation	PPPoE	Licensing	Syslog	Inter-VLAN
VTP*		Broadband	Manage	Netflow	
			Booting		

https://t.me/learningnets

As indicated in the chart above, the upper area outlines ICND1 subjects and the lower area

outlines ICND2 subjects. If you are taking the CCNA exam, questions pertaining to all of the subjects above could be asked in the exam. The asterisks denote subjects for which you may get hands-on labs in the actual exam set by Cisco. As you go along, please tick off each area you feel you fully understand. Of course, each area needs to be ticked before you attempt the exam!

The chart above is not a definitive guide, by the way; however, it represents my best effort at making sure the core stuff is covered for each exam. There is no guarantee that Cisco won't throw the odd curveball at you! Also, remember that you could be required to troubleshoot all of the above (please check the syllabus via Cisco.com for more information). My recent experience retaking the ICND2 showed me that Cisco can also put ICND1 topics in the ICND2 exam, so please review those! For this reason you will see me putting ICND1 topics into some of the ICND2 labs.

Exam Questions

Cisco exams are recognised as amongst the toughest in the IT industry. You have not only a large amount of theory to learn for every exam, but you also need to know how to apply your knowledge under exam conditions whilst the clock is ticking.

The CCNA exams are broken down into theory questions and hands-on labs using a router or switch emulator which responds in much the same way as a live one will. Theory questions can be multiple choice or drag-and-drop, where you have to drop answers into the correct place. You can also be shown a network diagram or router output and then be asked to answer a question about it. Additionally, questions can entail multiple parts, for example, four different questions pertaining to the same issue.

The hands-on simulation questions can ask you to configure or troubleshoot routing or switching issues. You may have to connect to multiple devices in order to complete the task. You could also be asked to log in to one specific device and issue various "show" commands in order to answer questions. Cisco may even block you from using certain commands to test your knowledge of more specific IOS commands.

So I think we can agree that the exam is tough, but every day, hundreds of people just like you pass. I was working on a helpdesk when I passed my CCNA exam and I had very limited networking knowledge at the outset.

Your Study Plan

I've moved the study plan online so please download it at www.in60days.com.

Preparation Day

You want to start studying today, I know. But would you start a marathon without a good pair of trainers on and a bottle of water? If you did, you would quit soon afterwards. I recently looked at the statistics of my free 60-day study videos on YouTube. Look at how people dropped off so quickly:

Day 1 – 14,353 views

https://t.me/learningnets

Day 2 – 4912 views
Day 3 – 2526 views
Day 41 – 264 views

It is quite sad, really, but it confirms my experience of teaching Cisco courses over the past 10 years. Cisco does not publish figures of how many people start and then quit the Cisco Academy programme, but the drop-off rate is horrendous. Very few even attempt the exam at the end of two years, and with an international pass rate of around 50%, the outlook is grim! All that money and time down the drain, and if Cisco can't get you through the CCNA exam, then who can?

I can, for one!

Preparation day is all about you writing down your goals and motivation for this course. Please print and follow the motivational e-book available online at www.in60days.com. Please read it all and do all of the exercises.

https://t.me/learningnets

Day 1 – Networks, Cables, OSI, and TCP Models

Day 1 Tasks

- Read today's lesson notes (below)
- Read the ICND1 cram guide (download from www.in60days.com)

Today you will learn about the following:

- Network devices and diagrams
- The OSI and TCP models
- Cables and media
- Connecting to a router

This module maps to the following ICND1 syllabus requirements:

- Recognise the purpose and functions of various network devices, such as routers, switches, bridges, and hubs
- Select the components required to meet a given network specification
- Identify common applications and their impact on the network
- Describe the purpose and basic operation of the protocols in the OSI and TCP/IP models
- Predict the data flow between two hosts across a network
- Identify the appropriate media, cables, ports, and connectors to connect Cisco network devices to other network devices and hosts in a LAN

Network Devices

As a network engineer, you will be using a range of network cables and other media. You need to know which cables will work with which devices and interfaces for WAN, LAN, and management ports. Much of the information will serve as a review if you have studied the CompTIA Network+ before the CCNA (which I recommend).

Common Network Devices

Network Switches

Only a few years ago, networks were still pretty small. This meant that you could simply plug all devices into a hub or a number of hubs. The hub's job was to boost the signal on the network cable, if required, and then pass out the data on the wire to every other device plugged in. The problem with this, of course, is that the message was intended for only one network host, but it would be sent to tens or hundreds of other hosts connected to other hubs on the network. (Hubs and switching technology will be covered in more detail in the next module.)

Network switches are a more intelligent version of hubs. Switches use Content Addressable Memory (CAM) and therefore have the ability to remember which device is plugged into which

https://t.me/learningnets

port. Cisco manufactures switch models which are designed to work in small offices and all the way up to large enterprise networks consisting of thousands of devices. We will explore this in more detail later, but, basically, switches operate by using the device's MAC addresses (known as Layer 2) and IP addresses (known as Layer 3), or they can perform more complex tasks, such as processing lists of permit/deny traffic or protocols and port numbers (known as Layer 4), or a combination of all these layers and more. We will cover what comprises these layers and their functions later in this module.

Early versions of switches were referred to as network bridges. Bridges examined the source ports and MAC addresses of frames in order to build a table and make forwarding decisions. The tables were typically accessed via software, whereas switches used hardware (i.e., Application Specific Integreated Chips, or ASICs) to access a CAM table (more on this later). Therefore, a switch can be thought of as a multiport bridge.

Using a switch (see Figure 1.1) allows you to divide your network into smaller, more manageable sections (known as segments). This in turn allows the teams who work inside your company, such as human resources, finance, legal, etc., to work on the same section of the network at the same time, which is useful because the devices will spend most of their time communicating with each other.

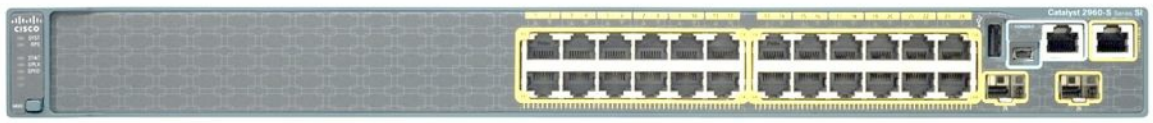
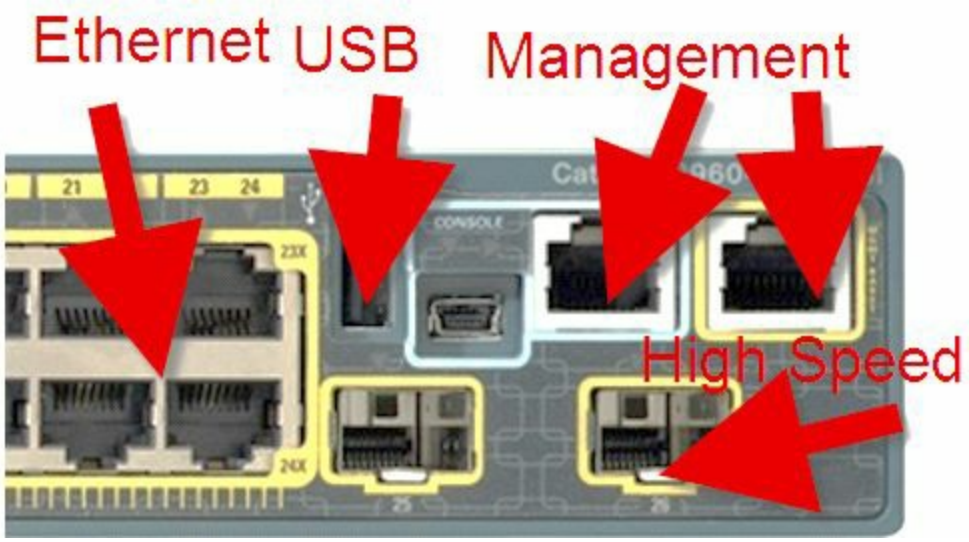


Figure 1.1 – Cisco 2960 Switch

Each device will connect to an interface on the switch, which is referred to as a port. Common network port speeds are 100Mbps and 1000Mbps (usually referred to as 1Gbps). There are often fibre ports you can use to connect a switch to another switch. Each switch features management ports, which you can connect to in order to perform an initial configuration and gain general access for maintenance over the network.

Figure 1.2 below shows a close-up of a Cisco 2960 switch. Several models of the 2960 are available to meet the needs of a small- to medium-sized business.



https://t.me/learningnets

Figure 1.2 – Switch Interface Types

You can also use IP telephones with the switches and, even better, the switch ports can provide power to these telephones (using power over Ethernet (PoE) interfaces). The basic network switch will be used to:

- Connect network devices such as printers and PCs
- Give access to network servers and routers
- Segment the network with VLANs

VLANs are virtual Local Area Networks. We will cover these in detail in Day 2.

Routers

As a Cisco engineer, you will spend a lot of time installing, configuring, and troubleshooting routers. For this reason, over half of the CCNA syllabus is dedicated to learning all about router configuration.

A router (see Figure 1.3) is a device used for networking. While network switches involve devices on the same network communicating with each other, the router communicates with devices on different networks. Older models of routers only had ports, which were physically built into them and attached to the motherboard. This is still sometimes the case, but modern networks now require a router to perform functions for IP telephony, switching, and security, and to connect to several types of telecoms companies. For this reason, routers are also modular, which means you have the router chassis and empty slots into which you can connect a variety of routing or switching modules.



Figure 1.3 – Modular Cisco Router with a Blank Slot to the Right

The Cisco website has a lot of advice and information available to explain which router model will suit your business needs. There are also tools which will help you select the correct model and operating system. It's well worth your time learning how to navigate the support and configuration pages and bookmarking them for quick reference.

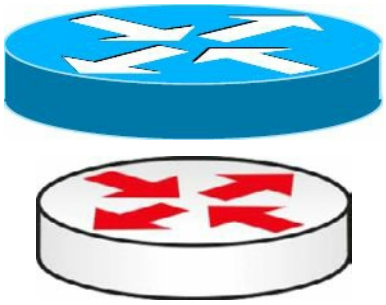
How Networks Are Represented in Diagrams

All network engineers need a common method to communicate, despite which vendor and telecoms provider they are using. If I had to describe my network topology to you for design or security recommendations, it would work much better if it were in an agreed format as opposed to something I had drawn by hand from memory. The Cisco Certified Design Associate (CCDA) exam is where you will learn about network topologies in far more detail. As for the CCNA exam, you will need a basic understanding of these topologies because the exam may present network issues and ask where you think the problem lies.

Here are the common symbols for network devices you will encounter in your work as a network engineer. You can download these icons from the Cisco website if you type "Cisco

https://freelearning.net

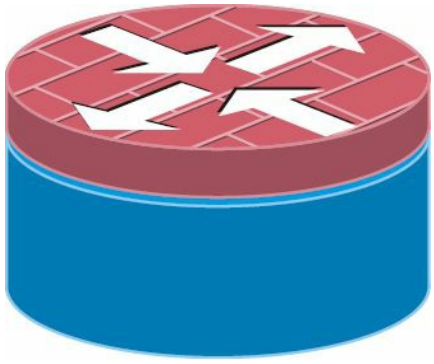
icons” in your browser’s search engine. We use either plain blue or color (for the Kindle version). I’ve used a mix of the most common router and switch symbols throughout the book so get used to the types you will see in network diagrams in the real world.



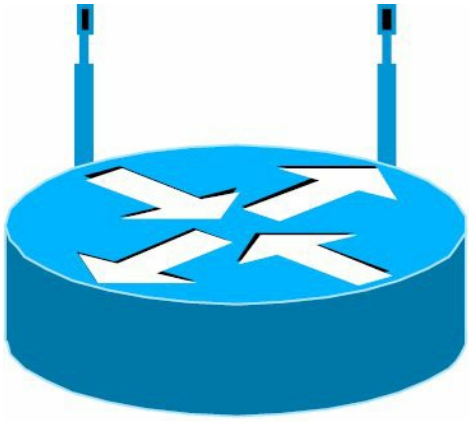
Routers



Switch (Layer 2)

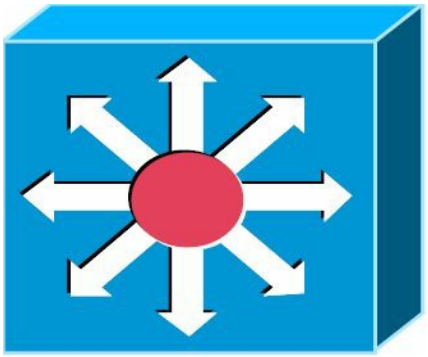


Router with Firewall

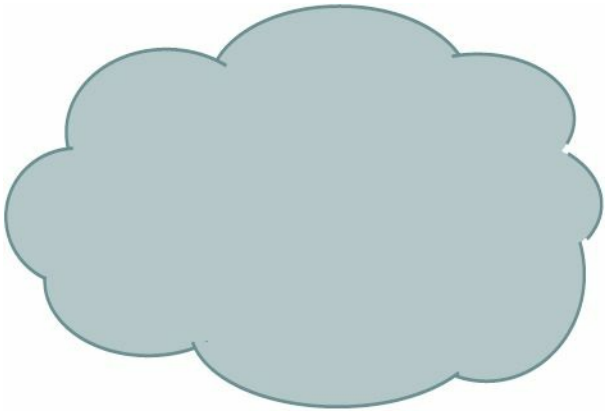


Wireless Router

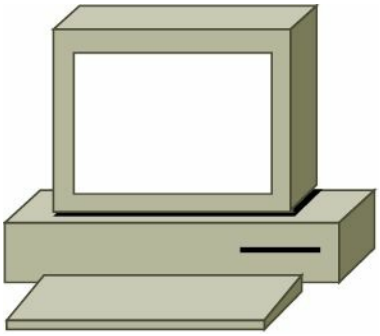
https://t.me/learningnets



Multilayer Switch



The Cloud – Equipment Owned by the Telecoms Provider



End Device – a PC

Serial Line

Ethernet Link



IP Telephone



Firewall

https://t.me/learningnets

LAN and WAN Topologies

Topology refers to how network equipment is arranged in order to communicate. How this is done could be limited by the communication protocols the equipment uses, cost, geography, or other factors, such as the need for redundancy should the main link fail.

You should also note that there is often a difference between physical and logical topology. Physical topology is how the network appears when you look at it, whereas logical topology is how the network sees itself. The most common topologies are described in the following sections.

Point-to-Point

This topology is used mainly for WAN links. A point-to-point link is simply one in which one device has one connection to another device. You could add a secondary link connecting each device but if the device itself fails, then you lose all connectivity.



Figure 1.4 – Point-to-Point Topology

Bus

This topology was created with the first Ethernet networks, where all devices had to be connected to a thick cable referred to as the backbone. If the backbone cable fails, then the network goes down. If a cable linking the device to the backbone cable fails, then only that device will lose connection.

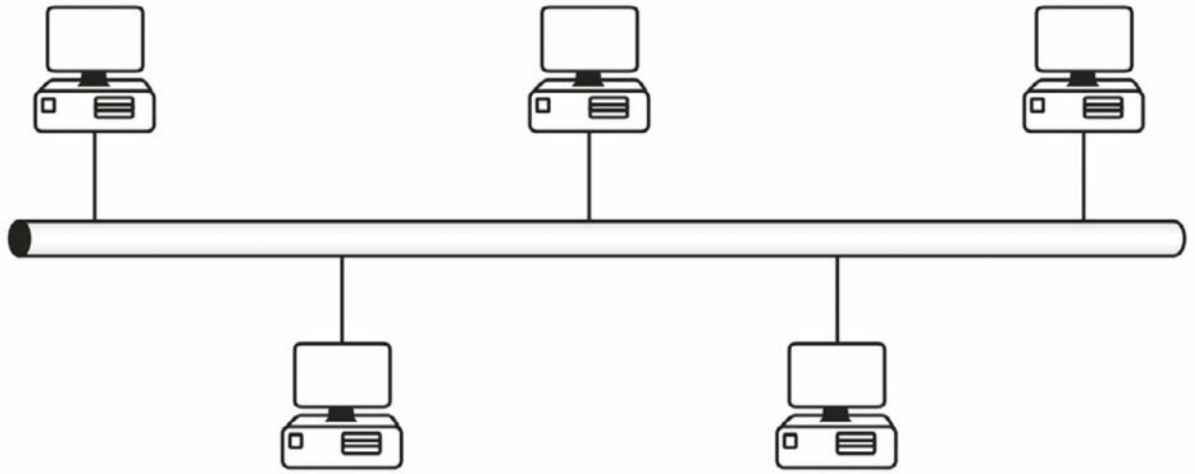


Figure 1.5 – Bus Topology

Star

This is probably the most common topology you will encounter. Each network device is connected to a central hub or switch. If one of the cables to the devices fails, then only that device becomes disconnected.

https://t.me/learningnets

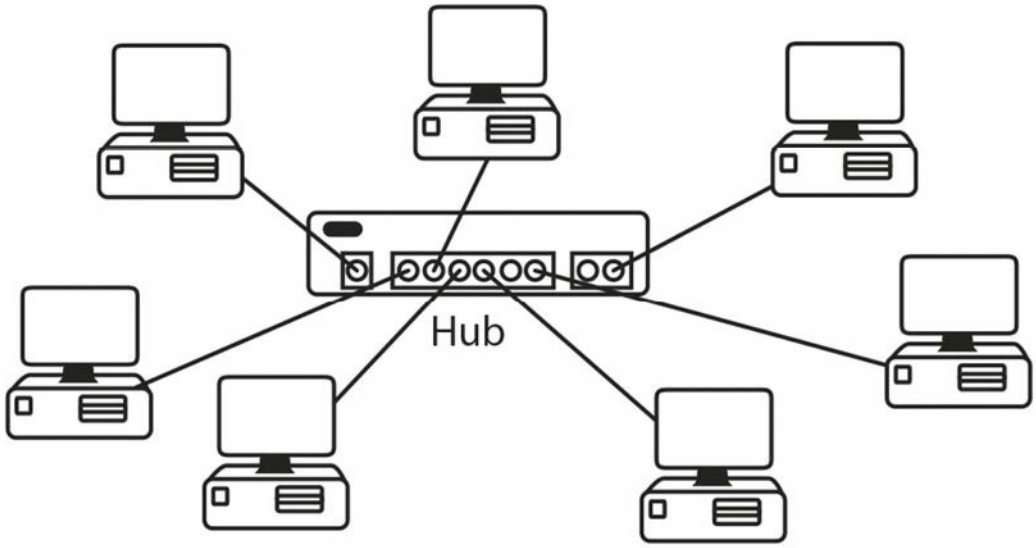


Figure 1.6 – Star Topology

Ring

A ring topology is used by token ring networks and Fiber Distributed Data Interface (FDDI) networks, both of which went out of use several years ago.

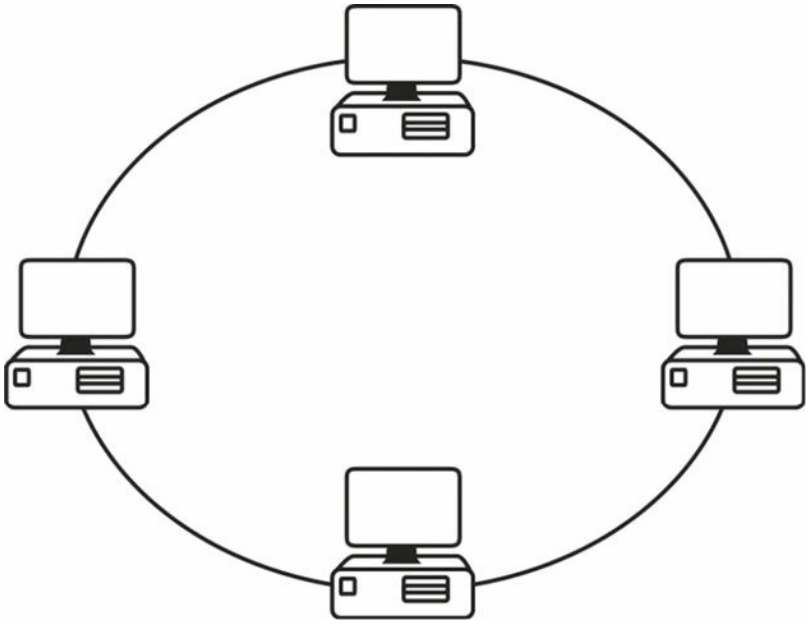


Figure 1.7 – Token Ring Topology

A ring topology that is used with FDDI networks employs a dual-ring connection to provide redundancy should one ring fail.

https://t.me/learningnets

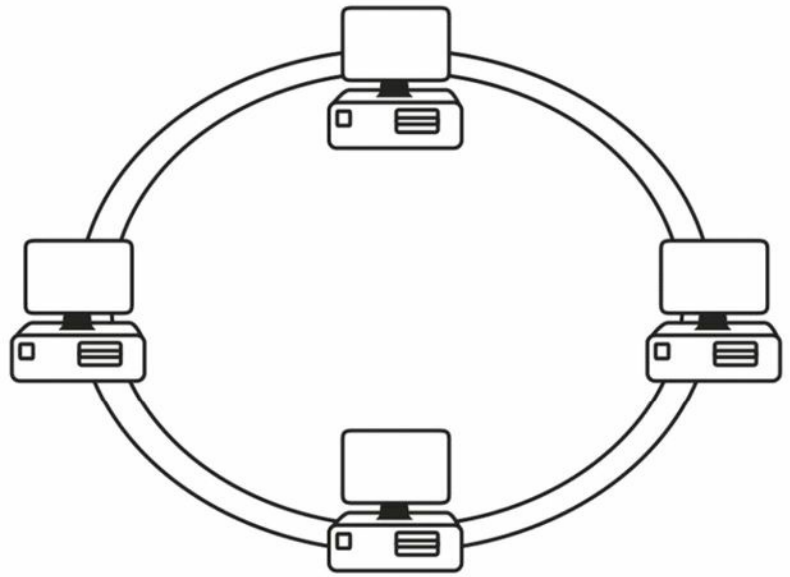


Figure 1.8 – Dual-Ring Topology

Mesh

When downtime is not an option, a mesh topology can be considered. Full-mesh networks provide a connection to each device from every other device. This solution is often used with WAN connections.

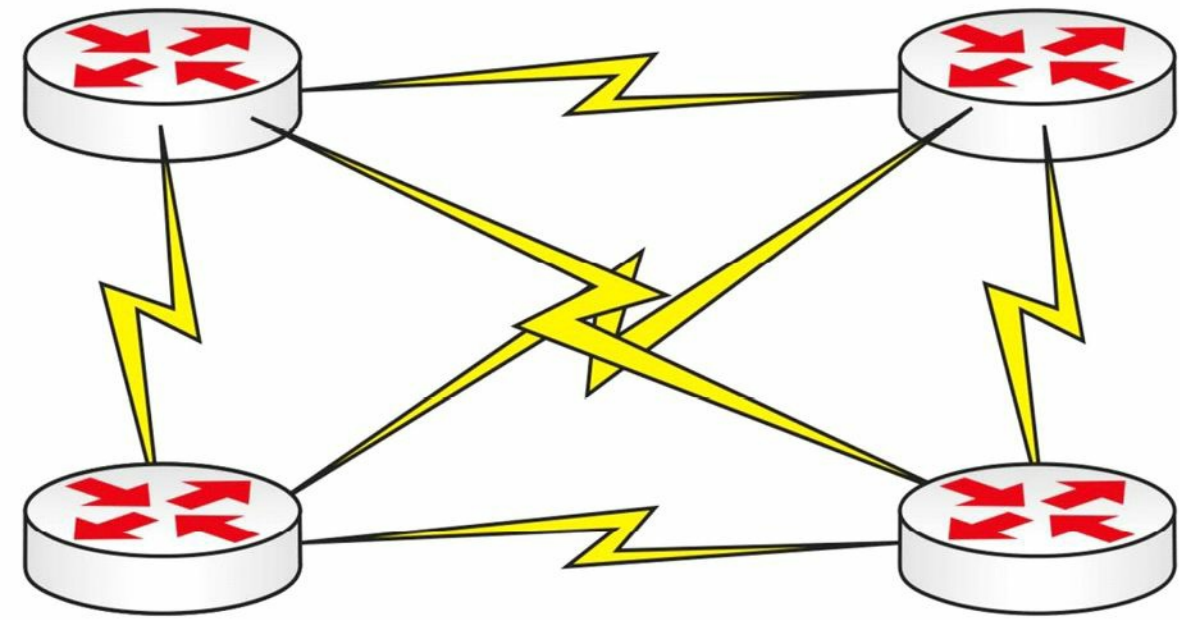


Figure 1.9 – Full-Mesh Topology

Typically, this type of solution will prove very costly. For this reason, partial-mesh topologies can be considered. This means that there may be one or more “hops,” or routers, to get to each device.

https://t.me/learningnets

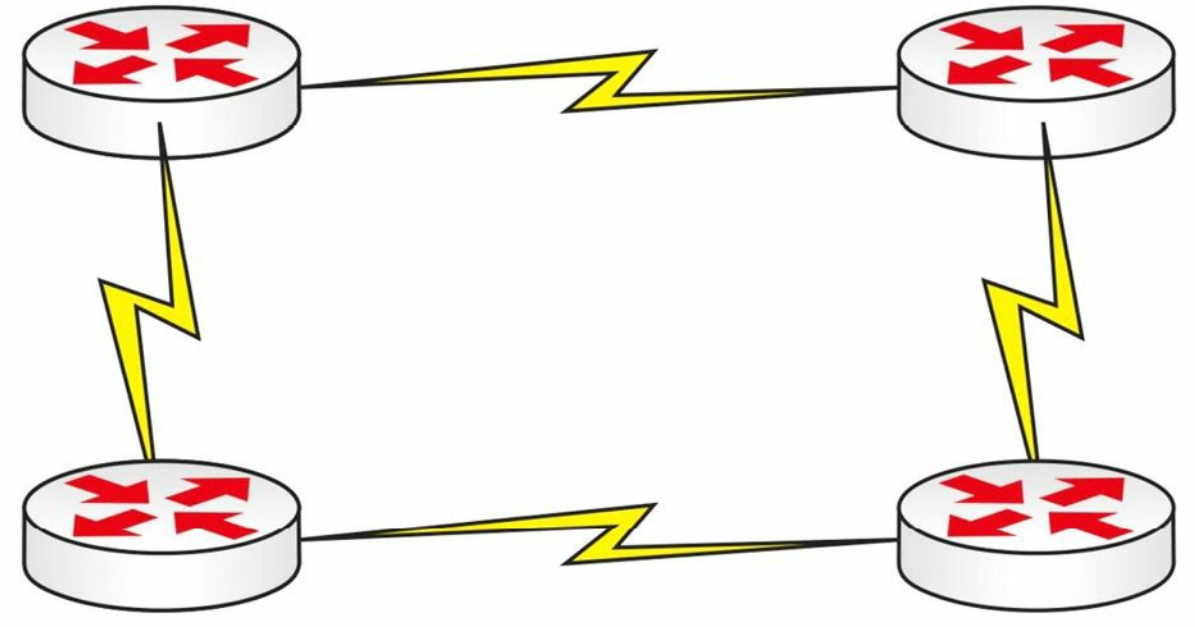


Figure 1.10 – Partial-Mesh Topology

Hub-and-Spoke

Due to the cost of equipment and WAN connections and bandwidth, companies often use a hub-and-spoke design. A powerful router is in the centre (hub), usually at a company's HQ, while the spokes represent remote offices, which require less powerful routers. There are obviously issues with this type of topology; however, it is still widely used. We will revisit hub-and-spoke topologies again in the Frame Relay section, as it still forms a large part of the CCNA syllabus because of the routing issues it creates.

https://t.me/learningnets

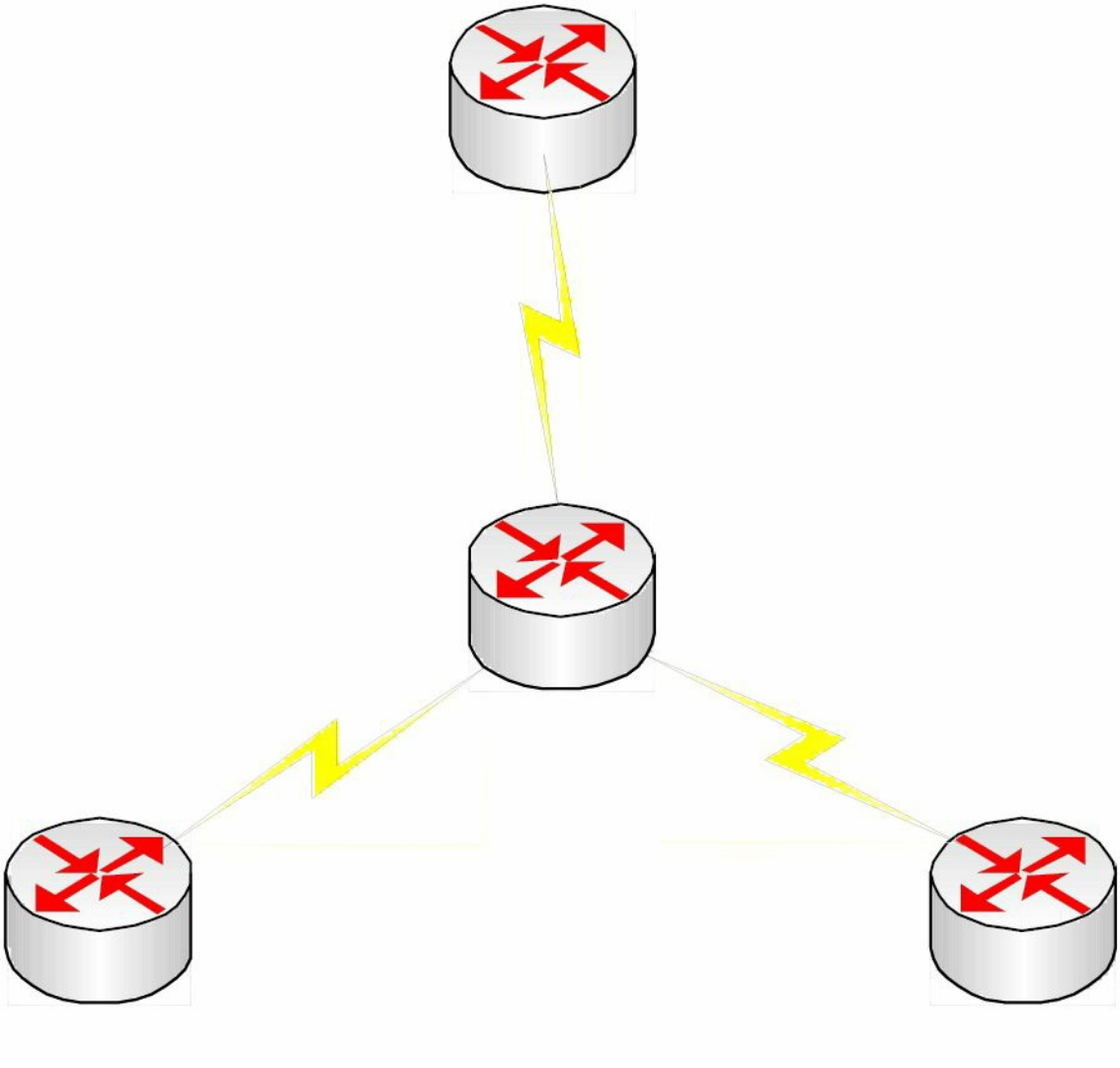


Figure 1.11 – Hub-and-Spoke Topology

Physical versus Logical

When you can see the network equipment, you are looking at the physical topology. This can be misleading because, although the network appears to be wired in a star fashion, it could in fact be working logically as a ring. A classic example of this is a ring network. Although the traffic circulates round the ring in a circular fashion, all of the devices plug into a hub. The ring is actually inside the token ring hub, so you can't see it from the outside, as illustrated in Figure 1.12 below:

https://t.me/learningnets

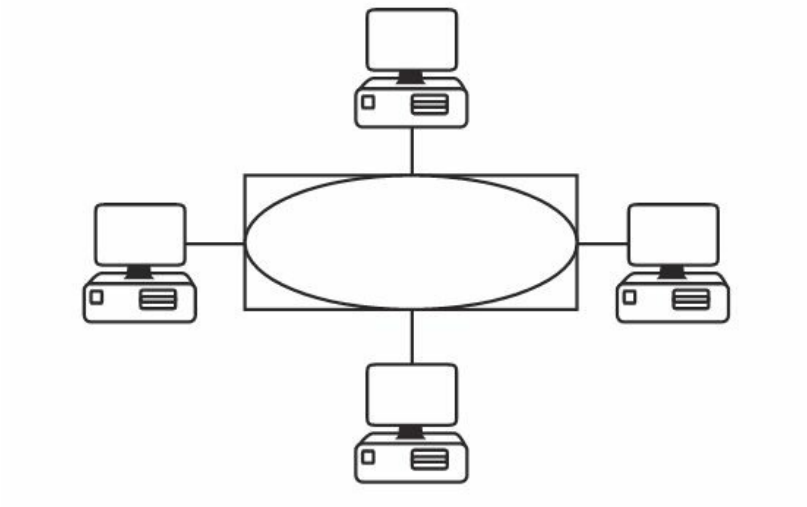


Figure 1.12 – The Ring Is Inside the Hub

You may be asked to identify the different types of networks, both physically and logically. It is a good idea to remember that the physical topology is what you can see and the logical topology is what the network can see (i.e., how the data flows). This is summarised in Table 1.1 below:

Table 1.1 – Physical versus Logical Topologies

Topology	Physical	Logical
Bus	Bus	Bus
Star	Star	Bus
Token Ring	Star	Ring
Point-to-Point	Bus	Bus
FDDI	Ring	Ring

OSI and TCP Models

The OSI Model

Open Standards Interconnection (OSI) was created by the International Organization for Standardization (ISO). With the technology boom came the rise of several giants in the fields of networking devices and software, including Cisco, Microsoft, Novell, IBM, HP, Apple, and others. Each vendor had their own cable types and ports and ran their own communication protocols. This caused major problems if you wanted to buy routers from one company, switches from another, and servers from yet another.

There were workarounds for these problems, such as deploying gateways on the network that could translate between protocols, but such solutions created bottlenecks (i.e., slow portions of the network) and made troubleshooting very difficult and time-consuming. Eventually, vendors had to agree on a common standard which worked for everyone, and the free suite of protocols called Transmission Control Protocol/Internet Protocol (TCP/IP) was ultimately adopted by most. In the end, those vendors who failed to adopt TCP/IP lost market share and

https://t.me/learningnets

went bust.

The ISO created the OSI model to help vendors agree on a set of common standards with which they could all work. This involved dividing network functions into a set of logical levels or layers. Each layer would perform a specific set of functions, so, for example, if your company wanted to focus on network firewalls, they would work with other vendors' equipment.

The advantage was that each device was designed to perform a specific role well, rather than several roles inadequately. Customers could choose the best device for their solution without being tied to one vendor. Troubleshooting became much easier because certain errors could be traced to a certain OSI layer.

The OSI model divides all network functions into seven distinct layers. The layered model starts at Layer 7 and goes all the way down to Layer 1. The more complex functions, which are closer to the user, are at the top, moving down to network cable specifications at the bottom layer, as illustrated in Table 1.2 below:

Table 1.2 – The OSI Model

Layer #	Layer Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

You can easily remember the names of the layers with the mnemonic "**A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing." I would certainly get used to referring to each layer by its number because this is how real-world network technicians use the OSI.

As data is passed down from the top layers to the bottom for transportation across the physical network media, the data is placed into different types of logical data boxes. Although we often call these data boxes "packets," they have different names depending upon the OSI layer. The process of data moving down the OSI model is referred to as encapsulation (see Figure 1.13). Moving back up and having these boxes stripped of their data is called de-encapsulation.

https://t.me/learningnets

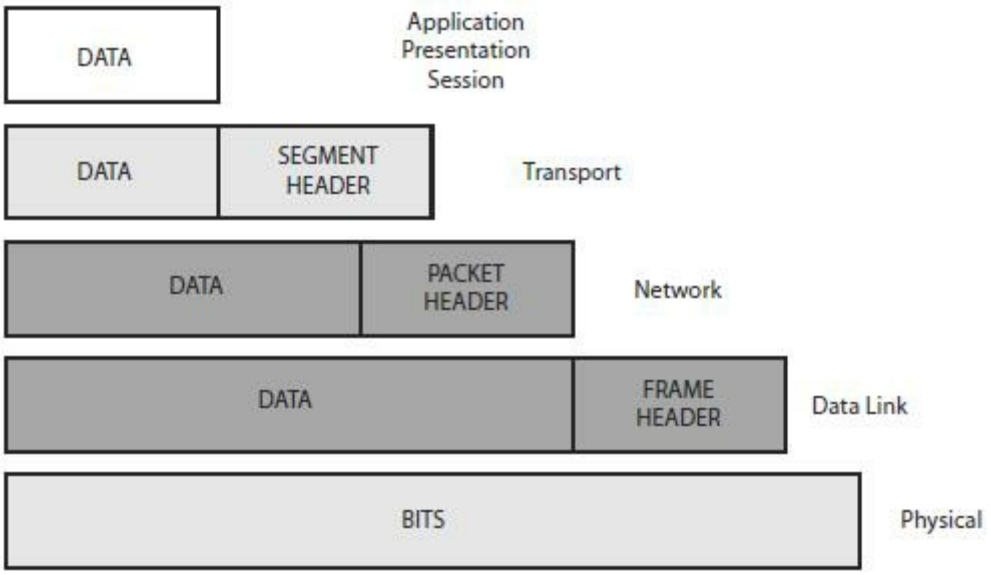


Figure 1.13 – Encapsulation

For the CCNA exam, you will be expected to understand the OSI model and which applications and protocols fit in which layer. You may also have to apply your troubleshooting knowledge using the OSI layered approach. Let's examine each layer of the OSI, starting with Layer 7.

Layer 7 – Application Layer

This layer is the closest layer to the end-user, you and me. The Application Layer isn't the operating system of the devices but usually provides services such as e-mail (SNMP and POP3), web browsing (using HTTP), and file transfer services (using FTP). The Application Layer determines resource availability.

Layer 6 – Presentation Layer

The Presentation Layer presents data to the Application Layer. Multimedia works here, so think MP4, JPEG, GIF, etc. Encryption, decryption, and data compression also take place at this layer.

Layer 5 – Session Layer

The role of the Session Layer is to set up, manage, and terminate sessions or dialogues between devices. These take place over logical links, and what is really happening is the joining of two software applications. SQL, RPC, and NFS all work at the Session Layer.

Layer 4 – Transport Layer

The role of the Transport Layer is to break down the data from the higher layers into smaller parts, which are referred to as segments (at this layer). Virtual circuits are set up here, which are required before devices can communicate.

Before the data can be passed across the network, the Transport Layer needs to establish how much data can be sent to the remote device. This will depend upon the speed and reliability of the link from end to end. If you have a high-speed link but the end-user has a low-speed link, then the data will need to be sent in smaller chunks.

The three methods used to control data flow are as follows:

- Flow control

https://t.me/learningnets

- Windowing
- Acknowledgements

Flow Control

If the receiving system is being sent more information than it can process, it will ask the sending system to stop for a short time. This normally happens when one side uses broadband and the other uses a dial-up modem. The packet sent telling the other device to stop is known as a source quench message.

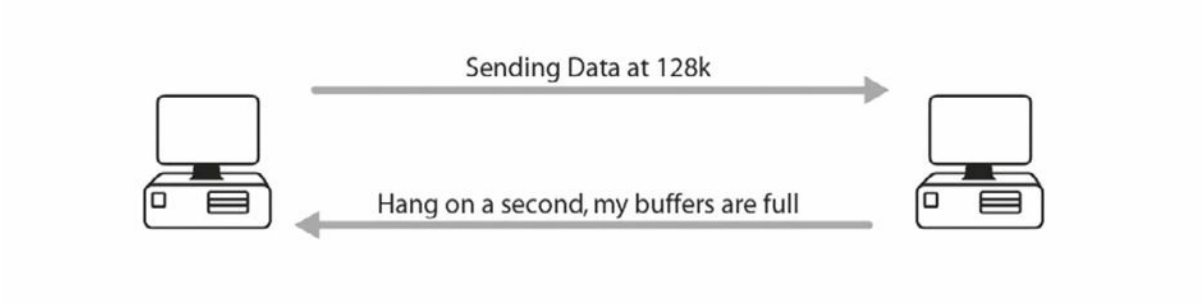


Figure 1.14 – Flow Control

Windowing

With windowing, each system agrees upon how much data is to be sent before an acknowledgment is required. This "window" opens and closes as data moves along in order to maintain a constant flow.

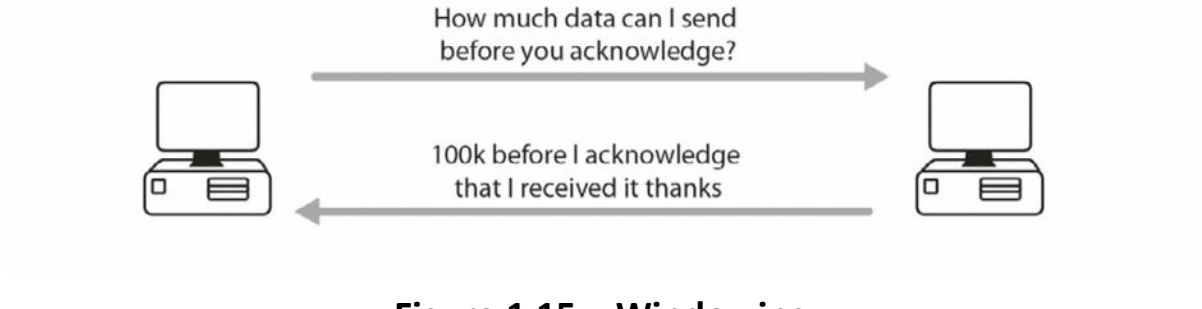


Figure 1.15 – Windowing

Acknowledgements

When a certain amount of segments is received, the fact that they all arrived safely and in the correct order needs to be communicated to the sending system.

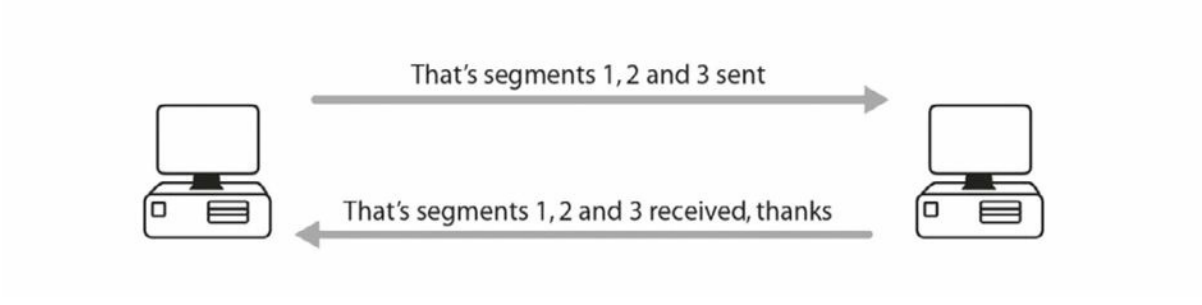


Figure 1.16 – Acknowledgements

All of this is agreed upon during a process known as a three-way handshake (see Figure 1.17). This is where you send a packet to establish the session. This first packet is called a synchronise

https://t.me/learningnets

(SYN) packet. Then the remote device responds with a synchronise acknowledgement (SYN-ACK) packet. The session is established in the third phase when an acknowledgement (ACK) packet is sent. This is all done via the TCP service.

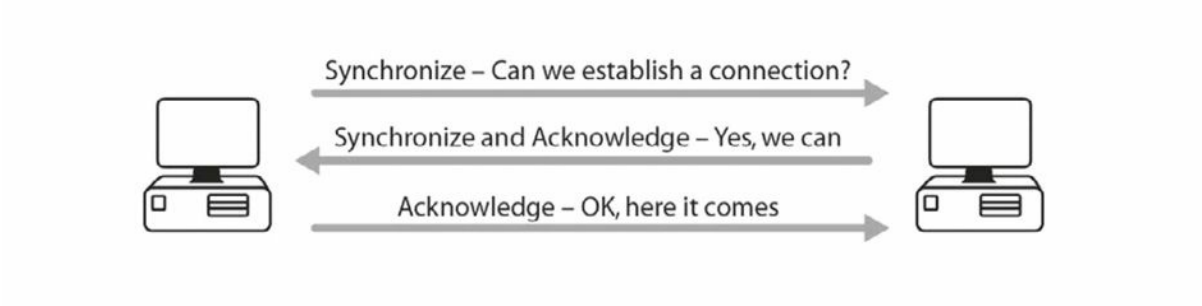


Figure 1.17 – Three-Way Handshake

The Transport Layer includes several protocols, and the most widely known are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), which are part of the TCP/IP suite of protocols. This suite is well known because it is the standard used on the Internet. TCP is known as a reliable connection-oriented protocol. It uses the three-way handshake, windowing, and other techniques to guarantee that the data gets to its destination safely. Many protocols use TCP, including Telnet, HTTPS, and FTP (although it sits at the Application Layer, it does use TCP).

UDP, on the other hand, is known as a connectionless protocol. It numbers each packet and then sends them to their destination. It never checks to see whether they arrived safely and will never set up a connection before sending the packet. Sometimes data is not that important and the application developer decides that the information can always be sent again if it fails to arrive at its destination.

Why is UDP used at all? TCP uses a lot of bandwidth on the network and there is a lot of traffic sent back and forth to set up the connection, even before the data is sent. This all takes up valuable time and network resources. UDP packets are a lot smaller than TCP packets and they are very useful if a really reliable connection is not that necessary. Protocols that use UDP include TFTP.

Layer 3 – Network Layer

The Network Layer takes the segments from the Transport Layer and breaks them down into smaller units called packets. Most network engineers refer to data as packets, no matter what the OSI layer, which is fine; however, just remember that they are technically packets at the Network Layer.

The Network Layer must determine the best path to take from one network to another; for this reason, routers work at this layer. Routers use logical addressing here, and TCP/IP addressing is called IP addressing, which will be covered in detail later.

Layer 2 – Data Link Layer

The Data Link Layer chops down packets into smaller units referred to as frames. Layer 2 switches work at this layer and use hardware or MAC addresses, so they can switch traffic much faster because there is no need to check IP addresses and routing tables. WAN protocols work

at Layer 2, including HDLC, ISDN, and PPP. Ethernet also works at Layer 2.

In order to interface with the upper and lower levels, the Data Link Layer is further subdivided into the Logical Link Control (LLC) Sublayer and the Media Access Control (MAC) Sublayer. The LLC Sublayer interfaces with the Network Layer and the MAC Sublayer interfaces with the Physical Layer.

Layer 1 – Physical Layer

At this layer, frames are converted into bits for placing on the wire. These bits consist of electrical pulses, which are read as “on” and “off” bits, or in binary 1s and 0s, respectively. Hubs work at this layer, and here is where you will find cable specifications, such as RJ45.

OSI Troubleshooting

Using a layered approach can be very effective when you’re troubleshooting your network. The only decision from this point onwards is to determine which way you want to use the OSI stack – top-down, bottom-up, or divide-and-conquer method, which involves focusing on sections of the network in turn.

I recommend using the bottom-up method at the beginning so you don’t waste time looking at applications when the cause can often be found at the lower layers, such as loose or broken cables or incorrect IP addressing. As you gain more experience, using the divide-and-conquer method will probably be faster, depending on the symptoms. If you start at the bottom layer and work your way up, you would do something like this:

Layer 1 – Are all the cables inserted into the ports correctly, or have they come loose? Are the cable ends bent or worn out? If cables are the problem, you will usually see an amber light showing on the device when it should be green. Has somebody forgotten to add the correct speed to the interface? Has the speed of the Ethernet port been set correctly? Has the interface been opened for use by the network administrator?

Layer 2 – Has the correct protocol been applied to the interface so it agrees with the other side, such as Ethernet/PPP/HDLC, etc.?

Layer 3 – Is the interface using the correct IP address and subnet mask?

Layer 4 – Is the correct routing protocol being used, and is the correct network being advertised from the router?

You will see how to apply these steps as you complete the labs in this book. Experts may argue that some Layer 4 issues are at Layer 3, some Layer 2 issues are actually at Layer 1, and so on. I prefer to focus on the fact that we are applying a layered troubleshooting method rather than debating about whether the correct issue is at the correct layer.

The TCP/IP, or DoD, Model

The TCP/IP model is another framework and an alternative to the OSI model. The TCP/IP model is a four or five-layered model created by an association known as DARPA. It is also known as the Department of Defense (DoD) model. The four layers from the top down are as follows:

4 – Application [Telnet/FTP/DNS/RIP]

https://t.me/learningeths

3 – Transport/Host-to-Host [UDP/TCP/ICMP]

2 – Internet or Internetwork [IPSec/IP]

1 – Link/Network Interface [Frame Relay/Ethernet/ATM]

The TCP/IP model has been updated from four to five layers, so you may be asked questions about a five-layered TCP model in the exam. The upper layers are closer to the end-user and the lower layers describe how the technology or protocols interact with other systems. The five-layered TCP model is as follows:

5 – Application [Telnet/FTP/DNS/RIP/HTTP]

4 – Transport/Host-to-Host [UDP/TCP/ICMP]

3 – Network [IPSec/IP]

2 – Data Link [Ethernet/Frame Relay/PPP]

1 – Link/Network Interface/Physical [Bits on the wire]

A five-layered TCP model allows for more granularity and it more accurately represents what actually occurs before data is put onto the wire. For example, at Layer 2 encapsulation of data occurs and addressing takes place (i.e., Data Link addressing). Cisco seem to prefer the five-layered model when it comes to exam questions.

Data is encapsulated as it travels down from the Application Layer to the Physical Layer in exactly the same way as demonstrated in the OSI model, as illustrated in Table 1.3 below:

Table 1.3 – The Five-Layered TCP Model

Application	Data, but not encapsulated yet	
Transport	TCP header added to the data	Segment
Network	IP header added (including IP address)	Packet
Data Link	Data Link header added (Data Link address)	Frame
Physical	Turned into electrical signals	Bits on the wire

You may be asked how the TCP/IP model maps to the OSI model. This is illustrated below in Table 1.4:

Table 1.4 – Mapping the TCP/IP Model to the OSI Model

Layer #	OSI	Data
7	Application	Application
6	Presentation	
5	Session	
4	Transport	Host to Host
3	Network	Internetwork
2	Data Link	Network
1	Physical	Interface

https://t.me/learningnets

Cisco now prefer the (new) TCP model over the OSI model as a network framework, but they still expect you to understand the OSI model and thus have left it in the syllabus for now.

Table 1.5 – Old versus New TCP Model

Old TCP Model	Layer	New TCP Model
Application	5	Application
Transport	4	Transport
Internet	3	Network
Link/Network Interface	2	Data Link
	1	Physical

TCP/IP

TCP/IP is a complete suite of protocols and services which enable communication to take place over networks. Earlier competitors to TCP/IP, such as IPX/SPX, have all but died out due to their lack of adoption and ongoing development.

TCP/IP is a freely available and free to use set of standards maintained by the Internet Engineering Task Force (IETF), and it is used for end-to-end device connectivity. It has been developed and improved upon through submission of Requests for Comments (RFCs), which are documents submitted by engineers to convey new concepts or for peer review. One example is Network Address Translation (NAT) discussed in RFC 2663. IETF adopted some of these RFCs as Internet standards. You can learn more about the IETF and RFCs at the link below:

www.ietf.org/rfc.html

TCP/IP offers many services but many are outside the scope of the CCNA exam and will not be covered. I will also omit those covered in other sections, such as DNS and DHCP. The following sections outline the basics of TCP/IP. Because the CCNA isn't a basic networking exam, it is expected that you already have a good grasp of networking concepts such as those learned in the Network+ exam from CompTIA.

Transmission Control Protocol (TCP)

TCP operates at the Transport Layer of the OSI model. It provides a connection-oriented service for reliable transfer of data between network devices. TCP also provides flow control, sequencing, windowing, and error detection**.** It attaches a 32-bit header to the Application Layer data, which is in turn encapsulated in an IP header. TCP is described in RFC 793. Common TCP ports include the following:

- FTP Data – 20
- FTP Control – 21
- SSH – 22

https://t.me/learningnets

- Telnet – 23
- SMTP – 25
- DNS – 53 (also uses UDP)
- HTTP – 80
- POP3 – 110
- NNTP – 119
- NTP – 123
- TLS/SSL – 443

Internet Protocol (IP)

IP operates at the Network Layer of the OSI model. It is connectionless and is responsible for transporting data over the network. IP addressing is a function of Internet Protocol. IP examines the Network Layer address of every packet and determines the best path for that packet to take to reach its destination. IP is discussed in detail in RFC 791.

User Datagram Protocol (UDP)

UDP also operates at the Transport Layer of the OSI model. It transports information between network devices but, unlike TCP, no connection is established first. UDP is connectionless, gives best-effort delivery, and gives no guarantee that the data will reach its destination. UDP is much like sending a letter with no return address. You know it was sent, but you never know if the letter got there.

UDP consumes less bandwidth than TCP does and is suitable for applications in which low latency is preferred over reliability or guarantees. Both TCP and UDP are carried over IP. UDP is described in RFC 768. Common UDP port numbers include the following:

- DNS – 53
- TFTP – 69
- SNMP – 161/162

File Transfer Protocol (FTP)

FTP operates at the Application Layer and is responsible for reliably transporting data across a remote link. Because it has to be reliable, FTP uses TCP for data transfer.

You can debug FTP traffic with the `debug ip ftp` command.

FTP uses ports 20 and 21. Usually, a first connection is made to the FTP server from the client on port 21. A second data connection is then made either leaving the FTP server on port 20 or from a random port on the client to port 20 on the FTP server. You may wish to read more about active versus passive FTP for your own information, but it is unlikely that this will be covered in CCNA-level exams.

https://t.me/learningnets

Trivial File Transfer Protocol (TFTP)

For less reliable transfer of data, TFTP provides a good alternative. TFTP provides a connectionless transfer by using UDP port 69. TFTP can be difficult to use because you have to specify exactly the directory in which the file is located.

To use TFTP, you need to have a client (the router, in your case) and a TFTP server, which could be a router or a PC, or a server on the network (preferably on the same subnet). You need to have TFTP software on the server so the files can be pulled off it and forwarded on to the client.

> **IN THE REAL WORLD:** Having a server on a network containing backup copies of the startup configuration and IOS is a very good idea indeed.

TFTP is used extensively on Cisco routers to back up configurations and upgrade the router. The following command will carry out these functions:

```
RouterA#copy tftp flash:
```

You will be prompted to enter the IP address of the other host in which the new flash file is located:

```
Address or name of remote host []? 10.10.10.1
```

You will then have to enter the name of the flash image on the other router:

```
Source filename []? / c2500-js-l.121-17.bin
Destination filename [c2500-js-l.121-17.bin]?
```

If you have an older version of IOS, you may be prompted to erase the flash on your router before copying, and then the file will be transferred. When the router reloads, your new flash image should be available for use.

Other optional commands are `copy flash tftp` if you want to store a backup copy or `copy running config tftp` if you want to back up your running configuration file.

You can run a debug on TFTP traffic with the `debug tftp` command.

Simple Mail Transfer Protocol (SMTP)

SMTP defines how e-mails are sent to the e-mail server from the client. It uses TCP to ensure a reliable connection. SMTP e-mails are pulled off the SMTP server in different ways, and SMTP is used as an e-mail delivery service by most networks. POP3 is another popular way to do this. POP3 is a protocol that transfers the e-mail from the server to the client. SMTP uses TCP port 25.

Hyper Text Transfer Protocol (HTTP)

HTTP uses TCP (port 80) to send text, graphics, and other multimedia files from a web server to clients. This protocol allows you to view web pages, and it sits at the Application Layer of the OSI model. HTTPS is a secure version of HTTP that uses Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to encrypt the data before it is sent.

https://t.me/learningnets

You can debug HTTP traffic with the `debug ip http` command.

Telnet

Telnet uses TCP (port 23) to allow a remote connection to network devices. You will learn more about Telnet in the labs. Telnet is not secure so many administrators are now using Secure Shell (SSH), which uses TCP port 22, as an alternative to ensure a secure connection. Telnet is the only utility that can check all seven layers of the OSI model, so if you Telnet to an address, then all seven layers are working properly. If you can't Telnet to another device, it doesn't necessarily indicate a network problem. There could be a firewall or an access control list blocking the connection purposely, or Telnet may not be enabled on the device.

In order to connect remotely to a Cisco router or switch, there must be an authentication method for VTY lines configured on the router. If you are trying to Telnet to another device but cannot connect to it, you can enter Ctrl+Shift+6 and then enter X to quit. To quit an active Telnet session, you can simply type `exit` or `disconnect`.

You can debug Telnet with the `debug telnet` command.

Internet Control Message Protocol (ICMP)

ICMP is a protocol used to report problems or issues with IP packets (or datagrams) on a network. ICMP is a requirement for any vendor who wishes to use IP on their network. When a problem is experienced with an IP packet, the IP packet is destroyed and an ICMP message is generated and sent to the host that originated the packet.

As defined in RFC 792, ICMP delivers messages inside IP packets. The most popular use of ICMP is to send ping packets to test the network connectivity of remote hosts. A ping command issued from a network device generates an echo request packet that is sent to the destination device. Upon receiving the echo request, the destination device generates an echo reply.

Because pings also have a Time to Live (TTL) field, they give a good indication of network latency (delay). The ping output below is from a desktop PC:

```
C:\>ping cisco.com

Pinging cisco.com [198.133.219.25] with 32 bytes of data:

Reply from 198.133.219.25: bytes=32 time=460ms TTL=237
Reply from 198.133.219.25: bytes=32 time=160ms TTL=237
Reply from 198.133.219.25: bytes=32 time=160ms TTL=237
Reply from 198.133.219.25: bytes=32 time=180ms TTL=237

Ping statistics for 198.133.219.25:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 160ms, Maximum = 460ms, Average = 240ms
```

In the output above, the ping packet is 32 bytes long, the Time field reports how many milliseconds the response took, and the TTL is the Time to Live field (i.e., how many milliseconds before the packet expires).

The ping command on a Cisco router has a verbose facility that provides more granularity from which you can specify the source you are pinging, how many pings, and what size you are sending, along with other parameters. This feature is very useful for testing and is used several

https://t.me/learningnets

times in the accompanying lab scenarios, as illustrated in the output below:

```
Router#ping  ← press Enter here
Protocol [ip]:
Target IP address: 172.16.1.5
Repeat count [5]:
Datagram size [100]: 1200
Timeout in seconds [2]:
Extended commands [n]: yes
Source address:  ← you can specify a source address or interface here
Type of service [0]:
Set DF bit in IP header? [no]: yes
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Sending 5, 1000-byte ICMP Echos to 131.108.2.27, timeout is 2 seconds:
U U U U U
Success rate is 0% percent, round-trip min/avg/max = 4/6/12 ms
```

Several notations represent the response the ping packet receives, as follows:

- ! – One exclamation mark per response
- . – One period for each timeout
- U – Destination unreachable message
- N – Network unreachable message
- P – Protocol unreachable message
- Q – Source quench message
- M – Could not fragment
- ? – Unknown packet type

You can terminate a ping session by holding down the Ctrl+Shift+6 keys (all together) and then the X key (on its own).

ICMP packet types are defined in RFC 1700. Learning all the code numbers and names is outside the scope of the CCNA syllabus.

Many junior network engineers misuse the ping facility when it comes to troubleshooting. A failed ping could indicate a network issue or that ICMP traffic is blocked on the network. Because ping attacks are a common way to attack a network, ICMP is often blocked.

Traceroute

Traceroute is a very widely used facility which can test network connectivity and is a handy tool for measurement and management. Traceroute follows the destination IP packets by sending UDP packets with a small maximum TTL field, and then listens for an ICMP time-exceeded response. As the Traceroute packet progresses, the records are displayed hop by hop. Each hop is measured three times. An asterisk [*] indicates that a hop has exceeded its time limit.

Cisco routers use the `traceroute` command, whereas Windows PCs use `tracert`, as illustrated in

https://t.me/learningnets

the output below:

```
C:\Documents and Settings\pc>tracert hello.com

Tracing route to hello.com [63.146.123.17]
over a maximum of 30 hops:

1 81 ms 70 ms 80 ms imsnet-cl10-hg2-berks.ba.net [213.140.212.45]
2 70 ms 80 ms 70 ms 192.168.254.61
3 70 ms 70 ms 80 ms 172.16.93.29
4 60 ms 81 ms 70 ms 213.120.62.177
5 70 ms 70 ms 80 ms core1-pos4-2.berks.ukore.ba.net [65.6.197.133]
6 70 ms 80 ms 80 ms core1-pos13-0.ealng.core.ba.net [65.6.196.245]
7 70 ms 70 ms 80 ms transit2-pos3-0.eang.ore.ba.net [194.72.17.82]
8 70 ms 80 ms 70 ms t2c2-p8-0.uk-eal.eu.ba.net [165.49.168.33]
9 151 ms 150 ms 150 ms t2c2-p5-0.us-ash.ba.net [165.49.164.22]
10 151 ms 150 ms 150 ms dcp-brdr-01.inet.qwest.net [205.171.1.37]
11 140 ms 140 ms 150 ms 205.171.251.25
12 150 ms 160 ms 150 ms dca-core-02.inet.qwest.net [205.171.8.221]
13 190 ms 191 ms 190 ms atl-core-02.inet.qwest.net [205.171.8.153]
14 191 ms 180 ms 200 ms atl-core-01.inet.net [205.171.21.149]
15 220 ms 230 ms 231 ms iah-core-03.inet.net [205.171.8.145]
16 210 ms 211 ms 210 ms iah-core-02.inet.net [205.171.31.41]
17 261 ms 250 ms 261 ms bur-core-01.inet.net [205.171.205.25]
18 230 ms 231 ms 230 ms bur-core-02.inet.net [205.171.13.2]
19 211 ms 220 ms 220 ms buc-cntr-01.inet.net [205.171.13.158]
20 220 ms 221 ms 220 ms msfc-24.buc.qwest.net [66.77.125.66]
21 221 ms 230 ms 220 ms www.hello.com [63.146.123.17]

Trace complete.
```

The fields in the Traceroute output are as follows:

- ... – Timeout
- U – Port unreachable message
- H – Host unreachable message
- P – Protocol unreachable message
- N – Network unreachable message
- ? – Unknown packet type
- Q – Source quench received

Traceroute is a very useful command when you want to troubleshoot network connectivity issues. Although it is outside the scope of the CCNA syllabus, here is a more detailed explanation of how it operates.

Traceroute works by sequentially incrementing the TTL field of UDP packets (only used in Cisco and Linux; Microsoft Windows `tracert` command uses ICMP echo request datagrams instead of UDP datagrams as probes) destined for a host and recording the replies received from intermediate routers.

Every packet has a TTL value associated with it and each time the packet reaches a hop, its TTL value is decreased by 1. The first packet is sent to the destination with TTL=1, which reaches

https://t.me/learningnets

Router 1, but because its TTL value has dropped to 0, the router sends an error message (TTL exceeded in transit). Then a second packet is sent with TTL=2. This reaches Router 2, which also sends the same error message that Router 1 sent. This is continued until the destination is reached.

All hops, except for the last one, should return a "TTL exceeded in transit" message, whereas the last hop should return a "destination unreachable/port unreachable" message, indicating that it cannot handle the received traffic (UDP Traceroute packets are typically addressed to a pseudorandom high port on which the end host is not likely to be listening).

Address Resolution Protocol (ARP)

Two types of addressing are used to identify network hosts – the IP (or Layer 3) address and the local (or Data Link Layer) address. The Data Link Layer address is also commonly referred to as the MAC address. Address resolution, as defined in RFC 826, is the process in which the IOS determines the Data Link Layer address from the Network Layer (or IP) address.

ARP resolves a known IP address to a MAC address. When a host needs to transfer data across the network, it needs to know the other host's MAC address. The host checks its ARP cache and if the MAC address is not there, it sends out an ARP Broadcast message to find the host, as illustrated in Figure 1.18 below:

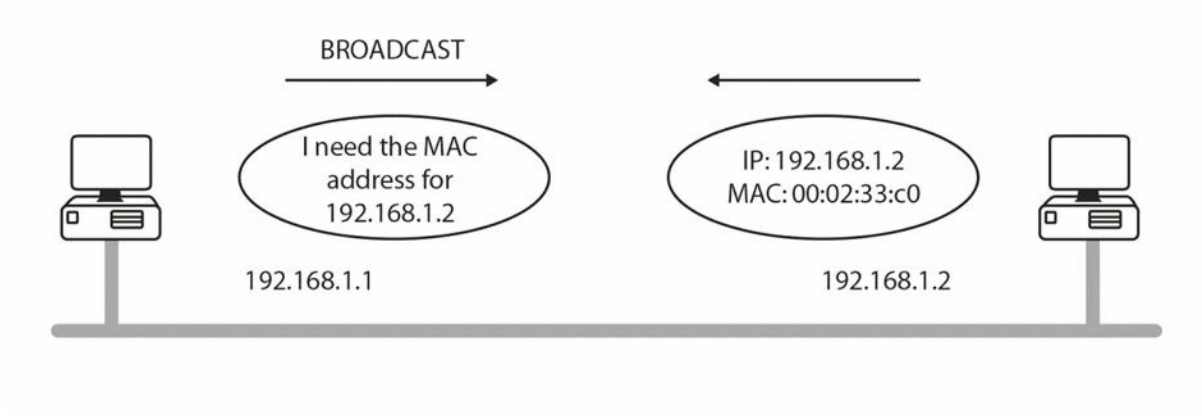


Figure 1.18 – One Host Broadcasts for Another Host's MAC Address

You can debug ARP with the `debug arp` command.

An ARP entry is required for communication across the network. You can see that a Broadcast has taken place if there is no ARP entry. It is also important to understand that ARP tables on routers and switches are flushed after a certain amount of time (four hours by default) to conserve resources and prevent inaccurate entries.

On the router below, it has an ARP entry only for its own FastEthernet interface until its neighbour is pinged, so the first of five ping (ICMP) packets fails, as shown by the period followed by four exclamation marks:

```
Router#show arp
Protocol  Address  Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1     -   0002.4A4C.6801  ARPA   FastEthernet0/0
Router#ping 192.168.1.2
Type escape sequence to abort.
```

https://t.me/learningnets

```
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.!!!! ← first packet fails due to ARP request
Success rate is 80 percent(4/5),round-trip min/avg/max = 31/31/31 ms
Router#show arp
Protocol  Address  Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1         0002.4A4C.6801  ARPA   FastEthernet0/0
Internet  192.168.1.2     0   0001.97BC.1601  ARPA   FastEthernet0/0
Router#
```

Proxy ARP

Proxy ARP (see Figure 1.19 below) is defined in RFC 1027. Proxy ARP enables hosts on an Ethernet network to communicate with hosts on other subnets or networks, even though they have no knowledge of routing.

If an ARP Broadcast reaches a router, it will not forward it (by default). Routers do not forward Broadcasts, but if they do know how to find the host (i.e., they have a route to it), they will send their own MAC address to the host. This process is called proxy ARP and it allows the host to send the data thinking it is going straight to the remote host. The router swaps the MAC address and then forwards the packet to the correct next hop.

The `ip proxy-arp` command is enabled on Cisco routers by default.

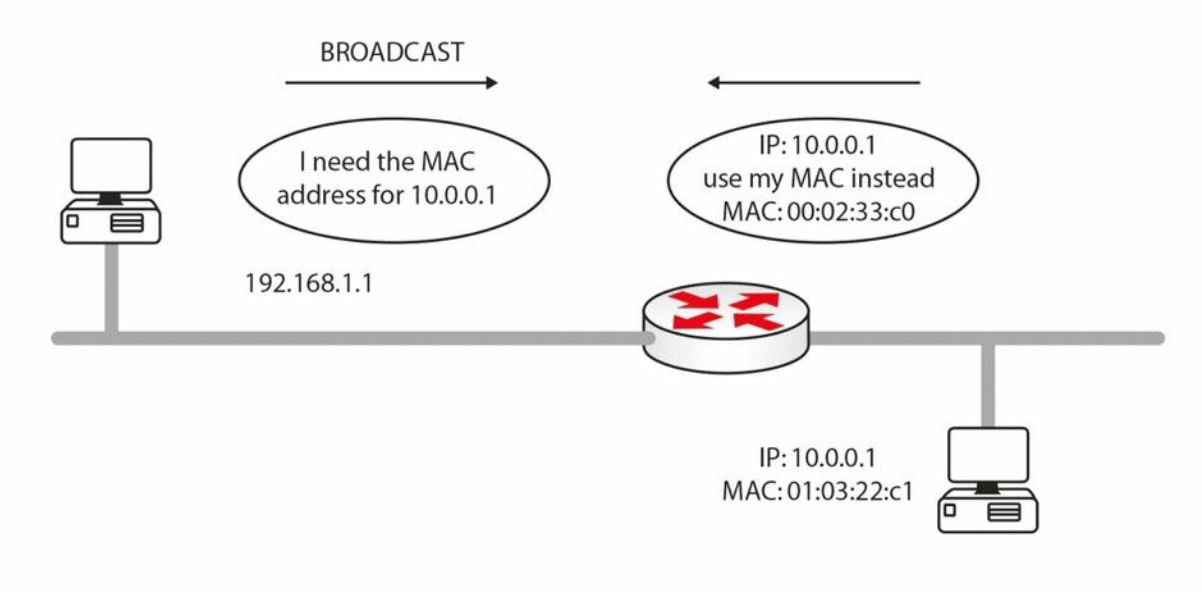


Figure 1.19 – Router Uses Proxy ARP to Allow the Hosts to Connect

Expanding upon the previous point, part of the exam requirements is understanding how addressing changes as packets traverse the network. As the packet traverses the network, there must be a way for each end device to communicate, but also a way for intermediary devices to be able to exchange the next-hop address for the packet to traverse. Proxy ARP provides the answer again. The source and destination IP address never change but in order for the packet to be passed to a next-hop address, the MAC address (in the frame) changes between devices.

In Figure 1.20 below, the frame will leave HOST A with the source IP address 192.168.1.1, the destination IP address 172.16.1.2, the source MAC address AAAA:AAAA:AAAA, and the

https://t.me/learningnets

destination MAC address AAAA: AAAA:BBBB. R1 will retain the IP addresses but change the source address to AAAA:AAAA:CCCC. By the time the packet leaves R2 for HOST B, the IP addresses will not have changed but the source MAC address is now AAAA:AAAA:DDDD and the destination MAC address is AAAA:AAAA:EEEE.

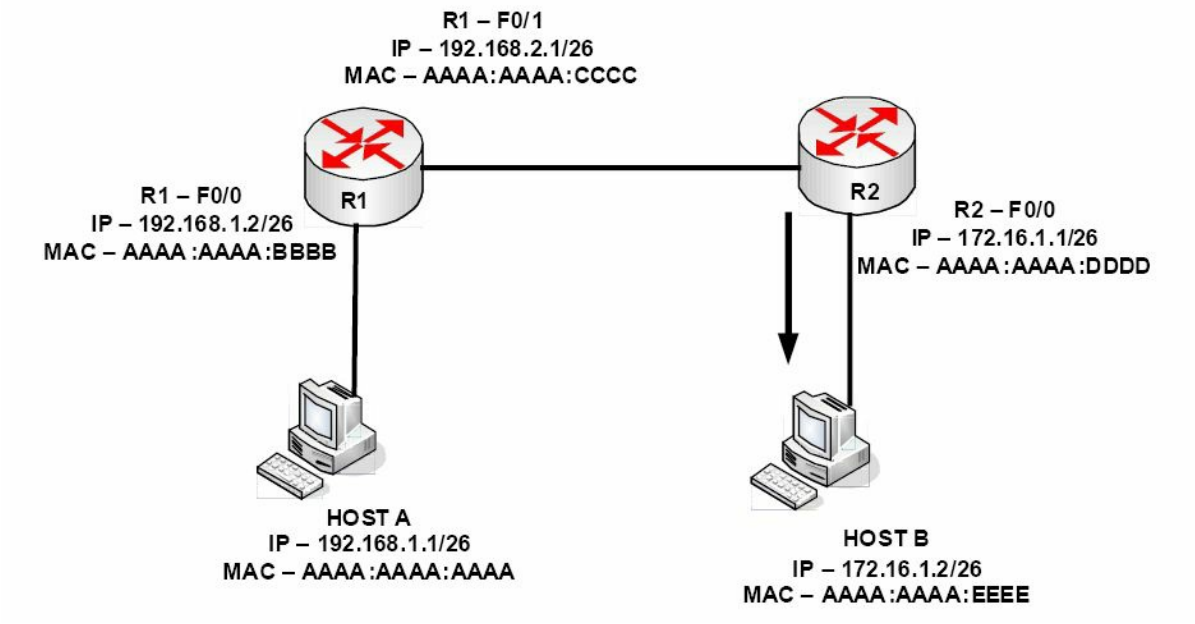


Figure 1.20 – MAC Address Changes as the Packet Traverses Network Devices

Reverse Address Resolution Protocol (RARP)

RARP maps a known MAC address to an IP address. Hosts such as diskless workstations (also known as thin clients) know their MAC address when they boot. They use RARP to discover their IP address from a server on the network.

Gratuitous Address Resolution Protocol (GARP)

GARP is a special ARP packet. A normal host will always send out a GARP request after the link goes up or the interface is enabled. Gratuitous in this case means a request/reply that is not normally needed according to the ARP RFC specification but could be used in some cases. A gratuitous ARP request is an ARP request packet where the source MAC, the source IP, and the destination IP addresses are all set to the IP address of the machine issuing the packet, and the destination MAC is the Broadcast address FFFF: FFFF: FFFF. Ordinarily, no reply packet will occur.

A GARP reply is one to which no request has been made (if you see a GARP reply, that means another computer on the network has the same IP address as you have). GARP is used when a change of state happens in FHRP protocols (e.g., HSRP; this will be covered later), with the objective of updating the Layer2 CAM table. We will discuss GARP again in the IPv6 section.

Simple Network Management Protocol (SNMP)

SNMP is used for network management services. An SNMP management system allows network devices to send messages called traps to a management station. This informs the network administrator of any faults on the network (such as faulty interfaces), high CPU utilisation on servers, etc.

https://t.me/learningnets

You can debug SNMP traffic with the `debug snmp` command. SNMP uses UDP ports 161 and 162.

Hyper Text Transfer Protocol Secure (HTTPS)

TLS, and the older protocol SSL, is used for secure communication over the Internet, which is carried out by means of cryptography. You will also find these used for e-mail and Voice over IP (VoIP), and when surfing sites which begin with the URL https://. HTTP with TLS/SSL (HTTPS) uses port 443.

IP Configuration Command

This is not actually a Cisco tool but it's part of your troubleshooting toolkit. The `ipconfig` command used at a Windows command prompt allows you to use several switches, but perhaps the most commonly used command is `ipconfig /all`, as shown in the screenshot below:

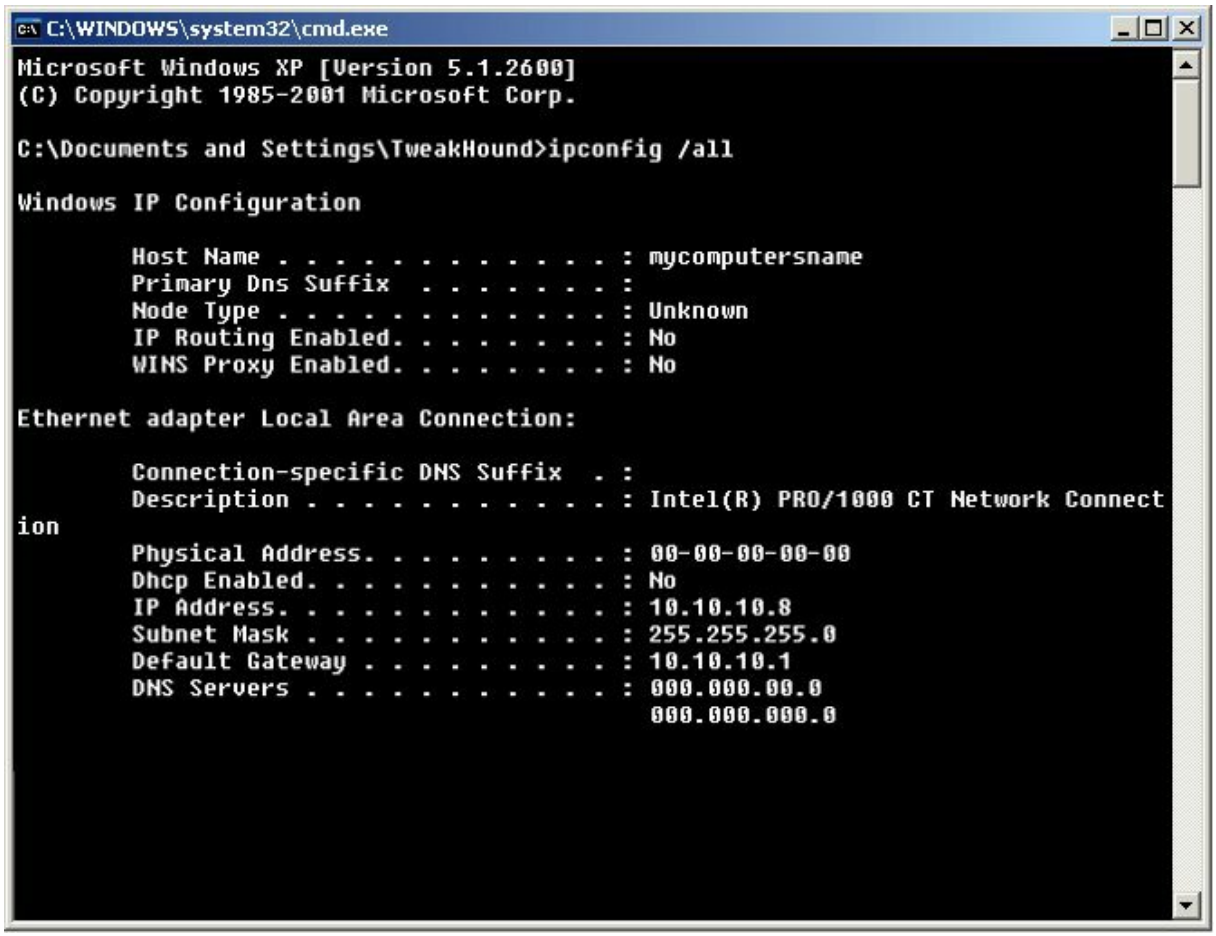


Figure 1.21 – The `ipconfig /all` Command Output

Other switches you can use with the `ipconfig` command are as follows:

```
/?          Display this help message
/all        Display full configuration information
/release    Release the IP address for the specified adapter
/renew      Renew the IP address for the specified adapter
/flushdns   Purges the DNS Resolver cache
/registerdns Refreshes all DHCP leases and re-registers DNS names
```

Cables and Media

Cabling and cable-related issues will become part of your day-to-day routine as a network

https://t.me/learningnets

engineer. You will need to know which cables plug into which devices, the industry limitations, and how to configure equipment for use with the correct cable type.

LAN Cables

Ethernet Cables

Most cable-related network problems will occur on the Local Area Network (LAN) side rather than on the Wide Area Network (WAN) side due to the sheer volume of cables and connectors, and the higher frequency of reseating (unplugging and plugging in) the cables for device moves and testing.

Ethernet cables are used to connect workstations to the switch, switch-to-switch, and switch-to-router. The specifications and speeds have been revised and improved many times in recent years, which means you can soon expect today's standard speeds to be left behind for new and improved high-speed links right to your desktop. The current standard Ethernet cable still uses eight wires twisted into pairs to prevent electromagnetic interference (EMI), as well as crosstalk, which is a signal from one wire spilling over into a neighbouring cable.

Cable categories, as defined by ANSI/TIA/EIA-568-A, include Categories 3, 5, 5e, and 6. Each one gives standards, specifications, and achievable data throughput rates, which can be achieved if you comply with distance limitations. Category 3 cabling can carry data up to 10Mbps. Category 5 cabling is primarily used for faster Ethernet networks, such as 100BASE-TX and 1000BASE-T. Category 5e cabling uses 100-MHz-enhanced pairs of wires for running GigabitEthernet (1000Base-T). Finally, with Category 6 cabling, each pair runs 250 MHz for improved 1000Base-T performance. ("1000" refers to the speed of data in Mbps, "Base" stands for baseband, and "T" stands for twisted pair.) Table 1.6 below demonstrates some common Ethernet standards you should be familiar with:

Table 1.6. Common Ethernet Standards

Speed	Name	IEEE Name	IEEE Standard	Cable/Length
10Mbps	Ethernet	10BASE-T	802.3	Copper/100 m
100Mbps	FastEthernet	100BASE-T	802.3u	Copper/100 m
1000Mbps	GigabitEthernet	1000BASE-LX	802.3z	Fibre/5000 m
1000Mbps	GigabitEthernet	1000BASE-T	802.3ab	Copper/100 m
10Gbps	TenGigabitEthernet	10GBASE-T	802.3an	Copper/100 m

Cisco like to sneak cable specification questions into the exam from time to time, so make sure you memorise the table above.

Duplex

When Ethernet networking was first used, data was able to pass on the wire in only one direction at a time. This is because of the limitations of the cables used at that time. The sending device had to wait until the wire was clear before sending data on it, without a guarantee that there wouldn't be a collision. This is no longer an issue because a different set

https://t.me/learningnets

of wires is used for sending and receiving signals.

Half duplex means that data can pass in only one direction at a time, while full duplex means that data can pass in both directions on the wire at the same time (see Figure 1.22). This is achieved by using spare wires inside the Ethernet cable. All devices now run at full duplex unless configured otherwise.

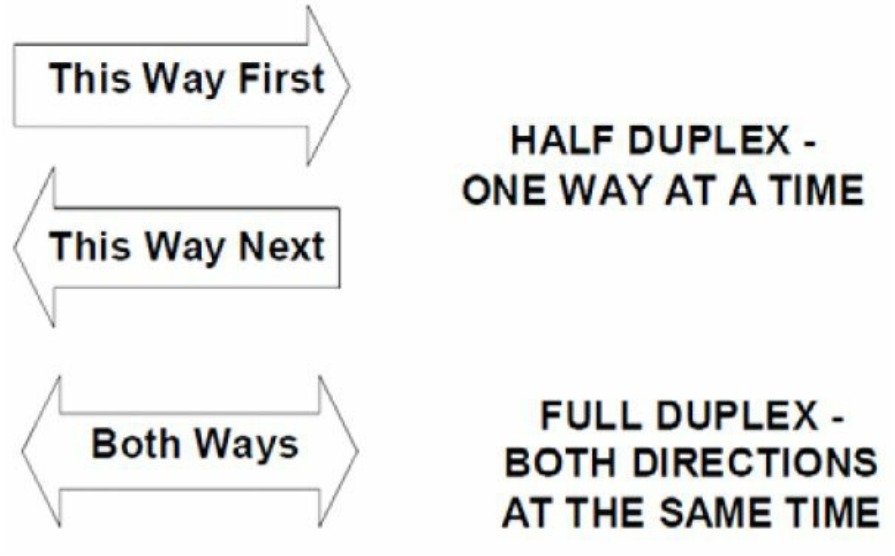


Figure 1.22 – Duplex Topology

You will still be expected to understand and troubleshoot duplex issues in the exam; we will cover troubleshooting Layer 1 and Layer 2 issues later in this guide. You can easily check an interface's duplex settings with the `show interface X` command.

```
Switch#show interface FastEthernet0/1
FastEthernet0/1 is down, line protocol is down (disabled)
  Hardware is Lance, address is 0030.a388.8401 (bia 0030.a388.8401)
BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, Loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
```

If this interface was connected to a full-duplex device, you would see interface errors immediately and experience slow traffic on the link. You can also issue the `show interfaces status` command on a live switch, although this command may not work in the exam because a router simulator has limited commands (same for Packet Tracer). You can see possible issues with interface Fast Ethernet 1/0/2 below:

```
Switch#show interfaces status
Port Name          Status       Vlan       Duplex  Speed  Type
Fa1/0/1            notconnect   1          auto    auto   10/100BaseTX
Fa1/0/2            notconnect   1          half      10   10/100BaseTX
Fa1/0/3            notconnect   1          auto    auto   10/100BaseTX
Fa1/0/4            notconnect   1          auto    auto   10/100BaseTX
Fa1/0/5            notconnect   1          auto    auto   10/100BaseTX
```

https://t.me/learningnets

And of course you can fix this issue easily, as shown below:

```
Switch(config)#int f1/0/2
Switch(config-if)#duplex ?
  auto  Enable AUTO duplex configuration
  full  Force full duplex operation
  half  Force half-duplex operation
Switch(config-if)#duplex full
```

Please do try this and all the other commands on live Cisco equipment, GNS3, or at least Packet Tracer in order to remember them! We will cover the speed setting next.

Speed

You can leave the speed of the Ethernet port on your routers or switches as auto-negotiate, or you can hard set them to 10Mbps, 100Mbps, or 1000Mbps.

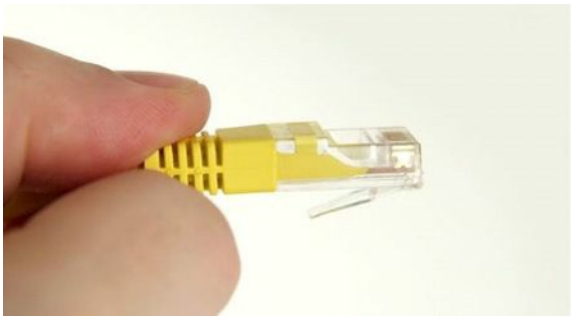
To set the speed manually, you would configure the router as follows:

```
Router#config t
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  1000  Force 1000 Mbps operation
  auto  Enable AUTO speed configuration
```

The following commands would allow you to view the router Ethernet interface settings:

```
Router#show interface FastEthernet0
FastEthernet0 is up, line protocol is up
  Hardware is DEC21140AD, address is 00e0.1e3e.c179 (bia 00e0.1e3e.c179)
  Internet address is 1.17.30.4/16
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, Loopback not set, keepalive set (10 sec)
  Half-duplex, 10Mb/s, 100BaseTX/FX
```

Specifications for Ethernet cables by EIA/TIA dictate that the end of the cable presentation should be RJ45 male (see Figure 1.23; Figure 1.24 shows the female end), which will allow you to insert the cable into the Ethernet port on your router/switch/PC.



https://t.me/learningnets

Figure 1.23 – RJ45 Male End



Figure 1.24 – RJ45 Female End

Straight Cables

Each Ethernet cable contains eight wires and each wire connects to a pin at the end. The position of these wires when they meet the pin determines what the cable can be used for. If each pin on one end matches the other side, then this is known as a straight-through cable. These cables can be used to connect an end device to an Ethernet port on a switch, and a switch to a router. You can easily check whether the wires match by comparing one side of the cable to the other, as shown in Figures 1.25 and 1.26 below:



Figure 1.25 – Comparing Cable Ends

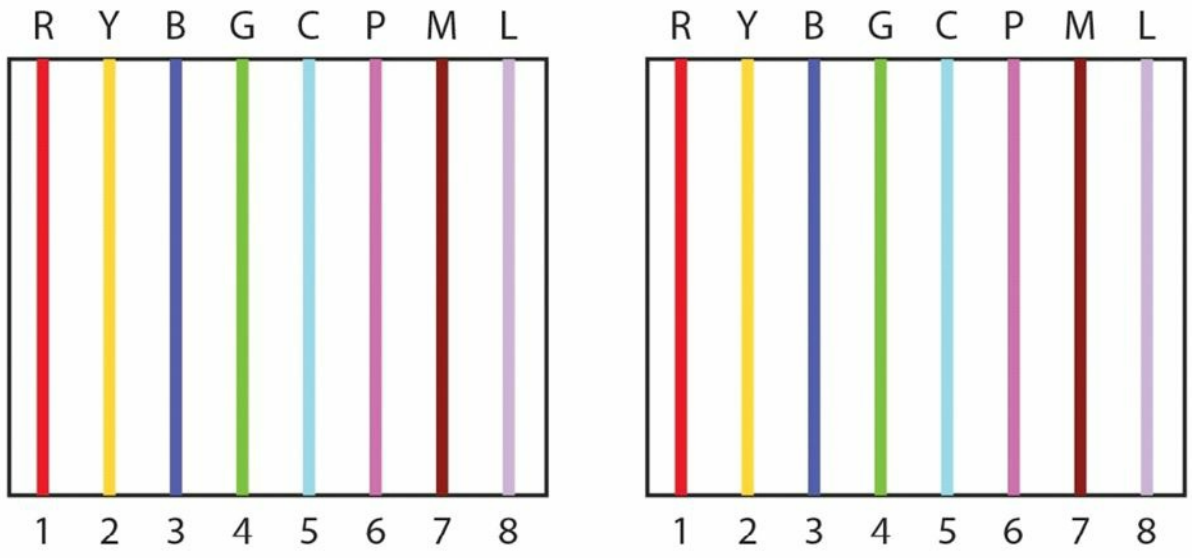


Figure 1.26 – Cable Ends Match

Crossover Cables

https://t.me/learningnets

By swapping two of the wires on the cable, it can now be used to connect a PC to a PC (without the use of a switch or a hub, although Auto-MDIX ports on newer network interfaces detect whether the connection requires a crossover, and automatically chooses the MDI or MDIX configuration to properly match the other end of the link) or a switch to a switch. The wire on pin 1 on one end needs to connect to pin 3 on the other end, and pin 2 needs to connect to pin 6 on the other end (see Figure 1.27). I have created my own colour scheme for the cables purely to illustrate my point – red, yellow, blue, green, cyan, pink, magenta, and lilac.

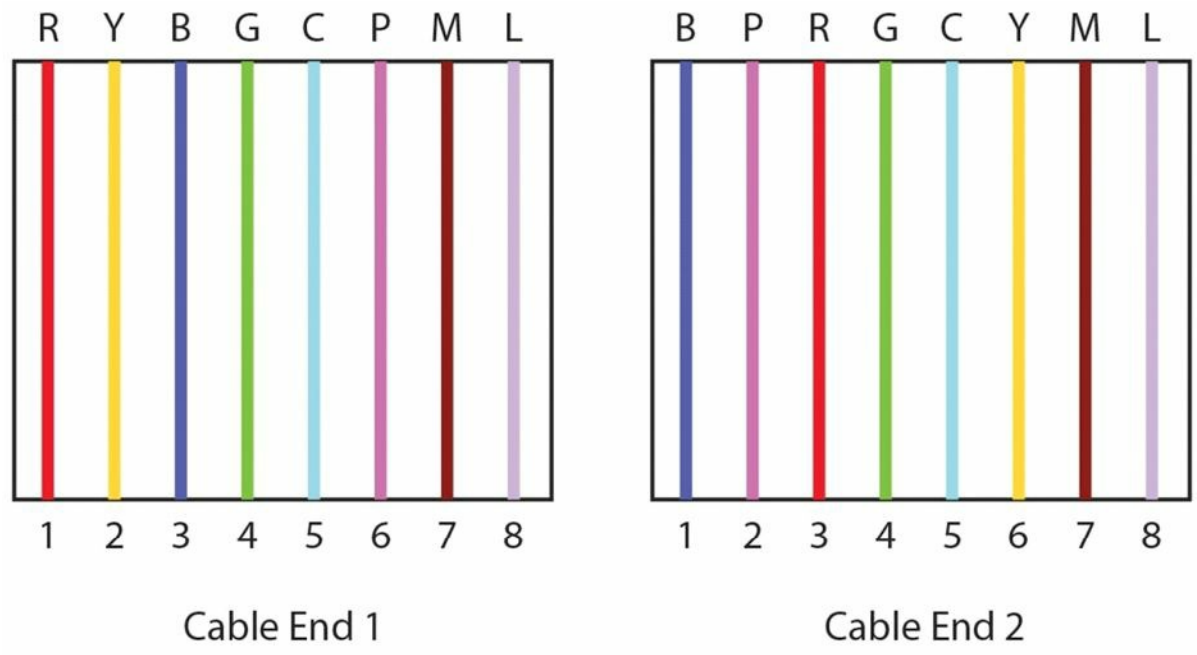


Figure 1.27 – Pin 1 to Pin 3 and Pin 2 to Pin 6

Rollover/Console Cables

All Cisco routers and switches have physical ports to connect to for initial set up and disaster recovery or access. These ports are referred to as console ports and you will regularly use these as a Cisco engineer. In order to connect to this port, you need a special type of cable called a rollover or console cable (see Figure 1.28). It can sometimes be referred to as a flat cable because, as opposed to most round-bodied Ethernet cables, it is often flat along its body.

A rollover cable swaps all pins (see Figure 1.29), so pin 1 on one end goes to pin 8 on the other end, pin 2 goes to pin 7, and so on.



Figure 1.28 – A Typical Rollover Cable

https://t.me/learningnets

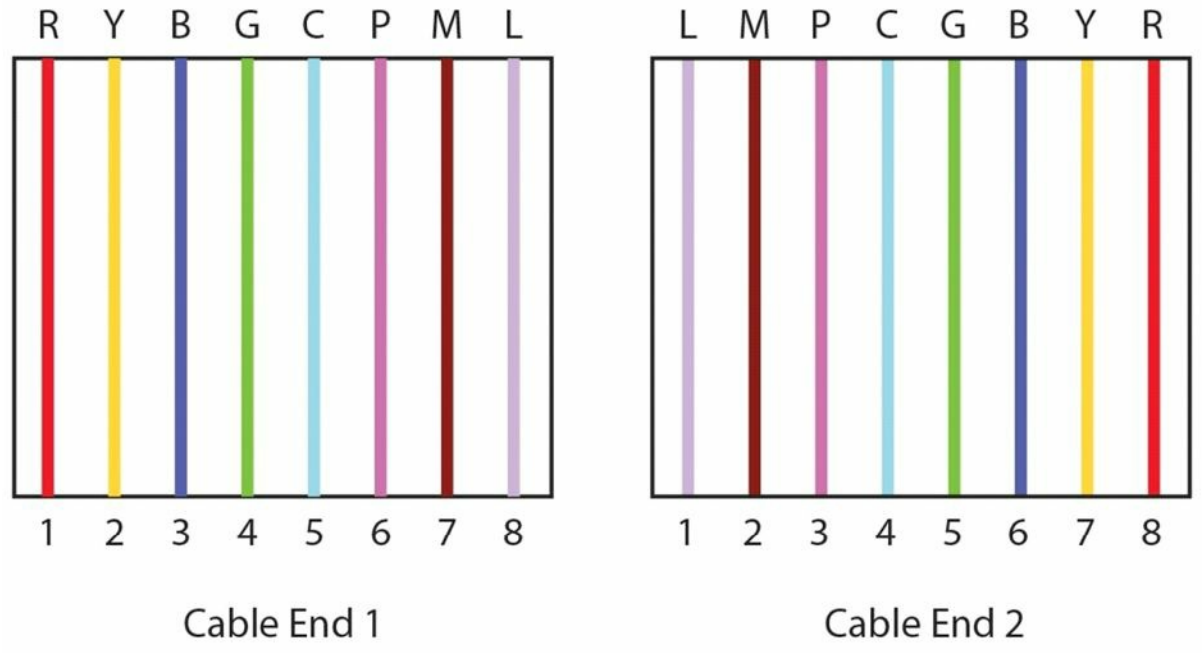


Figure 1.29 – All Pins Swapped

Rollover cables usually have an RJ45 connection on one end and a 9-pin D-shaped connection on the other end, which is designed to connect to the COM port on a PC or laptop. The trouble is that devices no longer come with these ports, as they were so rarely used. You can now buy a DB9-to-USB converter cable (see Figure 1.30) from many electrical stores or online. They come with software drivers which allow you to connect a logical COM port on your PC via a terminal programme, such as PuTTY or HyperTerminal.

Cisco have started to put mini-USB ports (in addition to RJ45 ports) on their devices to allow for console port connectivity using the USB Type A to 5-pin mini-Type B cable. If both console cables are plugged in at the same time, the mini-USB cable takes precedence and becomes active. Figures 1.31 and 1.32 below show the different connection types.

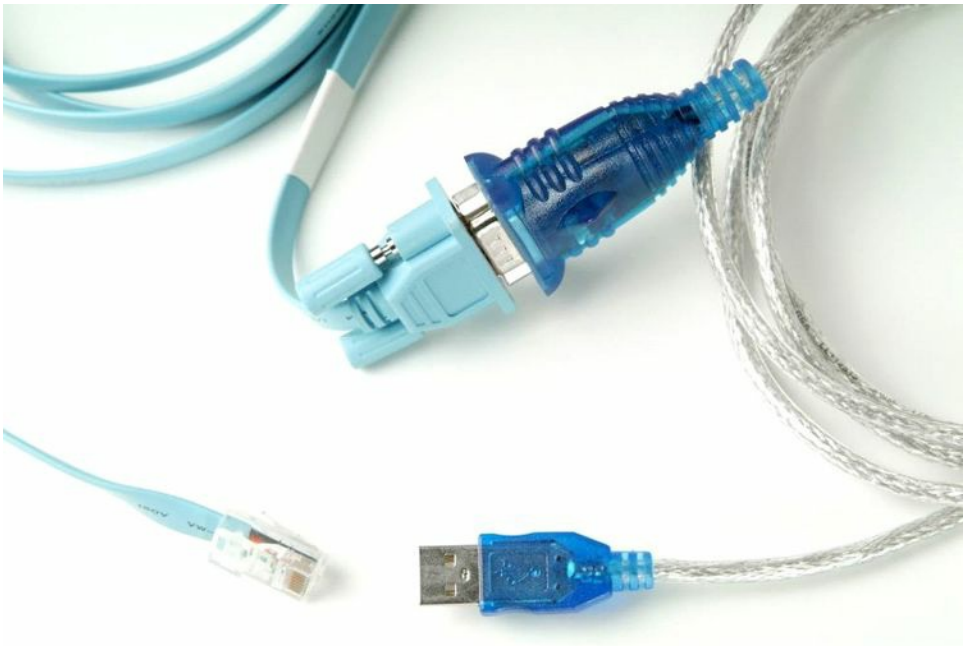


Figure 1.30 – A COM-to-USB Converter Cable

https://t.me/learningnets

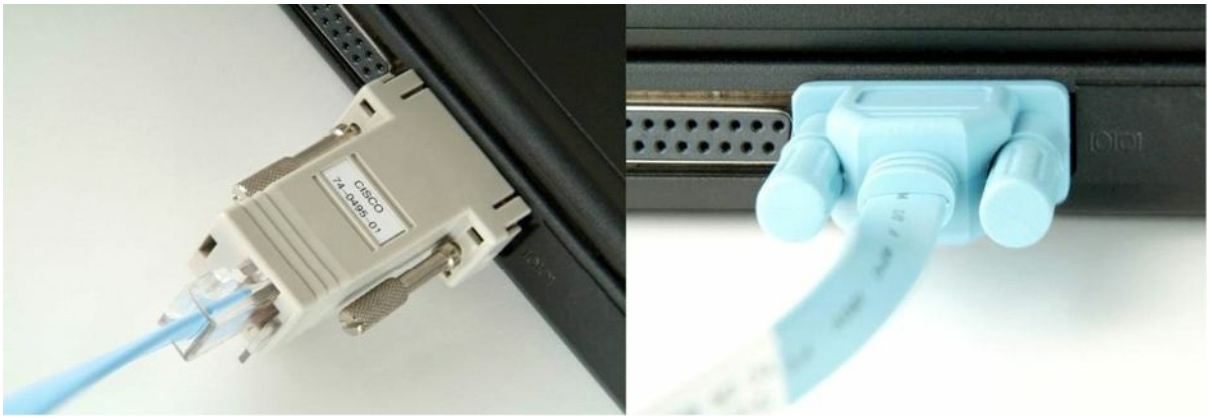


Figure 1.31 – Connecting the Cable to the COM Port

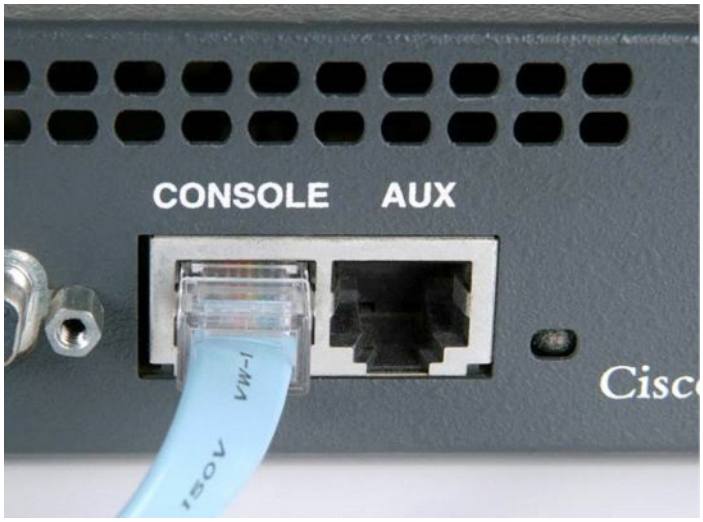


Figure 1.32 – Connecting the Cable to the Router or Switch Console Port

WAN Cables

Used for Wide Area Network connections, serial cables can come in several shapes, sizes, and specifications, depending upon the interface on the router and connection type. ISDN uses different cables than Frame Relay or ADSL do, for example.

One common type of WAN cable you will use, especially if you have a home network to practise on, is a DB60 (see Figure 1.33). For this type of cable, you will have a data terminal equipment (DTE) end, which plugs in to the customer equipment, and a data communication equipment (DCE) end, which determines the speed of the connection from the ISP. Figure 1.34 below shows a DB60 serial interface on a WIC-1T card.

https://t.me/learningnets



Figure 1.33 – A DB60 Cable

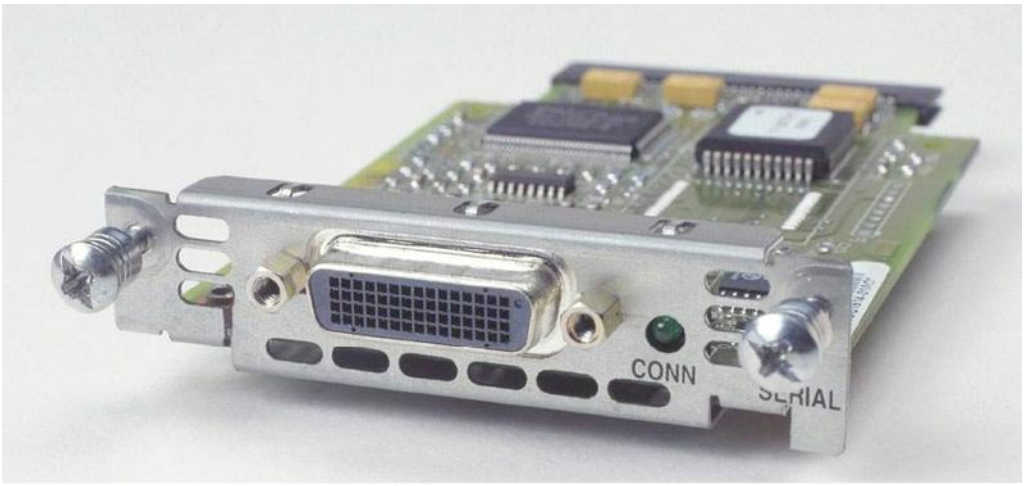


Figure 1.34 – The DB60 Serial Interface on a WIC-1T Card

There is another common presentation type for Cisco WAN Interface Cards (WICs) known as a smart serial cable:



https://t.me/learningnets

Figure 1.35 – Smart Serial Cable

Of course, you will need the correct interface card in the router if you use this cable type, as shown below in Figure 1.36:



Figure 1.36 WIC-2T Smart Serial Card

The smart serial WIC card gives you two connections for one slot on the router, as opposed to only one connection you would get with a standard WIC-1T card. Each serial connection can use a different encapsulation type, such as PPP for one and Frame Relay for the other.

The most important thing to remember about DCE and DTE cables is that you need to apply a clock rate to the DCE end in order for the line to come up. Normally, your ISP would do this because they own the DCE end, but on a home lab or live rack, you own the DCE end, which makes you the customer on one router and the ISP on the other router. The command you would enter is `clock rate 64000` (or whatever speed you like from the available options in bits per second). You can type `clock rate ?` to see your options.

Please ensure that you understand the following commands before typing them out on a router. Firstly, to establish which router has the DCE cable attached, you need to type the `show controllers` command, followed by the interface number. This is a very useful command to know for troubleshooting problems in the actual exam (and in the real world). You can see which interfaces you have on your router with the `show ip interface brief` command.

You can actually shorten most Cisco IOS commands, which is demonstrated in the output below. The shortened versions may not work in the exam, though, because the exam uses a router simulator (i.e., not a live router).

```
Router#sh ip int brie
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0   unassigned      YES unset  administratively down
down
FastEthernet0/1   unassigned      YES unset  administratively down
down
Serial0/1/0            unassigned      YES unset  administratively
down down
Vlan1                      unassigned      YES
unset  administratively down down
```

https://t.me/learningnets

```
Router#show controllers s0/1/0
Interface Serial0/1/0
Hardware is PowerQUICC MPC860
DCE V.35, no clock

Router(config-if)#clock rate ?
Speed (bits per second)
  1200
  2400
  4800
  9600
  19200
  38400
  56000
  64000

...

[Truncated Output]
```

Connecting to a Router

The first time you connect to a router or a switch, it can seem a little daunting. We have covered console connections above, so once you connect the cable, you will need to use a terminal emulation programme on your PC or laptop. This will allow you to see router output and type in the configuration commands.

HyperTerminal has been the default for many years, and you may need to use this still if you need to perform disaster recovery; however, for now you can stick to PuTTY, which is very widely used. You can download PuTTY from www.putty.org. An old-fashioned connection using the COM port on a PC almost always uses a logical port on it labelled COM1 or COM2. You can see the facility of using this on PuTTY, which actually calls this a serial connection, as shown in Figure 1.37 below:

https://t.me/learningnets

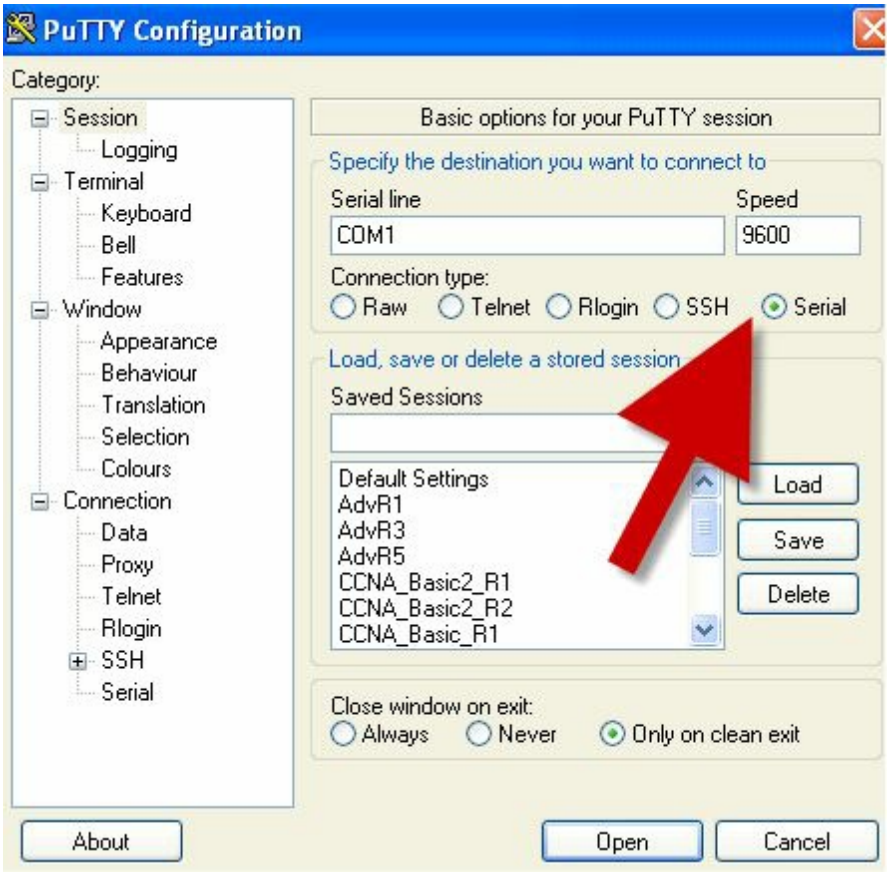


Figure 1.37 – PuTTY Uses COM Ports for Serial Access

If you are using a USB-to-rollover cable, then you will have received a driver CD, which, when run, will give you a COM port number to use. You can find this port number in the Device Manager if you are using Windows, as shown in Figure 1.38 below:

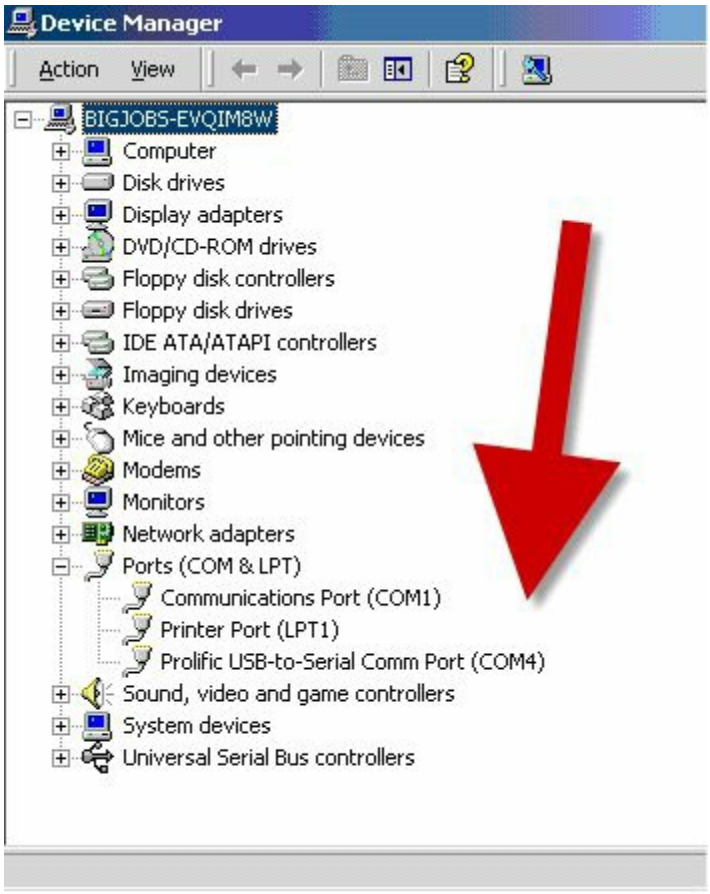


Figure 1.38 – The Driver Has Assigned COM4 for Console Connection

https://t.me/learningbots

If you are using HyperTerminal, you will also need to select more connection parameters, such as baud rate. You should choose the following, which is illustrated in Figure 1.39:

- Bits per second: 9600
- Data bits: 8 is the default
- Parity: None is the default
- Stop bits: 1 is the default
- Flow control: must be None

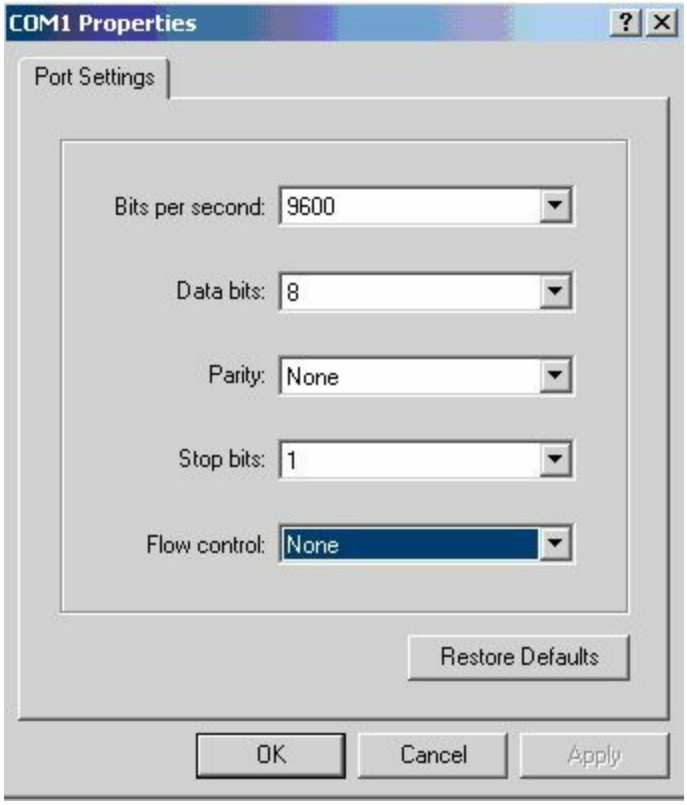


Figure 1.39 – Setting Your HyperTerminal Settings

When you turn on the router, if you have selected the correct COM port AND plugged the rollover cable into the console port (instead of a different port by accident), you should see the router boot-up text (see Figure 1.40). If you can't see any text, hit the Enter key a few times and then double-check your settings.

https://t.me/learningnets

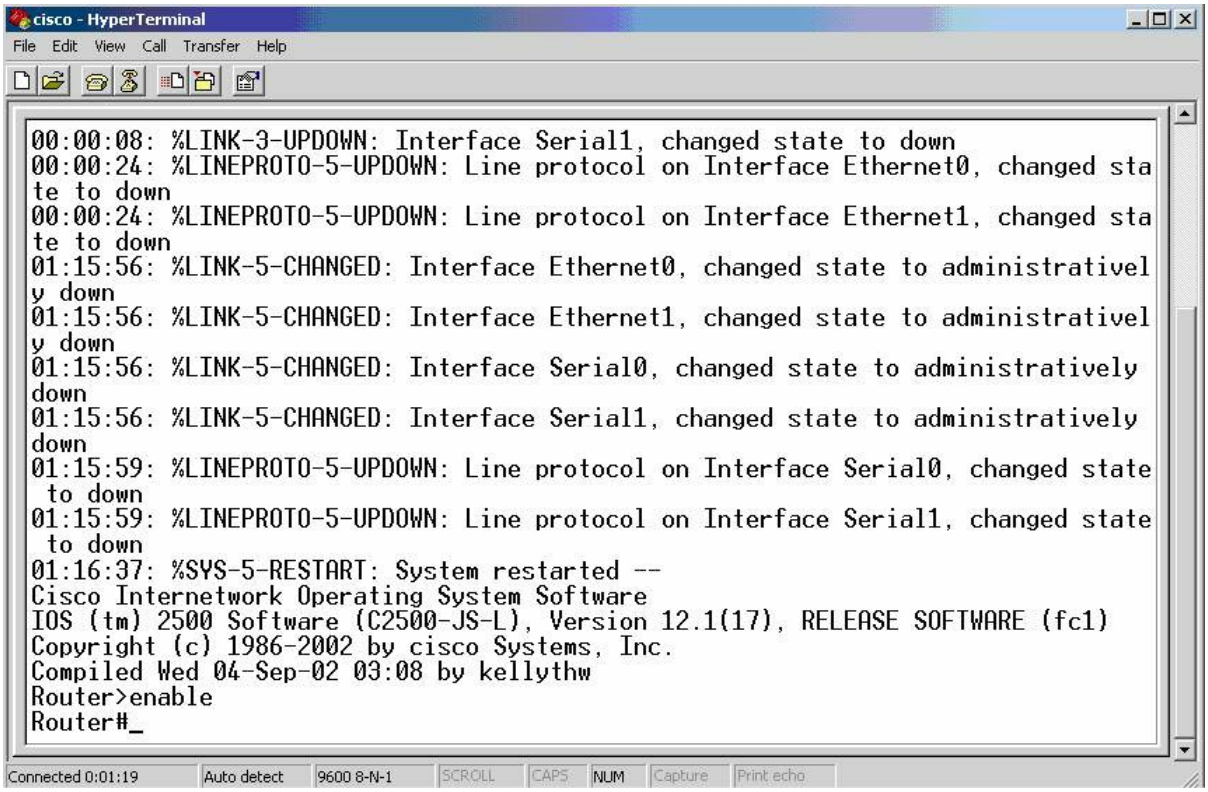


Figure 1.40 – The Router Boot-up Text

The router may ask whether you want to enter Initial Configuration mode. This happens when it can't find a startup configuration file in NVRAM (covered later) or if the configuration register is set to ignore the startup configuration file (usually 0x2142). Always type "n" or "no" because, otherwise, you will enter setup mode, which you don't want to do:

```
Would you like to enter the initial configuration dialog?
[yes/no]:
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog?
[yes/no]: no
Press RETURN to get started!
Router>
```

With a different router model, you would see the following output:

```
Technical Support: www.cisco.com/techsupport

Copyright (c) 1986-2007 by Cisco Systems, Inc.

Compiled Wed 18-Jul-07 04:52 by pt_team

         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>
```

Router Modes

In order to pass the CCNA exam, you will need to understand which router prompt you should

https://t.me/learningnets

start from to perform various actions. Whatever function you wish to perform, you will have to be in the correct mode (signified by the router prompt). This is the biggest mistake novice students make when they are having problems configuring the router and cannot find the right command to use. Make sure you are in the correct mode!

User Mode

The first mode you will be presented with when the router boots is known as User mode or User Exec mode. User mode has a very limited set of commands that can be used, but it can be useful for looking at basic router elements. The default name of the router is “Router” but this can be changed, as you will see later.

```
Router>
```

Privileged Mode

Typing enable at the User prompt takes you into the next mode, known as Privileged mode or Privileged Exec mode. To get back to User mode, you simply type disable. To quit the session altogether, type logout or exit.

```
Router>enable
Router#
Router#disable
Router>
```

Privileged mode is very useful for looking at the entire configuration of the router, the statistics about how it is performing, and even which modules you have connected to the router. At this prompt, you would type show commands and troubleshoot with debug commands.

Global Configuration Mode

In order to configure the router, you have to be in Global Configuration mode. To get to Global Configuration mode, you simply type configure terminal, or config t for short, at the Privileged Exec prompt. Alternatively, just type config and the router will ask you which mode you would like to enter. The default is terminal (the default options will be shown inside the square brackets [ ]). If you press Enter, the command inside the brackets will be accepted.

```
Router#config
Configuring from terminal, memory, or network[terminal]? ← press
Enter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Interface Configuration Mode

Interface Configuration mode allows you to enter commands for individual router interfaces, such as FastEthernet, Serial, etc. On a new router, all of the interfaces will be shut down by default, with no configuration present.

```
Router>enable
Router#config t
```

https://t.me/learningnets

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0
Router(config-if)#
```

It is okay to read through this the first time, but it will make far more sense if you try out all the commands on a real router as you read them. Remember to issue the `show ip interface brief` command to see which interfaces you have available. Your interface will probably not be Serial0.

Line Configuration Mode

Line Configuration mode is used to make any changes to the console, Telnet, or auxiliary ports (if your router has these). You can control who can access the router via these ports, as well as put passwords or a security feature called "access control lists" on them.

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#
```

You can also configure baud rates, exec levels, and more in Line Configuration mode.

Router Configuration Mode

In order to configure a routing protocol onto the router so it can dynamically build a picture of the network, you will need to be in Router Configuration mode.

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
```

VLAN Configuration Mode

This mode actually only applies to switches but it's worth mentioning it here while we are discussing modes. You will spend a lot of time in this mode when configuring the switching labs in this book.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#
```

Routers equipped with Ethernet switch cards use VLAN Database Configuration mode (this mode is deprecated on switches), which is similar to VLAN Configuration mode:

```
Router#vlan database

Router(vlan)#vlan 10

VLAN 10 added:

    Name: VLAN0010
```

https://t.me/learningnets

```
Router(vlan)#exit
APPLY completed.
Exiting....
Router#
```

Configuring a Router

There are no menus available on a router, and you cannot use a mouse to navigate between the different modes, as it is all done via the command line interface (CLI). There is, however, some context-sensitive help in the form of the `[?]` keyword. If you type a question mark at the router prompt, you will be presented with a list of all the available commands.

Please note that you will only see the commands available for your mode. If you want to see interface configuration commands, you must be at the interface prompt.

```
Router#?
Exec commands:
access-enable          Create a temporary Access-List entry
access-profile           Apply user-profile to interface
access-template       Create a temporary Access-List entry
alps                           ALPS exec commands
archive                      manage archive files
bfe                             For manual emergency modes
setting
cd                              Change current directory
clear                          Reset functions
clock                        Manage the system clock
cns                            CNS subsystem
configure                   Enter configuration mode
connect                    Open a terminal connection
copy                          Copy from one file to another
debug                       Debugging functions (see also
'undebug')
delete                        Delete a file
dir                              List files on a directory
disable                      Turn off privileged commands
disconnect                 Disconnect an existing network
connection
```

https://t.me/learningnets

```
enable                          Turn on privileged commands
erase                           Erase a file
exit                            Exit from the EXEC mode
help                            Description of the interactive
help system
-- More –
```

If there is too much information to display on the screen, you will see the -- More -- tab. If you want to see the next page, press the space bar. If not, hold down the Ctrl+Z keys together or press “Q” to get back to the router prompt.

In addition, if you have started to type a command but forget what else you need to type in, using the question mark will give you a list of options available. The [?] keyword WILL work in the CCNA exam, but if you are using it, you didn’t follow all my labs!

```
Router#cl?
clear clock
```

If you begin to type out a command, as long as there is only one possible word or command available with that syntax, you can press the Tab key to have it completed for you.

```
Router#copy ru   ← press the Tab key here
Router#copy running-config
```

The router has several modes from which to choose. This is to ensure that you do not make changes to parts of the router configuration you do not intend to change. You can recognise which mode you are in by looking at the command prompt. For example, if you wanted to make some changes to one of the FastEthernet interfaces, you would need to be in Interface Configuration mode.

First, go into Global Configuration mode:

```
Router#config t
Router(config)#
```

Next, tell the router which interface you want to configure:

```
Router(config)#interface FastEthernet0
Router(config-if)#exit
Router(config)#
```

If you are not sure which way to enter the interface number, then use the [?] keyword. Do not worry about all of the choices you will be given. Most people only use the FastEthernet, Serial, and Loopback interfaces.

```
Router(config)#interface ?
Async                           Async interface
BRI                             ISDN Basic Rate Interface
BVI                             Bridge-Group Virtual Interface
```

https://t.me/learningnets

```
CTunnel                    CTunnel interface
Dialer                       Dialer interface
FastEthernet             IEEE 802.3u
Group-Async              Async Group interface
Lex                            Lex interface
Loopback                 Loopback interface
Multilink                  Multilink-group interface
Null                           Null interface
Serial                       Serial interface
Tunnel                     Tunnel interface
Vif                              PGM Multicast Host interface
Virtual-Template      Virtual Template interface
Virtual-TokenRing    Virtual TokenRing interface
range                          interface range command


Router(config)#interface FastEthernet?
<0-0> FastEthernet interface number
Router(config)#interface FastEthernet0
```

Finally, the router drops into Interface Configuration mode:

```
Router(config-if)#
```

From here, you can put an IP address on the interface, set the bandwidth, apply an access control list, and do a lot of other things. Please note that your router and switch may well have different interface numbers from mine, so use the `?` or `show ip interface brief` commands to see your options.

If you ever need to exit out of a configuration mode, simply type `exit`. This takes you back to the next-highest level. To quit any sort of configuration mode, simply press Ctrl+Z together (or type `end`).

```
Router(config-if)#exit
Router(config)#
```

Or, if using the Ctrl+Z option:

```
Router(config-if)#^z
Router#
```

Loopback Interfaces

Loopback interfaces are not normally covered in the CCNA syllabus, but they are very useful in

https://t.me/learningnets

the real world and for practice labs. A Loopback interface is a virtual or logical interface that you configure, but it does not physically exist (so you will never see it on the router panel). The router will let you ping this interface, though, which will save you from having to connect devices to the FastEthernet interfaces in the labs.

An advantage of using Loopback interfaces is that they always remain up, if the router is working, because they are logical, meaning they can never go down. However, you cannot put a network cable into the Loopback interface because it is a virtual interface.

```
Router#config t
Router#(config)#interface Loopback0
Router#(config-if)#ip address 192.168.20.1 255.255.255.0
Router#(config-if)#^z ← press Ctrl+Z
Router#
Router#show ip interface brief
Interface                  IP-Address
OK?            Method          Status              Protocol
Loopback0              192.168.20.1
YES             manual              up                  up
```

Your output for this command will show all of the available interfaces on your router.

IN THE REAL WORLD: If you need to, you can shut down a Loopback interface with the `shutdown` command in Interface Configuration mode.

Loopback interfaces have to be given a valid IP address. You can then use them for routing protocols or for testing your router to see whether it is permitting certain traffic. You will be using these interfaces a lot throughout the course.

Editing Commands

It is possible to navigate your way around a line of configuration you have typed rather than deleting the whole line. The following keystrokes will move the cursor to various places in the line:

Keystroke	Meaning
Ctrl+A	Moves to the beginning of the command line
Ctrl+E	Moves to the end of the command line
Ctrl+B	Moves back one character
Ctrl+F	Moves forward one character
Esc+B	Moves back one word
Esc+F	Moves forward one word

https://t.me/learningnets

Ctrl+P or up arrow	Recalls the previous command
Ctrl+N or down arrow	Recalls the next command
Ctrl+U	Deletes a line
Ctrl+W	Deletes a word
Tab	Finishes typing a command for you
Show history	Shows the last 10 commands entered by default
Backspace	Deletes a single character

It is fairly common to have a question on the above in the exam.

Configuring a Router Interface

Router interfaces can be of different types, based on the following two factors:

- Underlying technology used (e.g., Ethernet)
- Interface bandwidth

The most common router and switch interfaces used in modern enterprise networks are:

- 100Mbps (commonly named FastEthernet)
- 1Gbps (commonly named GigabitEthernet)
- 10Gbps (commonly named TenGigabitEthernet)

In order to address a specific router interface and to enter Interface Configuration mode to configure specific parameters, you must know the interface notation. This can vary based on the router manufacturer, but the interface notation is usually made up of two parts:

- Interface type (Ethernet, FastEthernet, etc.)
- Interface slot/module and port number

For example, common interface notations include the following:

- Ethernet1/0 (slot 1, port 0)
- FastEthernet0/3 (slot 0, port 3)
- GigabitEthernet0/1/1 (module 0, slot 1, port 1)

NOTE: Slot 0 usually represents the built-in ports, and the other slots represent extension slots that can be added at any time. Slot and port numbering usually starts at 0.

In order for a router interface to have basic functionality, you must configure the following parameters:

- Speed
- Duplex

https://t.me/learningnets

- IP address

You can exemplify these basic configuration settings on a Cisco router, as they are commonly used in modern enterprise networks. To see the available interfaces and their current state, you can issue the following command:

```
Router#show ip interface brief
Interface        IP-Address   OK? Method Status            Protocol
FastEthernet0/0  unassigned   YES unset  administratively down down
FastEthernet0/1  unassigned   YES unset  administratively down down
```

From the output above, you can see that the router has two FastEthernet (100 Mbps) interfaces on slot 0, both unconfigured (i.e., no IP address) and administratively disabled (i.e., status: administratively down).

Before starting to configure interface parameters, you must enter Router Configuration mode using the `configure terminal` command on Cisco devices, and then Interface Configuration mode using the `interface <interface name>` command. The first step in the interface configuration process is enabling the interface. For example, the interface FastEthernet0/0 can be enabled using the `no shutdown` command:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#no shutdown
Router(config-if)#
*Mar  1 00:32:05.199: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:32:06.199: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
```

The next configuration step involves setting up speed and duplex settings and we have already covered these.

Configuring an IP Address on an Interface

In order for a router to communicate with other devices, it will need to have an address on the connected interface. Configuring an IP address on an interface is very straightforward, although you have to remember to go into Interface Configuration mode first.

Don’t worry about where to find the IP address at the moment, as we will look at that later on.

`Router>enable` ← takes you from User mode to Privileged mode

`Router#config t` ← from Privileged mode to Configuration mode

`Router(config)#interface Serial0` ← and then into Interface Configuration mode

```
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

`Router(config-if)#no shutdown` ← the interface is opened for traffic

https://t.me/learningnets

```
Router(config-if)#exit ← you could also hold down the Ctrl+Z keys together to exit
Router(config)#exit
Router#
```

A description can also be added to the interface, as shown in the following output:

```
RouterA(config)#interface Serial0
RouterA(config-if)#description To_Headquarters
RouterA(config-if)#^Z ← press Ctrl+Z to exit
```

After the router interface configuration is complete, you can verify the setting by inspecting the full interface-configured parameters using the commands below on Cisco routers:

```
RouterA#show interface Serial0
Serial0 is up, line protocol is up
Hardware is HD64570
Description: To_Headquarters
Internet address is 12.0.0.2/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input 00:00:02, output 00:00:03, output hang never
[Output restricted...]
```

Show Commands

You can look at most of the settings on the router simply by using the `show x` command from Privileged mode, with `x` being the next command, as illustrated in the following output:

```
Router#show ?
access-expression   List access expression
access-lists        List access lists
accounting          Accounting data for active sessions
adjacency           Adjacent nodes
aliases             Display alias commands
alps                Alps information
apollo              Apollo network information
appletalk           AppleTalk information
arap                Show AppleTalk Remote Access statistics
arp                 ARP table
async               Information on terminal lines used as router interfaces
backup              Backup status
bridge              Bridge Forwarding/Filtering Database [verbose]
bsc                 BSC interface information
bstun               BSTUN interface information
buffers             Buffer pool statistics
cca                 CCA information
cdapi               CDAPI information
```

https://t.me/learningnets

```
cdp                 CDP information
cef                 Cisco Express Forwarding
class-map           Show QoS Class Map
clns                CLNS network information
--More--
```

Some of the more common `show` commands and their meanings, along with an example, are listed below:

Show Command	Result
`show running-configuration`	Shows configuration in DRAM
`show startup-configuration`	Shows configuration in NVRAM
`show flash:`	Shows which IOS is in flash
`show ip interface brief`	Shows brief summary of all interfaces
`show interface Serial0`	Shows Serial interface statistics
`show history`	Shows last 10 commands entered

```
Router#show ip interface brief
Interface    Address        OK?    Method    Status                  Protocol
Ethernet0    10.0.0.1       YES    manual    up                        up
Ethernet1    unassigned     YES    unset     administratively down     down
Loopback0    172.16.1.1     YES    manual    up                        up
Serial0      192.168.1.1    YES    manual    down                      down
Serial1      unassigned     YES    unset     administratively down     down
```

The `method` tag indicates how the address has been assigned. It can state `unset`, `manual`, `NVRAM`, `IPCP`, or `DHCP`.

Routers can recall commands previously entered at the router prompt – the default is 10 commands – which can be recalled by using the up arrow. Using this feature can save a lot of time and effort, as it prevents you from having to re-enter a long line. The `show history` command shows the buffer of the last 10 commands.

```
Router#show history
show ip interface brief
show history
show version
show flash:
conf t
show access-lists
show process cpu
show buffers
show logging
```

https://t.me/learningnets

```
show memory
```

You can increase the history buffer with the `terminal history size` command:

```
Router#terminal history ?
size Set history buffer size
<cr>
```

```
Router#terminal history size ?
<0-256> Size of history buffer
```

```
Router#terminal history size 20
```

Verifuing Basic Router Configuration and Network Connectivity

The most useful commands that help verify basic router configuration are explained in the following sections.

Show Version

The `show version` command provides useful information that might represent a starting point in verifying most of the router operations. This information includes the following:

- Type of router (another useful command for listing the router hardware is `show inventory`)
- IOS version
- Memory capacity
- Memory usage
- CPU type
- Flash capacity
- Other hardware parameters
- Reason for last reload

Here is a shortened output of the `show version` command. Please try it out for yourself.

```
Router#show version
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed Serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)


Configuration register is 0x2102
```

Show Running-config

The `show running-config` command provides full configuration on the router, and it can be used to verify that the device is configured with the proper features. The output for this command is

https://t.me/learningnets

too extensive so it will not be presented here.

Show IP Interface Brief

The `show ip interface brief` command, as mentioned in a previous section, lists the router interfaces and their state, including:

- Interface name and number
- IP address
- Link status
- Protocol status

```
Router#show ip interface brief
Interface        IP-Address OK? Method Status                Protocol
FastEthernet0/0  unassigned YES unset  administratively down down
FastEthernet0/1  unassigned YES unset  administratively down down
Serial0/0/0      unassigned YES unset  administratively down down
Serial0/1/0      unassigned YES unset  administratively down down
Vlan1            unassigned YES unset  administratively down down
Router#
```

Show IP Route

The `show ip route` command provides deep information regarding the routing capabilities of the device. It lists all the networks the router can reach and information about the way they can be reached, including:

- Network
- Routing protocol
- Next hop
- Outgoing interface

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
       area, N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
       type 2, E1 - OSPF external type 1, E2 - OSPF external type 2,
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
       inter area, * - candidate default, U - per-user static route,
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
R       80.1.1.0/24 [120/1] via 10.1.1.2, 00:00:04, Ethernet0/0.1
D       80.0.0.0/8 [90/281600] via 10.1.1.2, 00:02:02, Ethernet0/0.1
O E2    80.1.1.0/24 [110/20] via 10.1.1.2, 00:00:14, Ethernet0/0.1
```

https://t.me/learningnets

In addition to the `show` commands presented above, other useful methods of verifying router connectivity include using the `ping` and `traceroute` commands.

Ping

The `ping` command provides a basic connectivity test to a specific destination. This way you can test whether the router can reach a network or not. Ping works (using ICMP) by sending echo requests to a machine to verify whether it is up and running. If a specific machine is operating, it will send an ICMP echo reply message back to the source, confirming its availability. A sample ping is presented below:

```
Router#ping 10.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/40/76 ms
```

A standard `ping` command sends five ICMP packets to the destination. When looking at the ping output, a dot (.) represents a failure and an exclamation mark (!) represents a successfully received packet. The ping command output also shows the round-trip time to the destination network (minimum, average, and maximum).

If you need to manipulate ping-related parameters, you can issue an extended ping from a Cisco router. This is done by typing `ping` and pressing Enter in the console. The router will prompt you with an interactive menu where you can specify the desired parameters, including:

- Number of ICMP packets
- Packet size
- Timeout
- Source interface
- Type of service

```
Router#ping
Protocol [ip]:
Target IP address: 10.10.10.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: FastEthernet0/0
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
```

https://t.me/learningnets

```
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/36/72 ms
```

Traceroute

The `traceroute` command is another useful tool that allows you to see the hops a packet passes until it reaches its destination. The output below shows that the packet has to cross a single hop until it reaches its destination:

```
R2#traceroute 192.168.1.1
Type escape sequence to abort.
Tracing the route to 192.168.1.1
  1 10.10.10.1 60 msec *  64 msec
```

Just like with ping, Cisco routers allow you to perform an extended `traceroute` command that can define a number of associated parameters, most of them similar to the ping-related parameters:

```
Router#traceroute
Protocol [ip]:
Target IP address: 192.168.1.1
Source address: 10.10.10.2
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.1.1
  1 10.10.10.1 76 msec *  56 msec
```

https://t.me/learningnets

Day 1 Questions

OSI/TCP Model Questions

1. Name each layer of the OSI model, from Layer 7 down to Layer 1.
2. The role of the Session Layer is to _____, _____, and _____ sessions or dialogues between devices.
3. What are the three methods used to control data flow at Layer 4?
4. The Transport Layer includes several protocols, and the most widely known are _____ and _____.
5. Why is UDP used at all if TCP/IP offers guaranteed delivery?
6. What is data referred to at each OSI layer?
7. In order to interface with the upper and lower levels, the Data Link Layer is further subdivided into which two Sublayers?
8. What are the five TCP/IP layers from the top down?
9. How does the TCP/IP model map to the OSI model?
10. Layer 2 addresses are also referred to as _____ addresses.
11. Using a switch will allow you to divide your network into smaller, more manageable sections known as _____ _____.

Cable Questions

1. The current standard Ethernet cable still uses eight wires twisted into pairs to prevent _____ _____ and _____.
2. _____ is when a signal from one Ethernet wire spills over into a neighbouring cable.
3. Which command would set the FastEthernet router interface speed to 10Mbps?
4. On a crossover cable, the wire on pin 1 on one end needs to connect to pin _____ on the other end and pin 2 needs to connect to pin _____.
5. Which cable would you use to connect a router Ethernet interface to a PC?
6. You can see a summary of which interfaces you have on your router with the show _____ _____ _____ command.
7. Line Configuration mode lets you configure which ports?
8. A Loopback interface is a _____ or _____ interface that you configure.
9. The keyboard shortcut Ctrl+A does what?
10. The _____ keyboard shortcut moves the cursor back one word.
11. By default, the _____ _____ command shows the last 10 commands entered.

https://t.me/learningnets

Day 1 Answers

OSI/TCP Model Answers

1. Application, Presentation, Session, Transport, Network, Data Link, and Physical.
2. Set up, manage, and terminate.
3. Flow control, windowing, and acknowledgements.
4. TCP and UDP.
5. TCP uses a lot of bandwidth on the network and there is a lot of traffic sent back and forth to set up the connection, even before the data is sent. This all takes up valuable time and network resources. UDP packets are a lot smaller than TCP packets and they are very useful if a really reliable connection is not that necessary. Protocols that use UDP include DNS and TFTP.
6. Bits (Layer 1), Frames (Layer 2), Packets (Layer 3), Segments (Layer 4) and Data (Layers 5-7).
7. LLC and MAC.
8. Application, Transport, Network, Data Link, and Network.
9.

Layer #	OSI	Data
7	Application	Application
6	Presentation	
5	Session	
4	Transport	Host to Host
3	Network	Internetwork
2	Data Link	Network Interface
1	Physical	

10. MAC.
11. Collision domains.

Cable Answers

1. Electromagnetic interference (EMI) and crosstalk.
2. Crosstalk.
3. The `speed 10` command.
4. 3 and 6.
5. A crossover cable.
6. `ip interface brief`.

https://t.me/learningnets

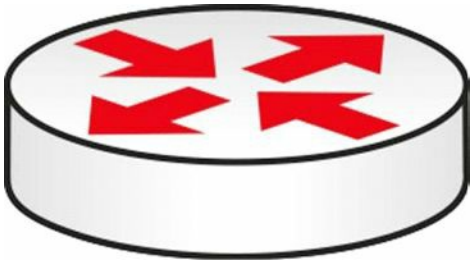
7. The console, Telnet, and auxiliary ports.
8. Virtual or logical.
9. Moves the cursor to the beginning of the command line.
10. Esc+B.
11. `show history`.

https://t.me/learningnets

Day 1 Lab

IOS Command Navigation Lab

Topology



Purpose

Learn how to connect to a router via the console port and try out some commands.

Walkthrough

1. Use a console cable, along with PuTTY (free online; search for “PuTTY”), to connect to a router console port. Check out my “Connect to a Cisco Router ” video if you get stuck:

   www.in60days.com

2. From the `Router>` prompt, enter the commands below, exploring various router modes and commands. If you are asked to enter Setup mode, type “no” and hit Enter. Please bear in mind that you will have a different router model from mine, so some output will differ.

```
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
Technical Support: www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
         --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]:no
Press RETURN to get started!
Router>enable
Router#show version
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed Serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Configuration register is 0x2102
Router#show ip interface brief
```

https://t.me/learningnets

```
Interface        IP-Address OK? Method Status                Protocol
```

```
FastEthernet0/0  unassigned YES unset  administratively down down
FastEthernet0/1  unassigned YES unset  administratively down down
Serial0/0/0      unassigned YES unset  administratively down down
Serial0/1/0      unassigned YES unset  administratively down down
Vlan1            unassigned YES unset  administratively down down
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial0/1/0 ← put your serial # here
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#interface Loopback0
Router(config-if)#ip address 10.1.1.1 255.0.0.0
Router(config-if)#^Z ← press Ctrl+Z keys together
Router#
Router#show ip interface brief
Interface       IP-Address  OK? Method Status                Protocol
FastEthernet0/0 unassigned  YES unset  administratively down down
FastEthernet0/1 unassigned  YES unset  administratively down down
Serial0/0/0     unassigned  YES unset  administratively down down
Serial0/1/0     192.168.1.1 YES manual administratively down down
Loopback0       10.1.1.1    YES manual up                    up
Vlan1           unassigned  YES unset  administratively down down
Router#show history
Router(config)#hostname My_Router
My_Router(config)#line vty 0 ?
  <1-15>  Last Line number
  <cr>
My_Router(config)#line vty 0 15 ← enter 0 ? to find out how many lines you have
My_Router(config-line)#
My_Router(config-line)#exit
My_Router(config)#router rip
My_Router(config-router)#network 10.0.0.0
My_Router(config-router)#
```

https://t.me/learningnets

Day 2 – CSMA/CD, Switching, and VLANs

Day 2 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Read the ICND1 cram guide

The bread-and-butter work of any Cisco engineer is installing, configuring, and troubleshooting switches. Strangely enough, this is the weakest area for many of those engineers. Perhaps some people rely on the switches' plug-and-play capabilities, or they try to work through issues as they crop up. This "fly by the seat of your pants" mentality backfires for many engineers when there is a switching-related issue.

I suggest that you give every subject in this book just a cursory read-over to start with, and then read them again a few times over, each time making notes or highlighting the main learning points.

Today you will learn about the following:

- CSMA/CD
- VLANs
- Configuring VLANs
- Troubleshooting VLANs

This module maps to the following CCNA syllabus requirements:

- Determine the technology and media access control method for Ethernet networks
- Identify basic switching concepts and the operation of Cisco switches
  - Collision domains
  - Broadcast domains
  - Types of switching
  - CAM table
- Configure and verify initial switch configuration, including remote access management
  - Cisco IOS commands to perform basic switch setup
- Verify network status and switch operation using basic utilities such as ping, Telnet, and SSH
- Describe how VLANs create logically separate networks and the need for routing between them
  - Explain network segmentation and basic traffic management concepts

https://t.me/learningnets

- Configure and verify VLANs

Switching Basics

Carrier Sense, Multiple Access with Collision Detection

Carrier sense, multiple access with collision detection (CSMA/CD) can be broken down as follows: Carrier sense means that the wire is listened to in order to determine whether there is a signal passing along it. A frame cannot be transmitted if the wire is in use. Multiple access simply means that more than one device is using the cables on the segment. Finally, collision detection means that the protocol is running an algorithm to determine whether the frames on the wire have become damaged due to hitting another frame. In Figure 2.1 below, you can see the switch port listening to the wire.



Figure 2.1 – Port Listening to the Wire

If there is a collision on the wire, the detecting device(s) send a jamming signal informing other network devices that a collison has occurred, so they should not attempt to send data onto the wire. Then, the algorithm runs and generates a random interval to wait before retransmitting. It must still wait for the wire to be clear before sending a frame. Here is how Wikipedia describe the process:

https://t.me/learningnets

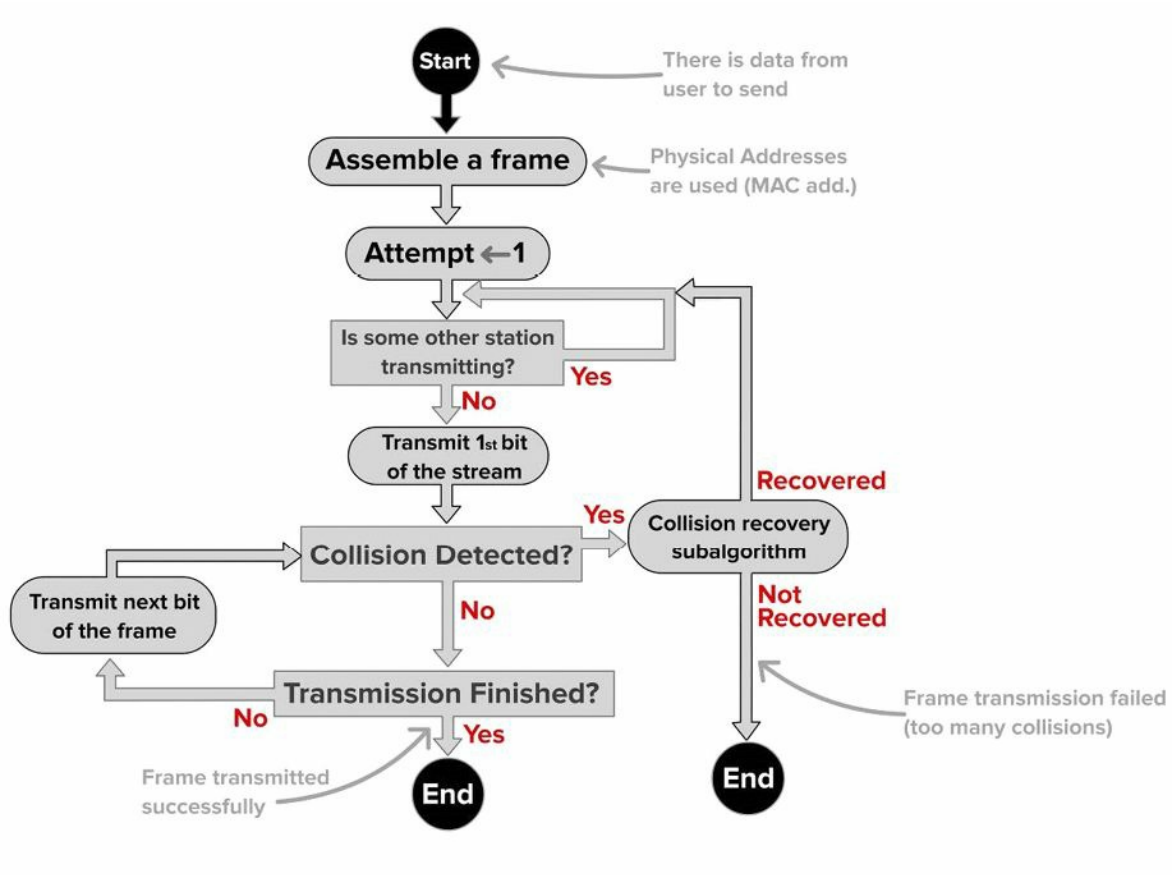


Figure 2.2 – CSMA/CD Process

Farai says – "Please note that modern Ethernet networks using switches with full-duplex connections no longer utilise CSMA/CD. It is still supported, but only for backwards compatibility."

Collision and Broadcast Domians

One of the main drawbacks of network hubs is that when there is a collision on the wire, that damaged frame is sent to all connected devices. One of the advantages of modern switches is that each port on the switch is considered to be a collision domain. In the event of a collision (not possible with full duplex) the damaged frame does not pass the interface. Figure 2.3 shows that a switch has been added to a small network using two hubs. The switch breaks the network into two collision domains.

https://t.me/learningnets

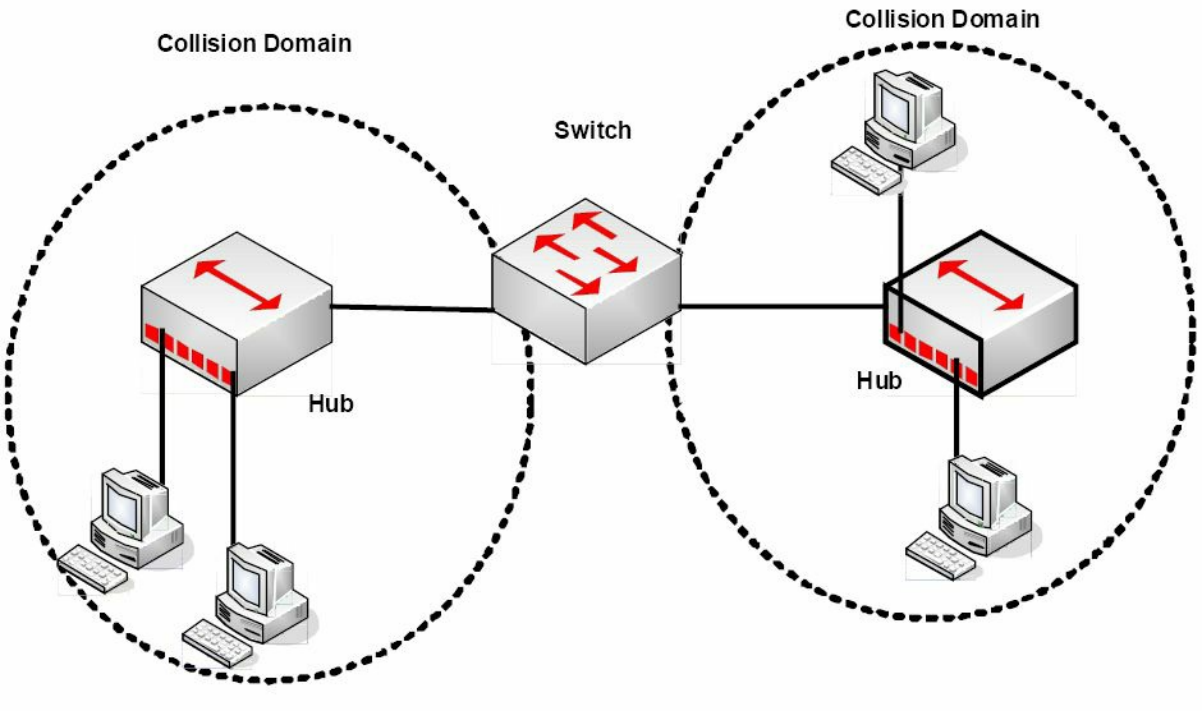


Figure 2.3 – A Switch Creates Two Collision Domains

Cisco commonly try to catch you out in the exam by asking whether switches reduce the amount of collision domains. In haste, you might be tempted to say they do but the opposite is actually the case, and this is a good thing. Switches increase the number of collision domains. It's also worth noting that hubs can only work at half duplex due to the limitations of the technology. In Figure 2.4 below, four PCs are connected to a switch, creating four collision domains. Each PC has full use of 100Mbps bandwidth operating in full duplex.

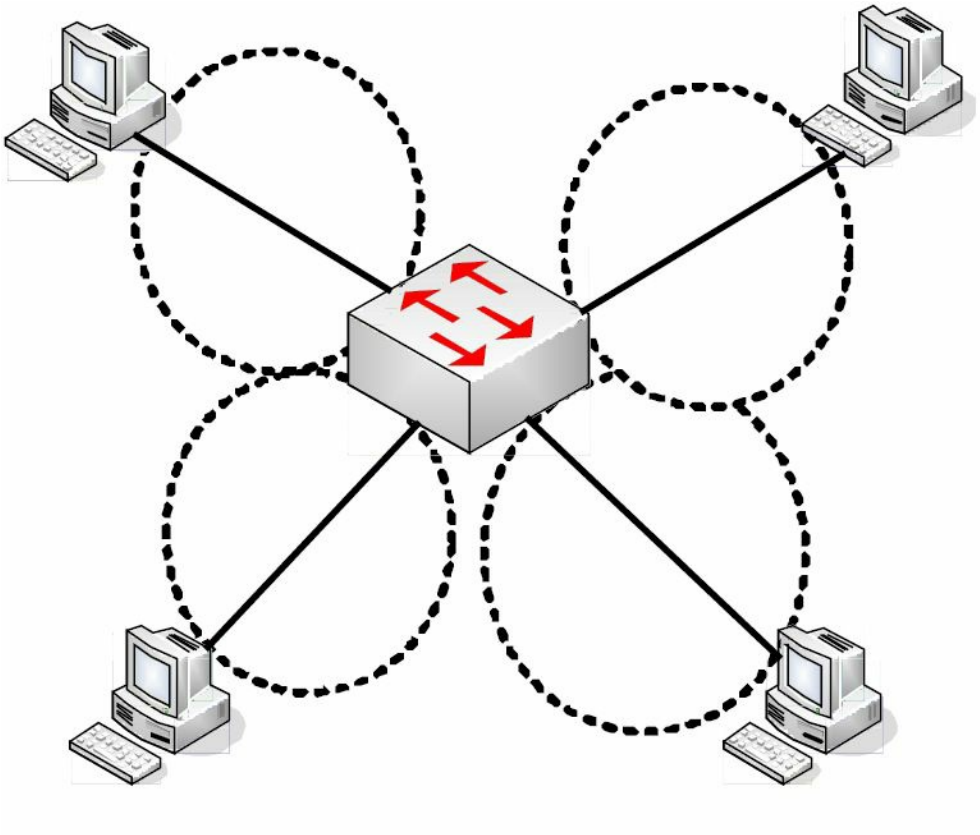


Figure 2.4 – Four Collision Domans

https://t.me/learningnets

Switches (here we are talking about Layer 2 switches) do not separate Broadcast domains,

routers do. If a switch receives a frame with a Broadcast destination address, then it must forward it out of all ports, apart from the port the frame was received on. A router is required to separate Broadcast domains. Figure 2.5 represents a small network using switches/bridges and a router to represent how collision domains are separated.

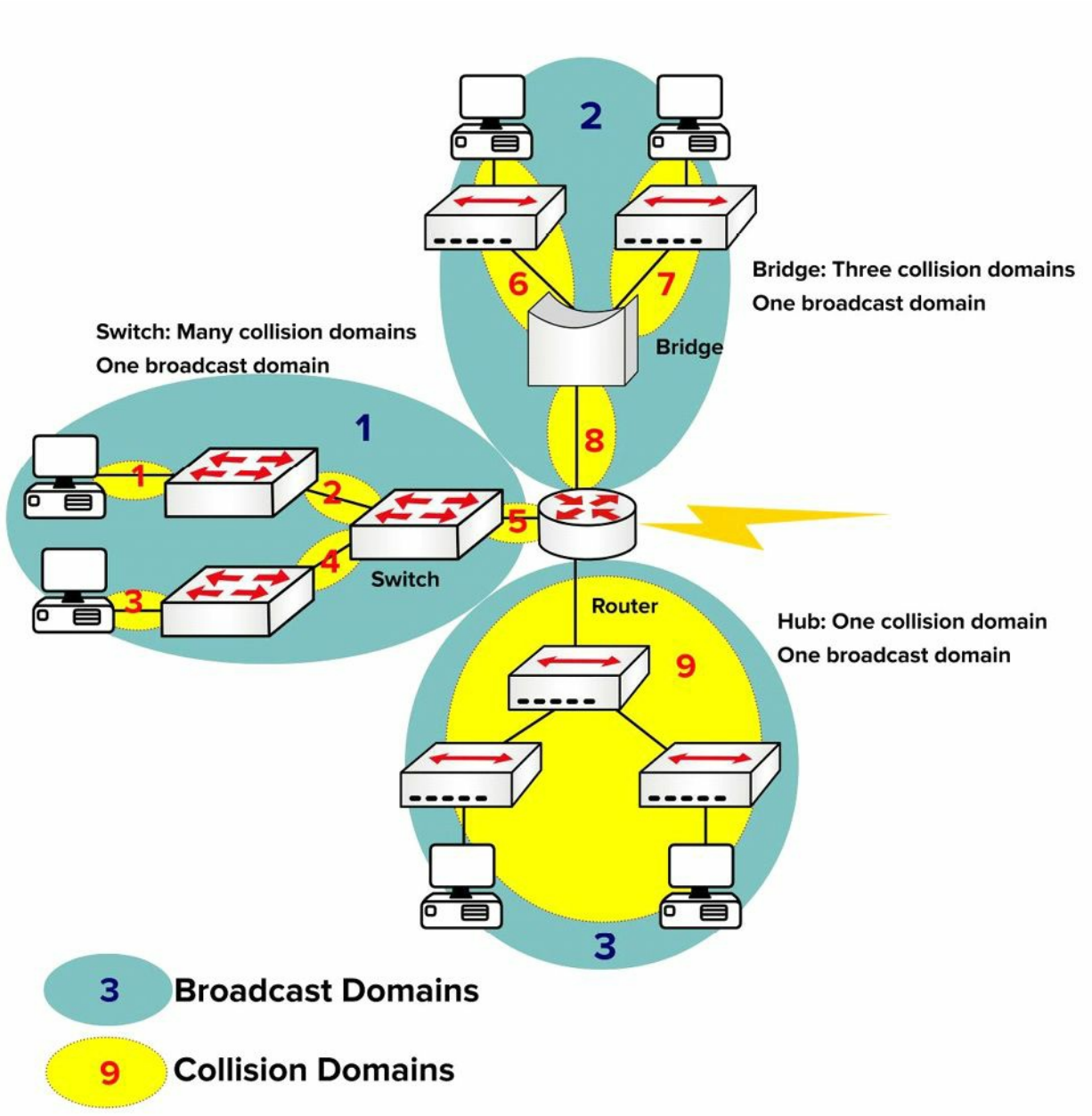


Figure 2.5 – Broadcast and Collision Domains

Auto-negotiation

You have already seen that issues can arise when you connect devices with different speeds and duplex settings. You can often upgrade one section of the network but have legacy equipment on another due to budget constraints. This can lead to duplex and speed mismatches, leading to errors and dropped frames. We will cover switch troubleshooting in more detail later.

The IEEE offer a solution to this issue with auto-negotiation, which allows devices to agree on the speed and duplex settings before passing traffic. The speed is set to the speed of the slower device. In the output below, the speed can be set manually to 10Mbps or 100Mbps, or set to auto negotiate.

```
Switch(config)#int f1/0/1
Switch(config-if)#speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration
```

You can check the settings with the `show interface x` command:

```
Switch#show int f1/0/1
FastEthernet1/0/1 is down, line protocol is down (notconnect)
  Hardware is FastEthernet, address is 001e.13da.c003 (bia 001e.13da.c003)
  MTU 1600 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, Loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100BaseTX
```

Bear in mind, though, that auto-negotiation may cause issues. This is why many production networks insist on configuring ports directly as 100/full or 1000/full for GigabitEthernet. According to Cisco:

> Auto-negotiation issues can result from nonconforming implementation, hardware incapabilities, or software defects. When NICs or vendor switches do not conform exactly to the IEEE specification 802.3u, problems can result. Hardware incompatibility and other issues can also exist as a result of vendor-specific advanced features, such as auto-polarity or cable integrity, which are not described in IEEE 802.3u for 10/100 Mbps auto-negotiation (Cisco.com).

Switching Frames

Switches exist to switch frames (i.e., transport a frame from an incoming interface to the correct outgoing interface). Broadcast frames are switched out of all interfaces (except the interface on which they were received), as are frames with an unknown destination (not in the MAC table). In order to achieve this function, a switch performs three actions:

- Forwarding or filtering (dropping) frames based on destination MAC addresses
- Learning MAC addresses from incoming frames
- Using STP to prevent Layer 2 loops (STP will be covered in ICND2 Day 31)

In Figure 2.6 below, the switch filters the frame from leaving interface F0/2 and correctly forwards it out of F0/3 when sourcing from Host A (F0/1) destined for Host C:

https://t.me/learningnets

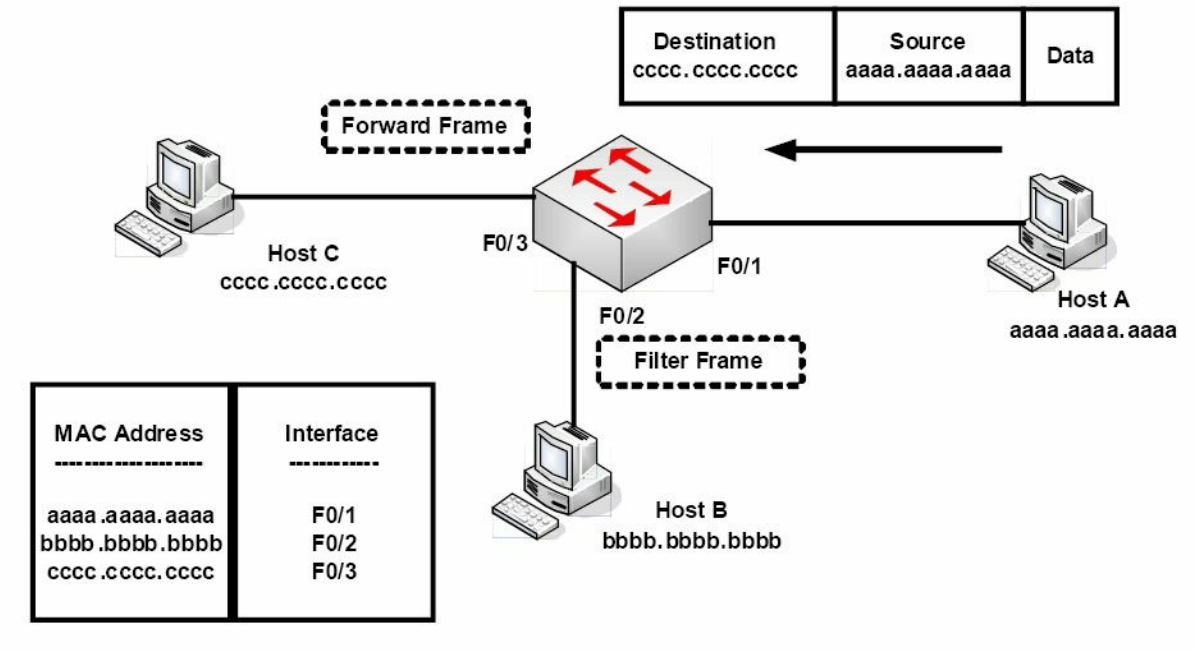


Figure 2.6 – Frame Filtering

If the destination address was not in the MAC address table, then the switch would have flooded the frame out of all interfaces, except the interface it was received on. The switch will also store MAC addresses for devices connected to another switch; however, the interface name will remain the same, so multiple MAC addresses will be listed with the same exit interface. This is a useful way to find a device on a network you are not familiar with. Figure 2.7 below illustrates this concept:

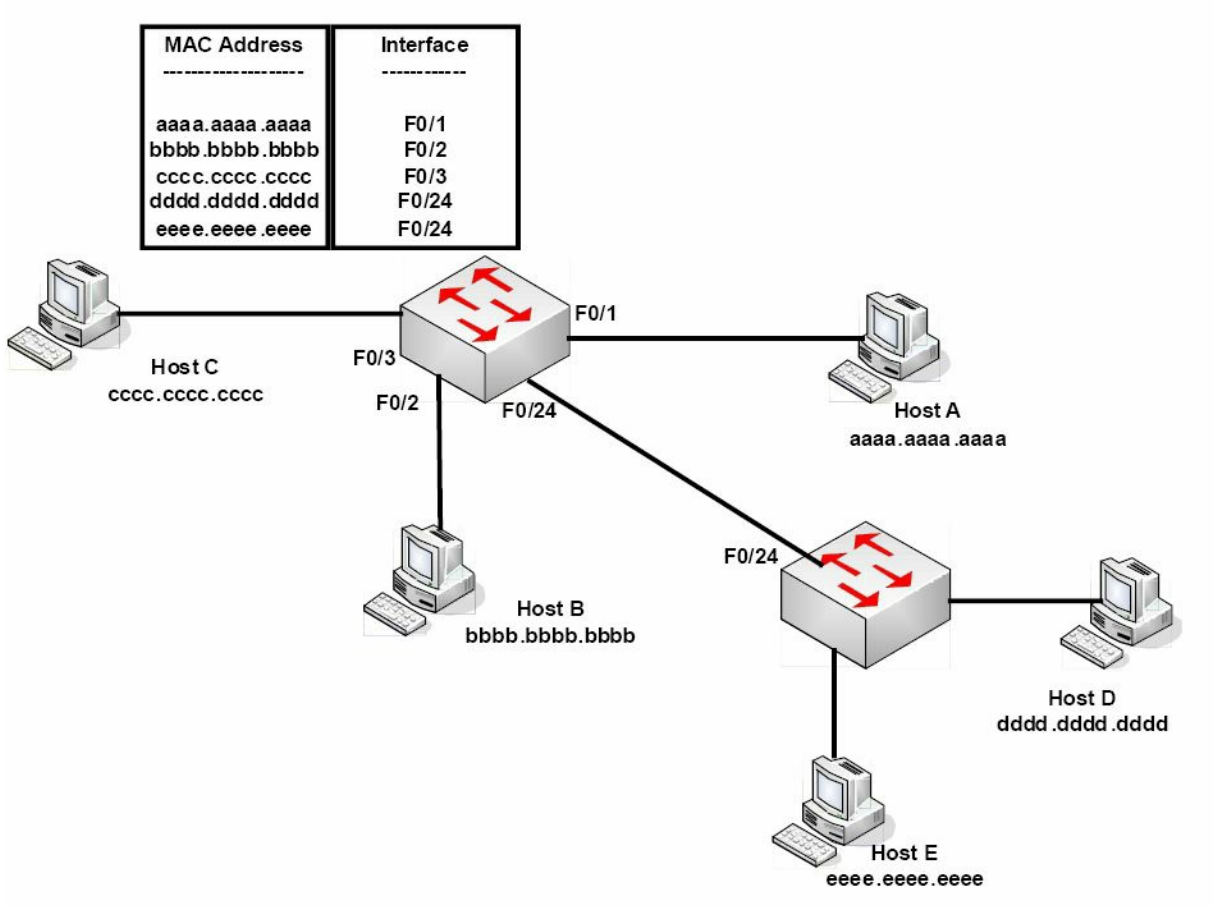


Figure 2.7 – Multiple MAC Addresses on the Same Interface

https://t.me/learningnets

Any delay in passing traffic is known as latency. Cisco switches offer three ways to switch the

traffic, depending upon how thoroughly you want the frame to be checked before it is passed on. The more checking performed, the more latency you will introduce to the switch. The three switching modes to choose from are:

- Cut-through
- Store-and-forward (default on modern switches)
- Fragment-free

Cut-through

Cut-through switching is the fastest switching method, meaning it has the lowest latency. The incoming frame is read up to the destination MAC address. Once it reaches the destination MAC address, the switch then checks its CAM table for the correct port to forward the frame out of and sends it on its way. There is no error checking, so this method gives you the lowest latency. The price, however, is that the switch will forward any frames containing errors.

The process of switching modes can best be described by using a metaphor. You are the bouncer at a nightclub and are asked to make sure that everyone who enters has a picture ID – you are not asked to make sure the picture matches the person, only that the ID has a picture. With this method of checking, people are surely going to move quickly to enter the establishment. This is how cut-through switching works.

Store-and-forward

Here, the switch reads the entire frame and copies it into its buffers. A cyclic redundancy check (CRC) takes place to check the frame for any errors. If errors are found, the frame is dropped. Otherwise, the switching table is examined and the frame forwarded. Store-and-forward ensures that the frame is at least 64 bytes but no larger than 1518 bytes. If the frame is smaller than 64 bytes or larger than 1518 bytes, then the switch will discard the frame.

Now imagine that once again you are the bouncer at a nightclub, only this time you have to make sure that the picture matches the person, and you must write down the name and address of everyone before they can enter. Checking IDs this way causes a great deal of delay, and this is how the store-and-forward method of switching works.

Store-and-forward switching has the highest latency of all the switching methods and is the default setting on the 2900 series switches.

Fragment-free (Modified Cut-through/Runt-free)

Since cut-through switching doesn't check for errors and store-and-forward takes too long, we need a method that is both quick and reliable. Using the example of the nightclub bouncer, imagine you are asked to make sure that everyone has an ID and that the picture matches the person. With this method you have made sure everyone is who they say they are, but you do not have to take down all of their information. In switching, this is accomplished by using the fragment-free method of switching, which is the default configuration on lower-level Cisco switches.

https://free learning.it

Fragment-free switching is a modified variety of cut-through switching. The first 64 bytes of a

frame are examined for any errors, and if none are detected, it will pass it on. The reasoning behind this method is that any errors are most likely to be found in the first 64 bytes of a frame.

As mentioned in the previous section, the minimum size of an Ethernet frame is 64 bytes; anything less than 64 bytes is called a “runt” frame. Since every frame must be at least 64 bytes before forwarding, this will eliminate the runts, and that is why this method is also known as “runt-free” switching.

Switching Concepts

The Need for Switches

Before switches were invented, every device on a network would receive data from every other device. Every time a frame was detected on the wire, the PC would have to stop for a moment and check the header to see whether it was the intended recipient. Imagine hundreds of frames going out on the network every minute. Every device would soon grind to a halt. Figure 2.8 below shows all the devices on the network; note that they all have to share the same bandwidth because they are connected by hubs, which only forward frames.

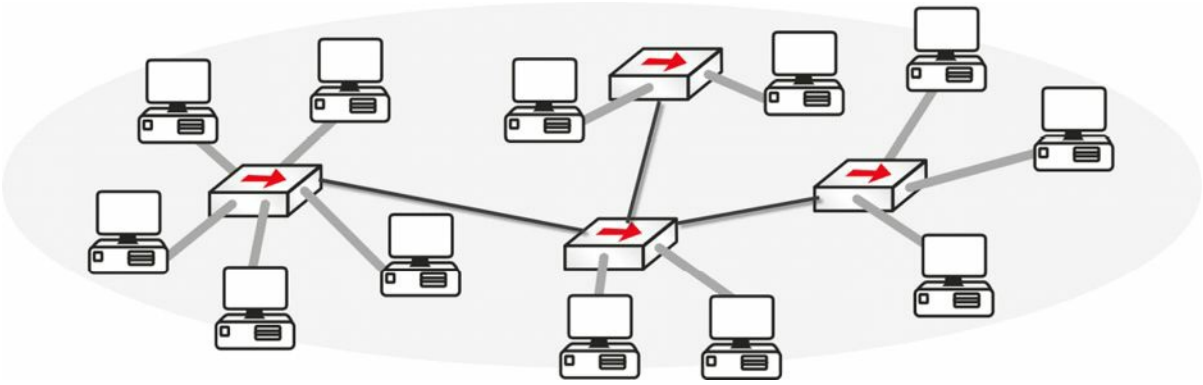
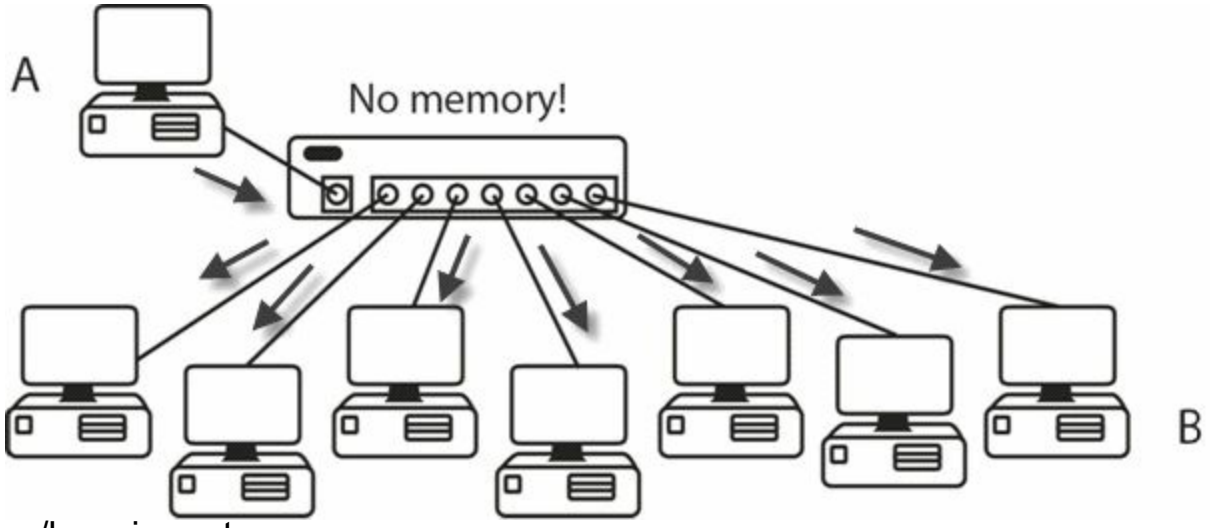


Figure 2.8 – Every Device Listens to Every Other Device

The Problem with Hubs

I mentioned before that hubs are simply multiport repeaters (see Figure 2.9). They take the incoming signal, clean it up, and then send it out of every port with a wire connected. They also create one huge collision domain.



https://t.me/learningnets

Figure 2.9 – Hubs Send the Frame Out of Every Port

Hubs are dumb devices. They have no way of storing MAC addresses, so each time Device A sends a frame to Device B, it is repeated out of every port. Switches, on the other hand, contain a memory chip known as an application-specific integrated circuit (ASIC), which builds a table listing which device is plugged into which port (see Figure 2.10). This table is held in Content Addressable Memory (CAM).

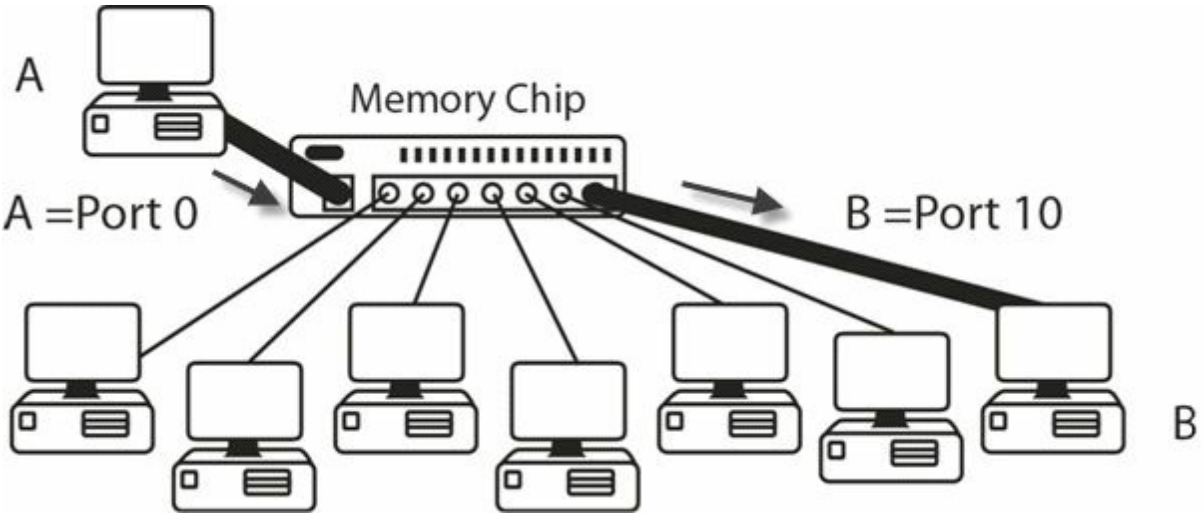


Figure 2.10 – Switches Build a Table of MAC Addresses

When first booted, a switch has no addresses stored in its CAM table (Cisco exams also refer to this as the MAC address table.) Once frames start to pass, the table builds. If no frames pass through the port for a specified period of time, then the entry ages out. In the following output, no frame has been sent through the switch yet:

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

Switch#
```

There is no entry in the switch, but when you ping from one router to another (both attached to the switch), the table entry is built.

```
Router#ping 192.168.1.2
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 62/62/63 ms

Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.c74a.0a01    DYNAMIC     Fa0/1

   1    0060.5c55.da01    DYNAMIC     Fa0/2
```

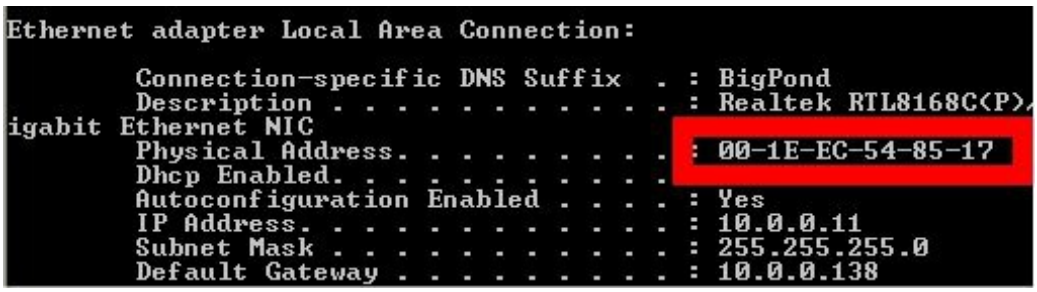
This entry means that any frames destined for the MAC addresses attached to FastEthernet

https://t.me/learningnets

ports 0/1 or 0/2 on the switch will be sent straight out of the relevant port. Any other frames would mean the switch would have to perform a one-off broadcast to see whether the destination devices were attached. You can see this with the period in the first of five pings above. The first ping times out whilst waiting for the switch to broadcast and receive a response from the destination router (80% success rate).

The `show mac-address-table` command is a very important one, so be sure to remember this both for the exam and for the real world.

You should already be aware of what a MAC address actually is, but as a brief refresher – MAC addresses are assigned to all devices to allow communication to take place at the Data Link Layer. You will see them assigned by vendors of Ethernet NICs, Ethernet interfaces on routers, and wireless devices. Here is the MAC address assigned to the Ethernet card on my laptop:



Vendors are assigned an address called an Organizationally Unique Identifier (OUI), which forms the first half of the MAC address. They are then free to create the second half of the address according to their own numbering system. A MAC address is 48 binary bits (we will cover binary and hex later on), so my address above consists of:

OUI	Vendor's Number
24 binary bits	24 binary bits
6 hexadecimal digits	6 hexadecimal digits
00 1E EC	54 85 17

If a switch receives a frame on an interface, it will add the source MAC address to its table. If it knows the destination address, it will forward the frame out of the relevant interface. If the destination address is not known, it will broadcast the frame out of all interfaces, except the interface the frame was received on. If the switch receives a Broadcast frame (i.e., all Fs address), it will forward the frame out of all interfaces, except the interface it was received on. We cover hexadecimal addressing later. The broadcast process is illustrated in Figure 2.11 below:

https://t.me/learningnets

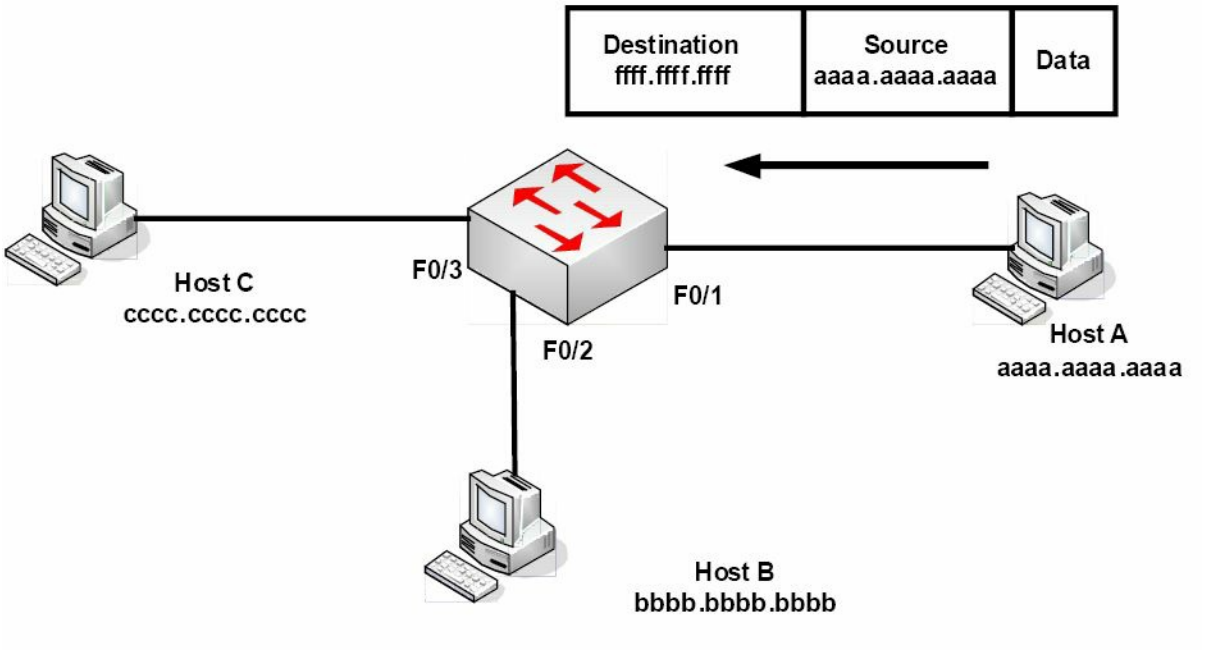


Figure 2.11 – Broadcast Frames Will Be Sent out of All Interfaces

Ethernet Frames

Ethernet has four different frame types available:

- Ethernet 802.3
- Ethernet II
- Ethernet 802.2 SAP
- Ethernet 802.2 SNAP

The first two Ethernet standards deal with the framing used for communication between network cards. They cannot identify the upper-layer protocols, which is where the 802.2 frames come in. You need only concern yourself with the 802.3 frame, which is shown below:

Preamble	SFD	Destination address	Source address	Length	Data	FCS

Figure 2.12 – Ethernet 802.3 Frame

The IEEE 802.3 Ethernet frame consists of specific fields that have been determined by the IEEE committee:

- Preamble – synchronises and alerts the network card for the incoming data
- Start-of-frame delimiter (SFD) – indicates the start of the frame
- Destination address – the destination MAC address (can be Unicast, Broadcast, or Multicast)
- Source address – the MAC address of the sending host
- Length – defines the length of the Data field in the frame
- Data – the payload in the frame (this is the data being transferred)

https://t.me/learningnets

- Frame-check sequence (FCS) – provides a cyclic redundancy check (CRC) on all data in the frame

Initial Switch Configuration

You will connect to a new switch via the console port, the same as with any new router, because in order to connect via Telnet or SSH (more on these later), you will need to have at least a line or two of configuration on the switch already. Many of the initial configuration commands for the switch are the same for an initial router configuration.

It's well worth issuing a `show version` command (see the output below) on any device you connect to for the first time. You will also be expected to know in the exam which `show` command provides which information. Most of the time you won't have access to the emulator to get the answer, so you will have to do it from memory.

The `show version` command provides a lot of useful information, including:

- Switch uptime
- Model
- IOS release
- Reason for last reload
- Interfaces and type
- Memory installed
- Base MAC address

```
Switch>en
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team
ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
System returned to ROM by power-on
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
24 FastEthernet/IEEE 802.3 interface(s)
2 GigabitEthernet/IEEE 802.3 interface(s)
63488K bytes of flash-simulated non-volatile configuration memory.
Base Ethernet MAC Address       : 0090.2148.1456
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Model revision number           : B0
```

https://t.me/learningnets

```
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC1033Z1EY
Top Assembly Part Number        : 800-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01
Switch   Ports  Model           SW Version        SW Image
------   -----  -----           ----------        ---------------
*    1   26     WS-C2960-24TT   12.2              C2960-LANBASE-M
Configuration register is 0xF
```

I know we haven't covered VLANs yet, but for now, consider a VLAN a logical Local Area Network where devices could be anywhere on the network physically but, as far as they are concerned, they are all directly connected to the same switch. In the configuration below, by default, all ports on the switch are left in VLAN 1:

```
Switch#show vlan
VLAN Name             Status    Ports
---- -------          ------    -------------------------------
1    default          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                                Fa0/5, Fa0/6, Fa0/7, Fa0/8,
                                Fa0/9, Fa0/10, Fa0/11, Fa0/12,
                                Fa0/13, Fa0/14, Fa0/15, Fa0/16,
                                Fa0/17, Fa0/18, Fa0/19, Fa0/20,
                                Fa0/21, Fa0/22, Fa0/23, Fa0/24,
```

If you want to add an IP address to the switch in order to connect to it over the network (known as a management address), you simply add an IP address to the VLAN; in this instance, it will be VLAN1:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan1
Switch(config-if)#ip add 192.168.1.3 255.255.255.0
Switch(config-if)# ← hold down Ctrl+Z keys now
Switch#show interface vlan1
Vlan1 is administratively down, line protocol is down
  Hardware is CPU Interface, address is 0010.1127.2388 (bia 0010.1127.2388)
  Internet address is 192.168.1.3/24
```

VLAN1 is shut down by default so you would have to issue a `no shut` command to open it. You should also tell the switch where to send all IP traffic because a Layer 2 switch has no ability to build a routing table; this is illustrated in the output below:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip default-gateway 192.168.1.1
Switch(config)#
```

https://t.me/learningnets

If you have more than one switch on your network, you will want to change the default hostname of your switch so it can be identified more easily when remotely connected (see configuration line below). Imagine trying to troubleshoot five switches from a remote Telnet connection when they are all named “Switch.”

```
Switch(config)#hostname Switch1
```

If you would like to Telnet (or SSH) to the switch over the network, you will need to enable this protocol as well. Remote access to the switch is disabled by default:

```
Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#line vty 0 15
Switch1(config-line)#password cisco
Switch1(config-line)#login
```

Please add the commands above to a switch, and then connect to it from another device (on the same subnet) to test your configuration. This is a fundamental CCNA topic.

VTYs are virtual ports on a router or switch used for Telnet or secure Telnet (SSH) access. They are closed until you configure an authentication method for VTY lines (the simplest way is to add a password to them and the `login` command). You can often see ports 0 to 4, inclusive, or 0 to 15. One way to learn how many you have available is to type a question mark after the number zero, or use the `show line` command, as illustrated in the output below:

```
Router(config)#line vty 0 ?
  <1-15>  Last Line number
Router#show line
   Tty Typ  Tx/Rx    A Modem  Roty AccO AccI   Uses  Noise  Overruns Int
*   0 CTY            -    -     -    -    -      0     0    0/0
    1 AUX 9600/9600  -    -     -    -    -      0     0    0/0      *
    2 VTY            -    -     -    -    -      2     0    0/0
    3 VTY            -    -     -    -    -      0     0    0/0
    4 VTY            -    -     -    -    -      0     0    0/0
    5 VTY            -    -     -    -    -      0     0    0/0
    6 VTY            -    -     -    -    -      0     0    0/0
```

CTY is the console line, whilst VTY lines are for Telnet connections and AUX is the auxilliary port.

For a more secure access method, you can permit only SSH connections into the switch, which means the traffic will be encrypted. You will need a security image on your switch in order for this to work, as shown in the output below:

```
Switch1(config-line)#transport input ssh
```

Now, Telnet traffic will not be permitted into the VTY ports.

Please configure all of these commands on a switch. Just reading them will not help you recall them come exam day!

Virtual Local Area Networks (VLANs)

As you have already seen, a switch breaks a collision domain. Taken a step further, a router breaks a Broadcast domain, which means a network would look something like the following figure:

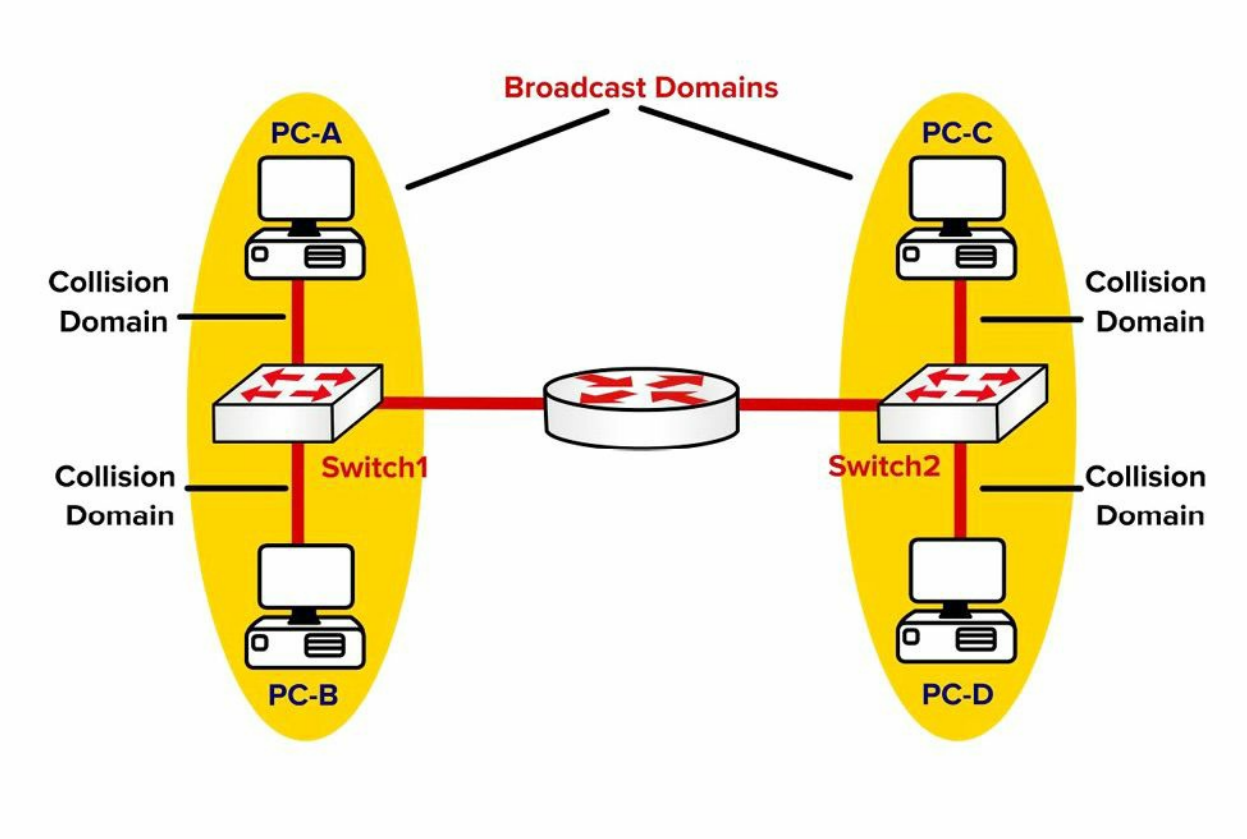
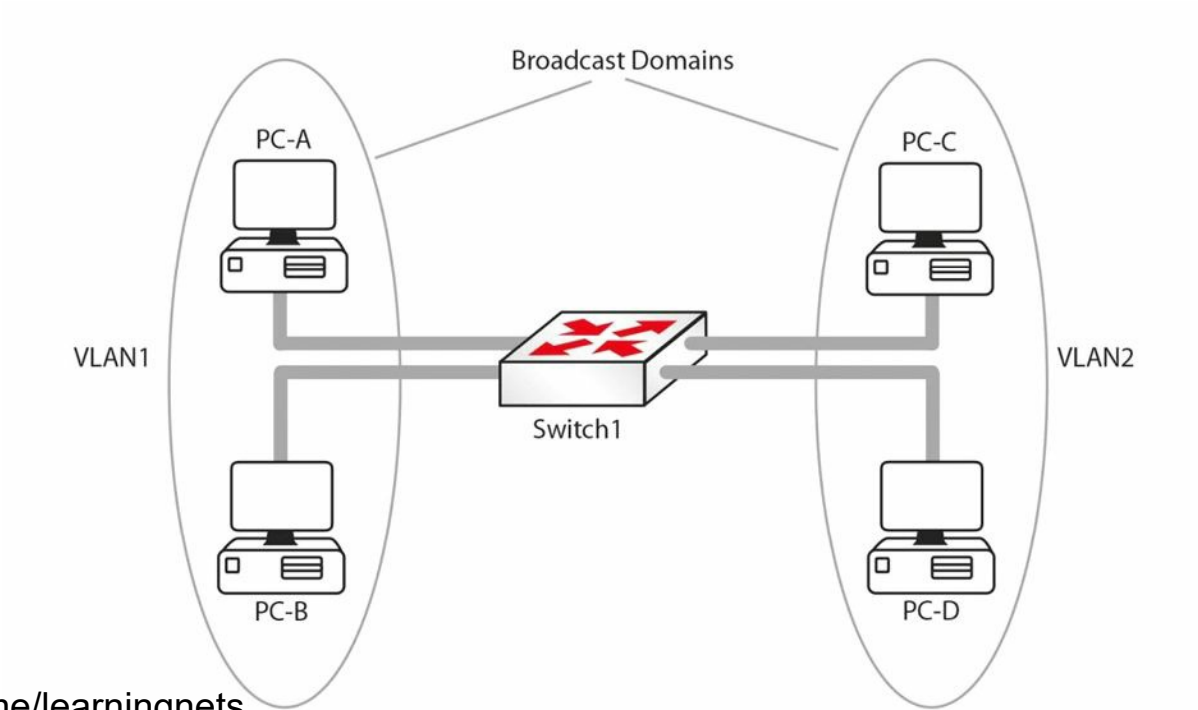


Figure 2.13 – Routers Separate Broadcast Domains

Before we continue, let's discuss what a LAN really is. A LAN is essentially a Broadcast domain. In the network shown in Figure 2.13, if PC-A sends a Broadcast, it will be received by PC-B but not by PC-C or PC-D. This is because the router breaks the Broadcast domain. Now you can use virtual LANs (VLANs) to put switch ports into different Broadcast domains, as illustrated in the figure below:



https://t.me/learningnets

Figure 2.14 – Broadcast Domains with VLAN

In Figure 2.14, the Layer 2 network has been divided into two Broadcast domains using VLANs. Now a Broadcast sent by PC-A will be received by PC-B but not by PC-C and PC-D. Without VLANs PC-C and PC-D would have received the Broadcasts sent by PC-A. The following are some advantages of VLANs:

- Containing Broadcasts within a smaller group of devices will make the network faster.
- Saves resources on devices because they process less Broadcasts.
- Added security by keeping devices in a certain group (or function) in a separate Broadcast domain. A group, as implied here, can mean department, security level, etc. For example, devices belonging to a development or testing lab should be kept separate from the production devices.
- Flexibility in expanding a network across a geographical location of any size. For example, it does not matter where in the building a PC is. It thinks it is on the same segment of the network as any other PC configured to be in the same VLAN. In Figure 2.15 below, all hosts in VLAN 1 can talk to each other, even though they are on different floors. The VLAN is transparent or invisible to them.

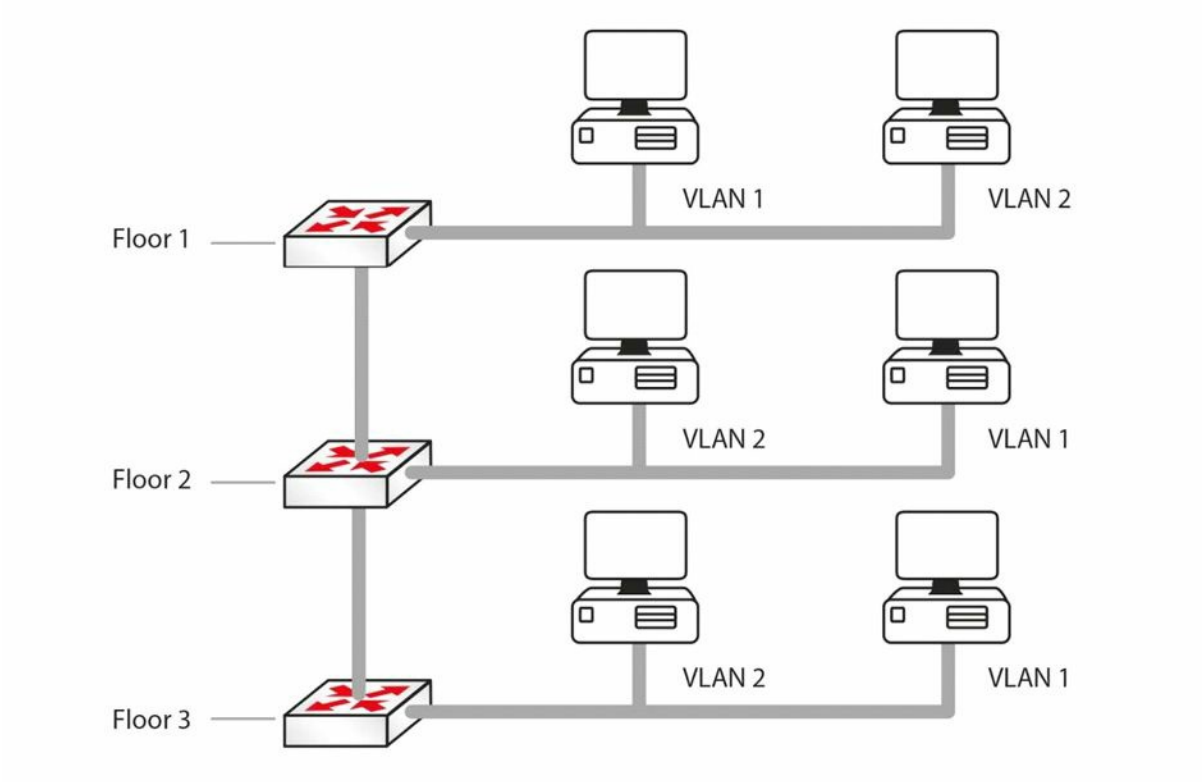


Figure 2.15 – VLANs Remove the Physical Boundaries from a LAN

VLAN Marking

Although vendors used individual approaches to create VLANs, a multi-vendor VLAN must be carefully handled to deal with interoperability issues. For example, Cisco developed the ISL standard that operates by adding a new 26-byte header, plus a new 4-byte trailer, encapsulating the original frame. To solve incompatibility problems, IEEE developed 802.1Q, a vendor-independent method to create interoperable VLANs.

https://techlearning.net

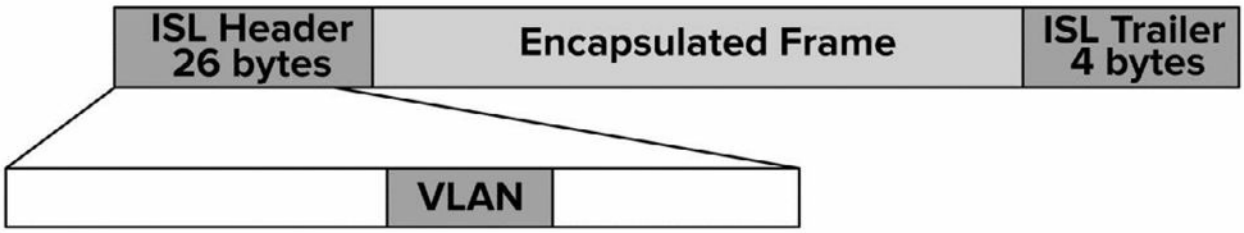


Figure 2.16 – ISL Marking Method

802.1Q is often referred to as frame tagging because it inserts a 32-bit header, called a "tag," into the original frame, after the Source Address field, without modifying other fields. The next 2 bytes after the Source Address field hold a registered Ethernet type value of 0x8100, which implies the frame contains an 802.1Q header. The next 3 bits represent the 802.1P User Priority field and are used as Class of Service (CoS) bits in Quality of Service (QoS) techniques. The next subfield is a 1-bit Canonical Format Indicator, followed by the VLAN ID (12 bits). This gives us a total of 4096 VLANs when using 802.1Q.

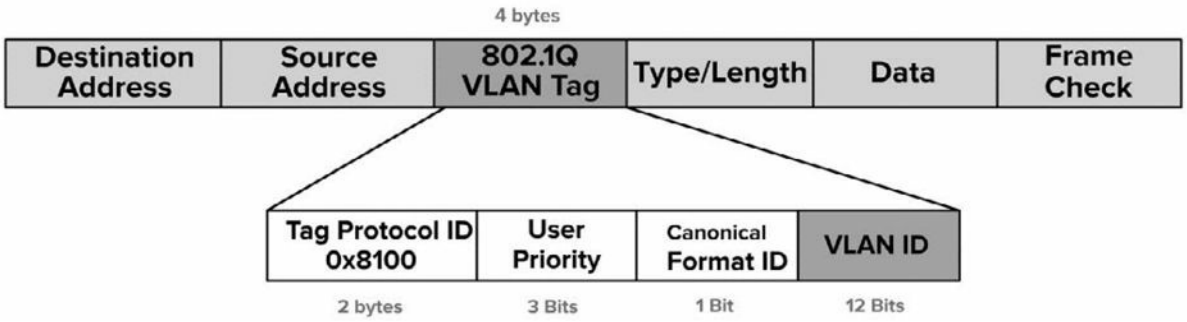


Figure 2.17 – 802.1Q Marking Method

A port that carries data from multiple VLANs is called a trunk. It can use either the ISL or the 802.1Q protocols. A special concept in the 802.1Q world is "native VLAN." This is a particular type of VLAN in which frames are not tagged. The native VLAN's purpose is to allow a switch to use 802.1Q trunking (multiple VLANs on a single link) on an interface, but if the other device does not support trunking, the traffic for the native VLAN can still be sent over the link. If a switch receives any untagged traffic over a trunk link, it will assume it is destined for the native VLAN. Cisco uses VLAN 1 as the default native VLAN.

VLAN Membership

There are two common ways to associate ports with VLANs – statically or dynamically.

With static VLAN assignment or configuration, the ports on the switch are configured by the network administrator to be in different VLANs, and the relevant device is then connected to the port. If the user needs to move to another part of the building, this will require the administrator to change the configuration on the switch. All switch ports belong to VLAN 1 by default.

Dynamic VLAN assignment allows devices to join a specific VLAN based on the MAC address of the device. This gives the administrator the flexibility to allow users to connect to any switch or move around the building without having to change the configuration on the switch. This is achieved using a VLAN Management Policy Server (VMPS).

https://t.me/learningnets

Farai says – “Ports are assigned to VLANs and devices are connected to ports.”

Please note that since each VLAN is a different Broadcast domain, this means:

- Hosts in one VLAN cannot reach hosts in another VLAN, by default
- A Layer 3 device is needed for inter-VLAN communication (this will be covered later)
- Each VLAN needs its own subnet, for example, VLAN 1 – 192.168.1.0/24, VLAN 2 – 192.168.2.0/24
- All hosts in a VLAN should belong to the same subnet

VLAN Links

We know that one switch can have hosts connected to multiple VLANs. But what happens when traffic goes from one host to another? For example, in Figure 2.15 above, when the host in VLAN 1 on Floor 1 tries to reach the host in VLAN 1 on Floor 2, how will the switch on Floor 2 know which VLAN the traffic belongs to?

Switches use a mechanism called “frame tagging” to keep traffic on different VLANs separate. The switch adds a header on the frame, which contains the VLAN ID. In Figure 2.15, the switch on Floor 1 will tag the traffic originating from VLAN 2 and pass it to Switch 2, which will see the tag and know that the traffic needs to be kept within that VLAN. Such tagged traffic can only flow across special links called trunk links. VLAN 1 is usually designated as the native VLAN and traffic on the native VLAN is not tagged. We will cover native VLANs in more detail later.

Switch ports (within the scope of the CCNA exam) can be divided into the following:

- Access links or ports
- Trunk links or ports
- Dynamic (this will be discussed shortly)

Access Links

A switch port, which is defined as an access link, can be a member of only one VLAN. The device connected to the access link is not aware of the existence of any other VLANs. The switch will add a tag to a frame as it enters an access link from the host and remove the tag when a frame exits the switch access link towards the host. Access links are used to connect to hosts, but they can also be used to connect to a router. Trunk links are covered in the following section.

Trunking

A switch port usually will connect either to a host on the network or to another network switch, router, or server. If this is the case, then the link may need to carry traffic from several VLANs. In order to do this, each frame needs to identify which VLAN it is from. This identification method is known as frame tagging, and all frames are tagged before passing over the trunk link, apart from the native VLAN. The tag in the frame contains the VLAN ID. When the frame reaches the switch where the destination host resides, the tag is removed.

https://t.me/learningnets

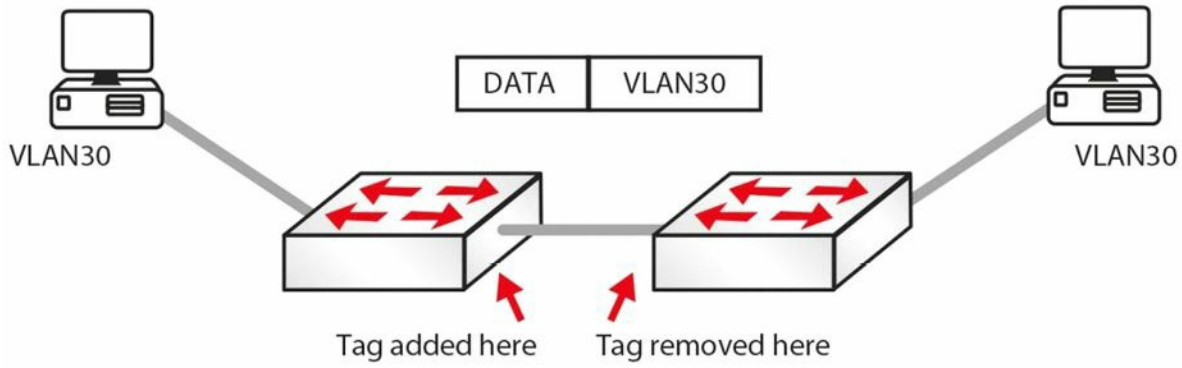


Figure 2.18 – VLAN Tagging

VLAN trunks are used to carry data from multiple VLANs. To differentiate one VLAN frame from another, all frames sent across a trunk link are specially tagged so that the destination switch knows which VLAN the frame belongs to. ISL and 802.1Q are the two primary encapsulation methods which can be used to ensure that VLANs that traverse a switch trunk link can be uniquely identified.

ISL is Cisco proprietary; however, the model tested in the CCNA exam is the 2960 switch, which only recognises 802.1Q. We cover it here for completeness and in case you have to configure an older switch model.

Farai says – "All new switches now default to 802.1Q. ISL is being deprecated."

802.1Q differs from ISL in several ways. The first significant difference is that 802.1Q supports up to 4096 VLANs, whereas ISL supports up to 1000. Another significant difference is that of the native VLAN concept used in 802.1Q. By default, all frames from all VLANs are tagged when using 802.1Q. The only exception to this rule is frames that belong to the native VLAN, which are not tagged.

However, keep in mind that it is possible to specify which VLAN will not have frames tagged by specifying that VLAN as the native VLAN on a particular trunk link. For example, to prevent tagging of frames in VLAN 400 when using 802.1Q, you would configure that VLAN as the native VLAN on a particular trunk. IEEE 802.1Q native VLAN configuration will be illustrated in detail later.

The following summarises some features of 802.1Q:

- Supports up to 4096 VLANs
- Uses an internal tagging mechanism, modifying the original frame
- Open standard protocol developed by the IEEE
- Does not tag frames on the native VLAN; however, all other frames are tagged

The following is a short sample configuration of a switch. I have included the `switchport` command, which tells the switch to act as a switch port for Layer 2, as opposed to Layer 3.

```
Sw(config)#interface FastEthernet 0/1
Sw(config-if)#switchport
```

https://t.me/learningnets

```
Sw(config-if)#switchport mode trunk
Sw(config-if)#switchport trunk encapsulation dot1q
Sw(config-if)#exit
```

Of course, on a 2960 switch, the `encapsulation` command won't be recognised because there is only one type available. You will need to set the interface as a trunking interface when connecting to another switch to allow VLANs to be tagged. The same thing goes for the `switchport` command. Again, I cover this because in the real world you may well have to configure a Layer 3 switch, and if we stuck strictly to the 2960 model, you may become confused, which we don't want!

A trunk link on a switch can be in one of five possible modes:

- On – forces the port into permanent trunking mode. The port becomes a trunk, even if the connected device does not agree to convert the link into a trunk link.
- Off – the link is not used as a trunk link, even if the connected device is set to "trunk."
- Auto – the port is willing to become a trunk link. If the other device is set to "on" or "desirable," then the link becomes a trunk link. If both sides are left as "auto," then the link will never become a trunk, as neither side will attempt to convert.
- Desirable – the port actively tries to convert to a trunk link. If the other device is set to "on," "auto," or "desirable," then the link will become a trunk link.
- No-negotiate – prevents the port from negotiating a trunk connection. It will be forced into an access or trunk mode as per the configuration.

Configuring VLANs

Now that you understand VLANs and trunk links, let's configure the network shown in Figure 2.19 below. You will need to configure the switches such that the hosts on fa0/1 are in VLAN 5 and the link on port fa0/15 is a trunk link.

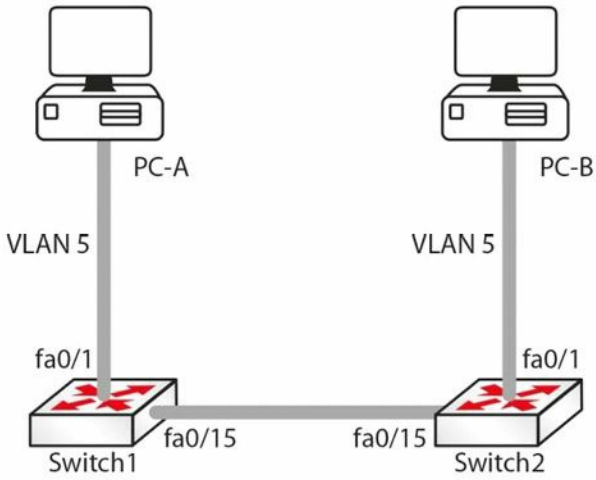


Figure 2.19 – Test Network

Before assigning ports to VLANs, the VLAN itself must be created using the `vlan <vlan#>` global configuration command. This will put you into VLAN Configuration mode, where a descriptive

name can be given to the VLANs. Here is an example:

```
Switch1(config)#vlan 5
Switch1(config-vlan)#name RnD

Switch2(config)vlan 5
Switch2(config-vlan)#name RnD
```

To see which VLANs exist on a switch, use the `show vlan` command. The output will be similar to the one below:

```
Switch1#show vlan

VLAN  Name   Status  Ports

----  --------  -------  -----------------------------------------

1  default   active   Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9,
Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa/15, Fa0/16, Fa0/17, Fa0/18


...

[Truncated Output]

...


5   RnD   active


...

[Truncated Output]
```

Let's assign port fa0/1 to VLAN 5 using the `switchport access vlan [vlan#]` interface configuration command:

```
Switch1(config)#int fa0/1

Switch1(config-if)#switchport access vlan 5


Switch2(config)#int fa0/1
Switch2(config-if)#switchport access vlan 5
```

On a Layer 3-capable switch, such as the 3560, you would have to set the port manually to access it with the `switchport mode access` command before putting it into a VLAN. Now let's look at the output for the `show vlan` command:

```
Switch1#show vlan


VLAN  Name   Status    Ports

----  ----  -----    -----------------------------------------

1   default  active     Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7,

  Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13,

  Fa0/14, Fa/15, Fa0/16, Fa0/17, Fa0/18

...

[Truncated Output]
```

https://t.me/learningnets

```
...
```

```
5  RnD  active  Fa0/1
...
[Truncated Output]
```

Note that fa0/1 is now assigned to VLAN 5. Let's configure interface fa0/15 on both switches as trunk links. It should be noted here that the default mode on (the 3550 model) switch ports is desirable (on the 3560 model it's auto, so check your platform notes). Dynamic Trunking Protocol (DTP) will cause fa0/15 on both switches to become ISL trunk links. We will cover DTP in the next lesson, but I wanted to mention it here briefly. This can be verified using the `show interface trunk` command:

```
Switch1#show interface trunk

Port    Mode    Encapsulation     Status    Native vlan
Fa0/15     desirable    n-isl    trunking     1
```

Note that the mode is desirable and the encapsulation is ISL ("n" stands for negotiated).

The following output shows how to configure the trunk to use ISL trunking:

```
Switch1(config)#interface fa0/15
Switch1(config-if)#switchport trunk encapsulation isl
Switch1(config-if)#switchport mode trunk
Switch2(config)#interface fa0/15
Switch2(config-if)#switchport trunk encapsulation isl
Switch2(config-if)#switchport mode trunk
```

The `switchport trunk encapsulation` command sets the trunking protocol on the port, and the `switchport mode trunk` command sets the port to trunking. The output for the `show interface trunk` command will now look like this:

```
Switch2#show interface trunk

Port    Mode    Encapsulation    Status    Native vlan
Fa0/15    on    isl    trunking    1
```

Note that the encapsulation is now ISL instead of N-ISL. This is because this time the protocol was not negotiated but configured on the interface.

IMPORTANT NOTE: Trunk encapsulation needs to be configured on the switch port before setting it to trunk mode. Please note that this does not apply to switch model 2960 (currently used for the CCNA syllabus), which can only use dot1q (another name for 802.1Q) encapsulation. For this reason, the `switchport trunk encapsulation` command will not work on the 2960 switch.

Similarly, you can configure the switch port to use 802.1Q instead of ISL, as illustrated in the output below:

```
Switch1(config)#interface fa0/15
```

https://t.me/learningnets

```
Switch1(config-if)#switchport trunk encapsulation dot1q
Switch1(config-if)#switchport mode trunk

Switch2(config)#interface fa0/15
Switch2(config-if)#switchport trunk encapsulation dot1q
Switch2(config-if)#switchport mode trunk
```

The `show interface trunk` output now looks like this:

```
Switch2#show interface trunk

Port  Mode  Encapsulation  Status  Native vlan
Fa0/15  on  802.1q  trunking  1
```

Note that the native VLAN is 1. That is the default native VLAN on an 802.1Q trunk and it can be changed using the `switchport trunk native vlan <vlan#>` command. The native VLAN of each port on the trunk must match. This command is part of the CCNA syllabus and is considered a security measure.

IMPORTANT NOTE: Switches remember all VLAN info, even when reloaded. If you want your switch to boot with a blank configuration, then you will need to issue the `delete vlan.dat` command on your switch, as shown in the output below. This applies to live switches only, not switch emulators such as Packet Tracer.

```
SwitchA#dir flash:
Directory of flash:/

    1  -rw-     3058048          <no date>  c2960-i6q4l2-mz.121-22.EA4.bin
    2  -rw-         676          <no date>  vlan.dat
64016384 bytes total (60957660 bytes free)
SwitchA#
SwitchA#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
SwitchA#dir flash:
Directory of flash:/
    1  -rw-     3058048          <no date>  c2960-i6q4l2-mz.121-22.EA4.bin
64016384 bytes total (60958336 bytes free)
SwitchA#
```

Basic Switching Troubleshooting

In theory, once a device is configured and working it should stay that way, but, often, you will be working on a network which you didn't configure, or you will be working on a shift pattern supporting many unfamiliar networks on which changes have been made, causing one or more issues for the company. I suggest you revisit this section after completing a few labs in this guide

as the days progress.

Common Switch Issues

Can't Telnet to Switch

The first question is was Telnet ever working? If it was and is no longer, then perhaps somebody has made a change on the switch, reloaded it, and lost the configuration, or a device is now blocking Telnet traffic somewhere on the network:

```
Switch#telnet 192.168.1.1
Trying 192.168.1.1 ...Open
[Connection to 192.168.1.1 closed by foreign host]
```

The first thing to check is whether Telnet has actually been enabled on the switch (see the output below). Around 80% of errors on the network are due to silly mistakes or oversights, so never presume anything, and check out everything personally, rather than relying on other people's words.

A simple `show run` command will reveal the switch configuration. Under the `vty` lines, you will see whether Telnet has been enabled. Note that you will need to have the `login` or `login local` (or configured AAA, which is beyond the scope of the CCNA exam) command under the `vty` lines and the `password` command, as shown below:

```
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
```

The `login local` command tells the switch or router to look for a username and password configured on it, as illustrated in the output below:

```
Switch1#sh run
Building configuration...
Current configuration : 1091 bytes!
version 12.1
hostname Switch1
username david privilege 1 password 0 football
line vty 0 4
password cisco
login local
line vty 5 15
password cisco
login local

...
[Truncated Output]
```

Can't Ping the Switch

Find out why the person wants to ping the switch in the first place. If you do want to ping a switch, there needs to be an IP address configured on it; in addition, the switch needs to know

https://t.me/learningnets

how to get traffic back out (the default gateway).

Can't Ping through the Switch

If a ping through the switch is unsuccessful, then check to ensure that the end devices are in the same VLAN. Each VLAN is considered a network and for this reason must have a different address range from any other VLAN. In order for one VLAN to reach another, a router must route the traffic.

Interface Issues

By default, all router interfaces are closed to traffic and switch interfaces are open. If you find that your switch has had its interfaces administratively shut, to open it, the interface must be set with the `no shut` interface-level command:

```
Switch1(config)#int FastEthernet0/3
Switch1(config-if)#no shut
```

Layer 2 interfaces can be set in three modes: trunk, access, or dynamic. Trunk mode lets the switch connect to another switch or a server. Access mode is for an end device, such as a PC or a laptop. Dynamic mode lets the switch detect which setting to select.

The default on platforms such as the 3550 model switch is usually dynamic desirable, but please check your model's settings and release notes on Cisco.com. For the CCNA exam, you will be asked to configure a 2960 model switch. It will select the mode dynamically unless you hard set it to trunk or access mode:

```
Switch1#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
```

The default can easily be changed, as shown in the output below:

```
Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#int FastEthernet0/1
Switch1(config-if)#switchport mode ?

  access   Set trunking mode to ACCESS unconditionally
  dynamic  Set trunking mode to dynamically negotiate access or           trunk mode
  trunk    Set trunking mode to TRUNK unconditionally

Switch1(config-if)#switchport mode trunk
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

Switch1(config-if)#^Z
Switch1#
%SYS-5-CONFIG_I: Configured from console by console
Switch1#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
```

More Interface Issues

Switch port default settings are auto-detect duplex and auto-detect speed. If you plug a

https://t.me/learningnets

10Mbps device into a switch running at half duplex (if you could even find such a device), then the port should detect this and work. This isn't always the case, though, so the generic advice is to hard set the switch port speed and duplex, as illustrated in the output below:

```
Switch1#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
```

```
Switch1#show interface FastEthernet0/2
FastEthernet0/2 is up, line protocol is up (connected)
  Hardware is Lance, address is 0030.f252.3402 (bia 0030.f252.3402)
BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
```

```
Switch1(config)#int fast 0/2
Switch1(config-if)#duplex ?
  auto  Enable AUTO duplex configuration
  full  Force full-duplex operation
  half  Force half-duplex operation

Switch1(config-if)#speed ?
  10    Force 10Mbps operation
  100   Force 100Mbps operation
  auto  Enable AUTO speed configuration
```

Signs of duplex mismatches (apart from error messages) include input and CRC errors on the interface, as illustrated in the output below. Please also see the Layer 1 and Layer 2 Troubleshooting sections in Day 15 of the ICND1 section.

```
Switch#show interface f0/1
FastEthernet0/1 is down, line protocol is down (disabled)
  Hardware is Lance, address is 0030.a388.8401 (bia 0030.a388.8401)
BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
```

https://t.me/learningnets

```
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
755 input errors, 739 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
0 output errors, 0 collisions, 10 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Hardware Issues

As with any electrical device, ports on a switch can fail or work only part of the time, which is harder to troubleshoot. Engineers often test the interface by plugging a known working device into another port on the switch. You can also bounce a port, which means applying the `shut` command and then the `no shut` command to it. Swapping the Ethernet cable is also a common troubleshooting step. Other common switch problems and solutions are shown in Figure 2.20 below.

Please check the documentation for your switch because, as well as featuring system and port LEDs, each port can display flashing or solid red, amber, and green, indicating normal function or port/system issues.

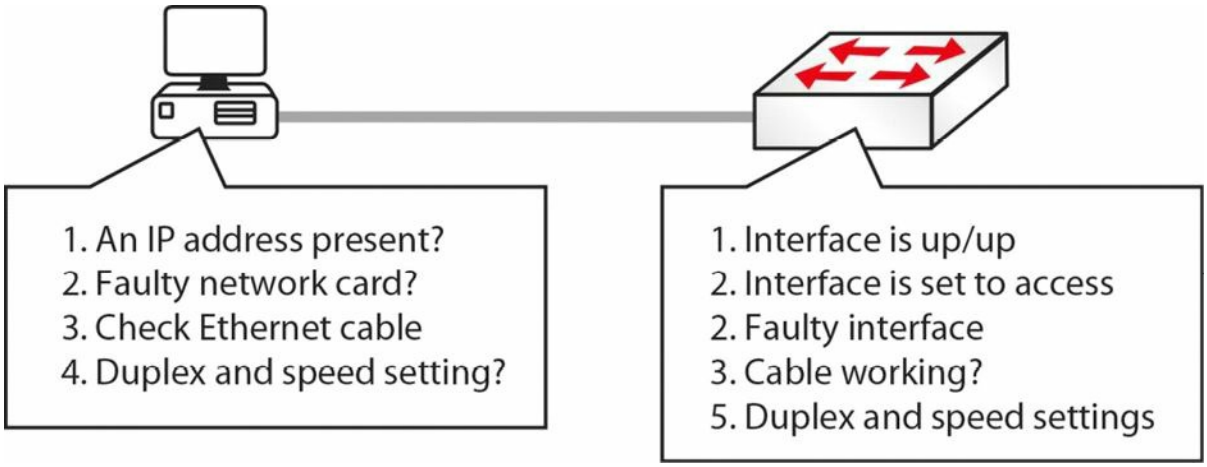


Figure 2.20 – Common Switch Problems and Solutions

VLAN Assignment Issues

Networks in small environments are relatively easy to manage because a limited number of features need to be implemented in order to achieve the business's goals. However, in an enterprise environment you won't be using small workgroup switches and SOHO devices. Rather, you will use high-end devices that are capable of optimising the traffic flow by offering a number of advanced functionalities.

One particular feature that might be configured in such an environment is logically separating different network areas using VLANs. Issues can appear when you have configuration issues related to a particular VLAN and this can become difficult to troubleshoot. One way of doing this is analysing the entire configuration on the switch and trying to identify the problem.

https://t.me/Earningnets

VLAN-related problems are usually detected by observing the lack of connectivity between network hosts (e.g., a user cannot ping a server), even though Layer 1 seems to operate without problems. One important characteristic of VLAN-related problems is that they do not generate any performance degradation on the network. If you misconfigure a VLAN, the connection will simply not work, especially considering that they usually separate IP subnets so that only devices within the same VLAN will be able to communicate with each other.

The first step in troubleshooting VLAN problems is to review the documentation and the logical diagrams developed in the design phase so you can identify the span area for each VLAN, including the associated devices and ports on each switch. The next step is to inspect each switch configuration and try to find the problem by comparing them with the documented solution.

You should also verify the IP addressing scheme. If you are statically assigning IP addresses to devices, you may want to go back and check the device to ensure that it has the proper IP address and subnet mask combination. If there are any mistakes in the IP addressing scheme, like configuring devices on the wrong network or with a wrong subnet mask/default gateway, then you are going to have connectivity problems, even though you have the correct VLAN configured on the switch.

You will also want to confirm that the trunk configuration on the switches is correct. If you have multiple switches, there are usually uplinks between them and VLANs carried across those uplinks. These inter-switch links are often configured as trunks to allow communication across multiple VLANs. The VLAN has to be a member of the trunk group if data is to be sent from one switch to the other, so you also have to make sure that the switch configuration on both sides is set up properly.

Finally, if you move a device to another VLAN, you will have to make changes to both the switch and the client because the client will have a different IP address in a different IP subnet as a result of that move.

If you follow all of these VLAN troubleshooting methods, you can be sure that when plugging in devices for the first time or moving them from VLAN to VLAN, you will have the exact connectivity you desired.

https://t.me/learningnets

Day 2 Questions

1. Switches contain a memory chip known as an _____, which builds a table listing which device is plugged into which port.
2. The _____ _____-_____-_____ command displays a list of which MAC addresses are connected to which ports.
3. Which two commands add an IP address to the VLAN?
4. Which commands will enable Telnet and add a password to the switch Telnet lines?
5. How do you permit only SSH traffic into your Telnet lines?
6. What is the most likely cause of Telnet to another switch not working?
7. Switches remember all VLAN info, even when reloaded. True or False?
8. A switch interface can be in which of three modes?
9. How do you set a switch to be in a specific mode?
10. Which commands will change the switch duplex mode and speed?

https://t.me/learningnets

Day 2 Answers

1. ASIC.
2. `show mac-address-table`.
3. The `interface vlan x` command and the `ip address x.x.x.x` command.
4.
```
Switch1(config)#line vty 0 15
Switch1(config-line)#password cisco
Switch1(config-line)#login
```
5. Use the `Switch1(config-line)#transport input ssh` command.
6. The authentication method is not defined on another switch.
7. True.
8. Trunk, access, or dynamic mode.
9. Apply the `switchport mode <mode>` command in Interface Configuration mode.
10. The `duplex` and `speed` commands.

https://t.me/learningnets

Day 2 Lab

Switching Concepts Lab

Please log on to a Cisco switch and enter the commands explained in this module. This should include:

- ☐ Configure different port speeds/auto-negotiation on various switch ports
- ☐ Verify the port parameters with the `show run` and the `show interface` commands
- ☐ Issue a `show version` command to see the hardware details and IOS version
- ☐ Verify the switch MAC address table
- ☐ Configure a password on the VTY lines
- ☐ Define a couple of VLANs and assign names to them
- ☐ Assign a VLAN to a port configured as switchport access
- ☐ Configure a port as a trunk (ISL and 802.1Q) and assign VLANs to the trunk
- ☐ Verify VLAN configuration using the `show vlan` command
- ☐ Verify interface trunking and VLAN configuration using the `show interface switchport` command and the `show interface trunk` command
- ☐ Delete the “vlan.dat” file

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 3 – Trunking, DTP, and Inter-VLAN Routing

Day 3 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's lab
- Read the ICND1 cram guide

You will only encounter networks using one switch in the smallest of offices, whereas you will usually find multiple switches forming part of the network infrastructure. This brings its own set of configuration challenges, which will require a good understading of trunking and associated issues. Cisco consider the ability to install and troubleshoot multiple switch connections a fundamental CCNA-level topic.

Today you will learn about the following:

- Trunking
- Dynamic Trunking Protocol (DTP)
- Inter-VLAN Routing

This module maps to the following ICND1 syllabus requirements:

- Configure and verify trunking on Cisco switches
- DTP
- Auto-negotiation
- Configure and verify inter-VLAN routing (router-on-a-stick)
  - Subinterfaces
  - Upstream routing
  - Encapsulation
- Configure SVI interfaces

Configuring and Verifying Trunk Links

A trunk is a switch port that can carry multiple traffic types, each tagged with a unique VLAN ID. As data is switched across the trunk port or trunk link, it is tagged (or coloured) by the egress switch trunk port, which allows the receiving switch to identify that it belongs to a particular VLAN. On the receiving switch ingress port, the tag is removed and the data is forwarded to the intended destination.

The first configuration task when implementing VLAN trunking in Cisco IOS Catalyst switches is to configure the desired interface as a Layer 2 switch port. This is performed by issuing the `switchport` interface configuration command.

https://t.me/learningnets

NOTE: This command is required only on Layer 3-capable or Multilayer switches. It is not applicable to Layer 2-only switches, such as the Catalyst 2960 series. A switch would need to support the command `ip routing` in order to be considered Layer 3 capable.

The second configuration task is to specify the encapsulation protocol that the trunk link should use. This is performed by issuing the `switchport trunk encapsulation [option]` command. The options available with this command are as follows:

```
Switch(config)#interface FastEthernet1/1
Switch (config-if)#switchport trunk encapsulation ?
dot1q - Interface uses only 802.1q trunking encapsulation when trunking
isl - Interface uses only ISL trunking encapsulation when trunking
negotiate - Device will negotiate trunking encapsulation with peer on interface
```

The `[dot1q]` keyword forces the switch port to use IEEE 802.1Q encapsulation. The `[isl]` keyword forces the switch port to use Cisco ISL encapsulation. The `[negotiate]` keyword is used to specify that if the Dynamic Inter-Switch Link Protocol (DISL) and the Dynamic Trunking Protocol (DTP) negotiation fails to successfully agree on the encapsulation format, then ISL is the selected format. DISL simplifies the creation of an ISL trunk from two interconnected FastEthernet devices. DISL minimises VLAN trunk configuration procedures because only one end of a link needs to be configured as a trunk.

DTP is a Cisco proprietary point-to-protocol that negotiates a common trunking mode between two switches. DTP will be described in detail later. The following output illustrates how to configure a switch port to use IEEE 802.1Q encapsulation when establishing a trunk:

```
Switch (config)#interface FastEthernet1/1
Switch (config-if)#switchport
Switch (config-if)#switchport trunk encapsulation dot1q
```

This configuration can be validated via the `show interfaces [name] switchport` command, as illustrated in the following output:

```
Switch#show interfaces FastEthernet1/1 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
...
[Truncated Output]
```

https://t.me/learningnets

The third trunk port configuration step is to implement configuration to ensure that the port is

designated as a trunk port. This can be done in one of two ways:

- Manual (static) trunk configuration
- Dynamic Trunking Protocol (DTP)

Manual (Static) Trunk Configuration

The manual configuration of a trunk is performed by issuing the `switchport mode trunk` interface configuration command on the desired switch port. This command forces the port into a permanent (static) trunking mode. The following configuration output shows how to configure a port statically as a trunk port:

```
VTP-Server(config)#interface FastEthernet0/1
VTP-Server(config-if)#switchport
VTP-Server(config-if)#switchport trunk encapsulation dot1q
VTP-Server(config-if)#switchport mode trunk
VTP-Server(config-if)#exit
VTP-Server(config)#
```

Feel free to ignore the `switchport` command if you are using a lower-end switch (the above output was from a Cat6K switch). This configuration can be validated via the `show interfaces [name] switchport` command, as illustrated in the following output:

```
VTP-Server#show interfaces FastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
...
[Truncated Output]
```

Although manual (static) configuration of a trunk link forces the switch to establish a trunk, Dynamic ISL and Dynamic Trunking Protocol (DTP) packets will still be sent out of the interface. This is performed so that a statically configured trunk link can establish a trunk with a neighbouring switch that is using DTP, as will be described in the following section. This can be validated in the output of the `show interfaces [name] switchport` command illustrated below:

```
VTP-Server#show interfaces FastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
```

https://t.me/learningnets

```
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
...
[Truncated Output]
```

In the output above, the text in bold indicates that despite the static configuration of the trunk link, the port is still sending out DTP and DISL packets. In some cases, this is considered undesirable. Therefore, it is considered good practice to disable the sending of DISL and DTP packets on a port statically configured as a trunk link by issuing the `switchport nonegotiate` interface configuration command, as illustrated in the following output:

```
VTP-Server(config)#interface FastEthernet0/1
VTP-Server(config-if)#switchport
VTP-Server(config-if)#switchport trunk encapsulation dot1q
VTP-Server(config-if)#switchport mode trunk
VTP-Server(config-if)#switchport nonegotiate
VTP-Server(config-if)#exit
VTP-Server(config)#
```

Again, the `show interfaces [name] switchport` command can be used to validate the configuration, as follows:

```
VTP-Server#show interfaces FastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
...
[Truncated Output]
```

Dynamic Trunking Protocol (DTP)

DTP is a Cisco proprietary point-to-protocol that negotiates a common trunking mode between two switches. This dynamic negotiation can also include trunking encapsulation. The two DTP modes that a switch port can use, depending upon the platform, are as follows:

- Dynamic desirable
- Dynamic auto

https://t.me/learningnets

When using DTP on two neighbouring switches, if the switch port defaults to a dynamic desirable state, the port will actively attempt to become a trunk. If the switch port defaults to a dynamic auto state, the port will revert to being a trunk only if the neighbouring switch is set to dynamic desirable mode.

Figure 3.1 below illustrates the DTP mode combinations that will result in a trunk either being established or not being established (in this case they are all established; see note after Figure 3.2) between two Cisco Catalyst switches:

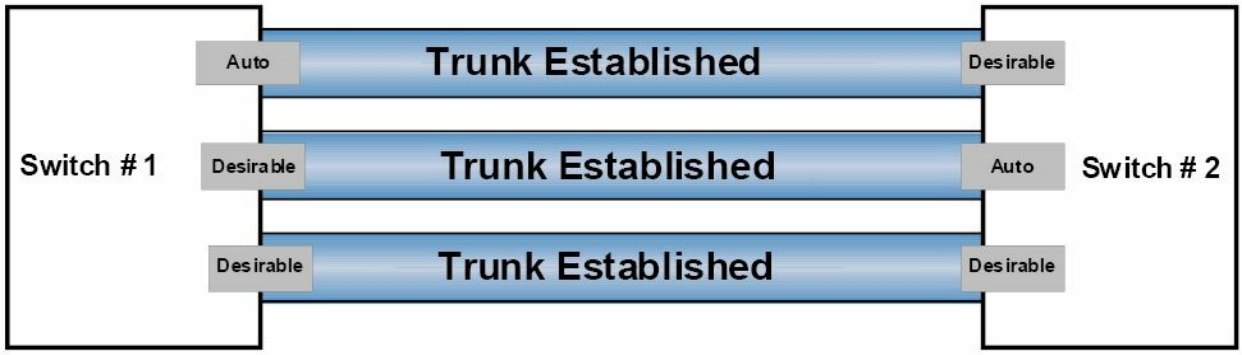


Figure 3.1 – DTP Mode Combinations

Figure 3.2 below illustrates the valid combinations that will result in the successful establishment of a trunk link between two neighbouring switches – one using DTP and the other statically configured as a trunk port:

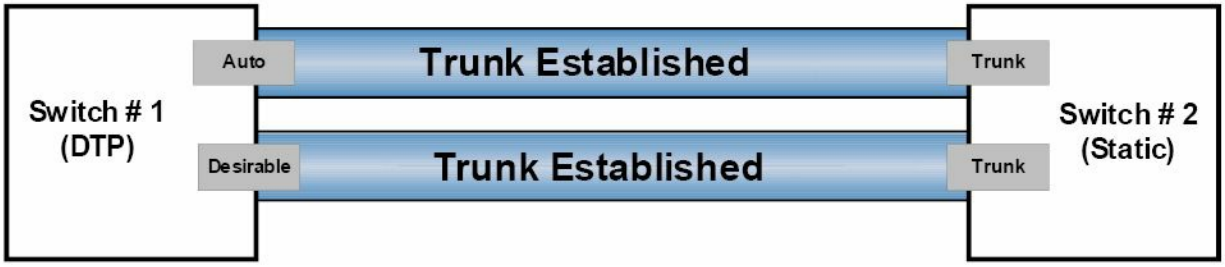


Figure 3.2 – DTP Mode Combinations, Part 2

NOTE: It is important to know that if the switches are both set to dynamic auto, they will not be able to establish a trunk between them. This is because, unlike dynamic desirable mode, dynamic auto mode is a passive mode that waits for the other side to initiate trunk establishment. Therefore, if two passive ports are connected, neither will ever initiate trunk establishment and the trunk will never be formed. Similarly, if a statically configured switch port is also configured with the `switchport nonegotiate` command, it will never form a trunk with a neighbouring switch using DTP because this prevents the sending of DISL and DTP packets out of that port.

When using DTP in a switched LAN, the `show dtp [interface <name>]` command can be used to display DTP information globally for the switch or for the specified interface. The following output shows the information printed by the `show dtp` command:

```
VTP-Server#show dtp
Global DTP information
        Sending DTP Hello packets every 30 seconds
        Dynamic Trunk timeout is 300 seconds
        4 interfaces using DTP
```

Based on the output above, the switch is sending DTP packets every 30 seconds. The timeout value for DTP is set to 300 seconds (5 minutes), and 4 interfaces are currently using DTP. The

https://TheCCIELearningLabs.com

`show dtp interface [name]` command prints DTP information about the specified interface, which includes the type of interface (trunk or access), the current port DTP configuration, the trunk encapsulation, and DTP packet statistics, as illustrated in the following output:

```
VTP-Server#show dtp interface FastEthernet0/1
DTP information for FastEthernet0/1:
  TOS/TAS/TNS:                              TRUNK/ON/TRUNK
  TOT/TAT/TNT:                              802.1Q/802.1Q/802.1Q
  Neighbor address 1:                       000000000000
  Neighbor address 2:                       000000000000
  Hello timer expiration (sec/state):       7/RUNNING
  Access timer expiration (sec/state):      never/STOPPED
  Negotiation timer expiration (sec/state): never/STOPPED
  Multidrop timer expiration (sec/state):   never/STOPPED
  FSM state:                                S6:TRUNK
  # times multi & trunk                     0
  Enabled:                                  yes
  In STP:                                   no
  Statistics
  ----------
  0 packets received (0 good)
  0 packets dropped
      0 nonegotiate, 0 bad version, 0 domain mismatches, 0 bad TLVs, 0 other
  764 packets output (764 good)
      764 native, 0 software encap isl, 0 isl hardware native
  0 output errors
  0 trunk timeouts
  2 link ups, last link up on Mon Mar 01 1993, 00:00:22
  1 link downs, last link down on Mon Mar 01 1993, 00:00:20
```

IEEE 802.1Q Native VLAN

In the previous module, you learned that 802.1Q, or VLAN tagging, inserts a tag into all frames, except those in the native VLAN. The IEEE defined the native VLAN to provide for connectivity to old 802.3 ports that did not understand VLAN tags.

By default, an 802.1Q trunk uses VLAN 1 as the native VLAN. The default native VLAN on an 802.1Q trunk link can be verified by issuing the `show interfaces [name] switchport` or the `show interfaces trunk` command, as illustrated in the following output:

```
VTP-Server#show interfaces FastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
```

https://t.me/learningnets

```
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
...
[Truncated Output]
```

VLAN 1 is used by the switch to carry specific protocol traffic, like Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), Port Aggregation Protocol (PAgP), and Dynamic Trunking Protocol (DTP) information. CDP and PAgP will be described in detail later in this guide. Although the default native VLAN is always VLAN 1, the native VLAN can be manually changed to any valid VLAN number that is not in the reserved range of VLANs.

However, it is important to remember that the native VLAN must be the same on both sides of the trunk link. If there is a native VLAN mismatch, Spanning Tree Protocol (STP) places the port in a port VLAN ID (PVID) inconsistent state and will not forward the link. Additionally, CDPv2 passes native VLAN information between switches and will print error messages on the switch console if there is a native VLAN mismatch. The default native VLAN can be changed by issuing the `switchport trunk native vlan [number]` interface configuration command on the desired 802.1Q trunk link, as illustrated in the following output:

```
VTP-Server(config)#interface FastEthernet0/1
VTP-Server(config-if)#switchport trunk native vlan ?
  <1-4094>  VLAN ID of the native VLAN when this port is in trunking mode
```

Inter-VLAN Routing

By default, although VLANs can span the entire Layer 2 switched network, hosts in one VLAN cannot communicate directly with hosts in another VLAN. In order to do so, traffic must be routed between the different VLANs. This is referred to as inter-VLAN routing. The three methods of implementing inter-VLAN routing in switched LANs below, including their advantages and disadvantages, will be described in the following sections:

- Inter-VLAN routing using physical router interfaces
- Inter-VLAN routing using router subinterfaces
- Inter-VLAN routing using switched virtual interfaces

Inter-VLAN Routing Using Physical Router Interfaces

The first method of implementing inter-VLAN routing for communication entails using a router with multiple physical interfaces as the default gateway for each individually configured VLAN. The router can then route packets received from one VLAN to another using these physical LAN interfaces. This method is illustrated below in Figure 3.3:

https://t.me/learningnets

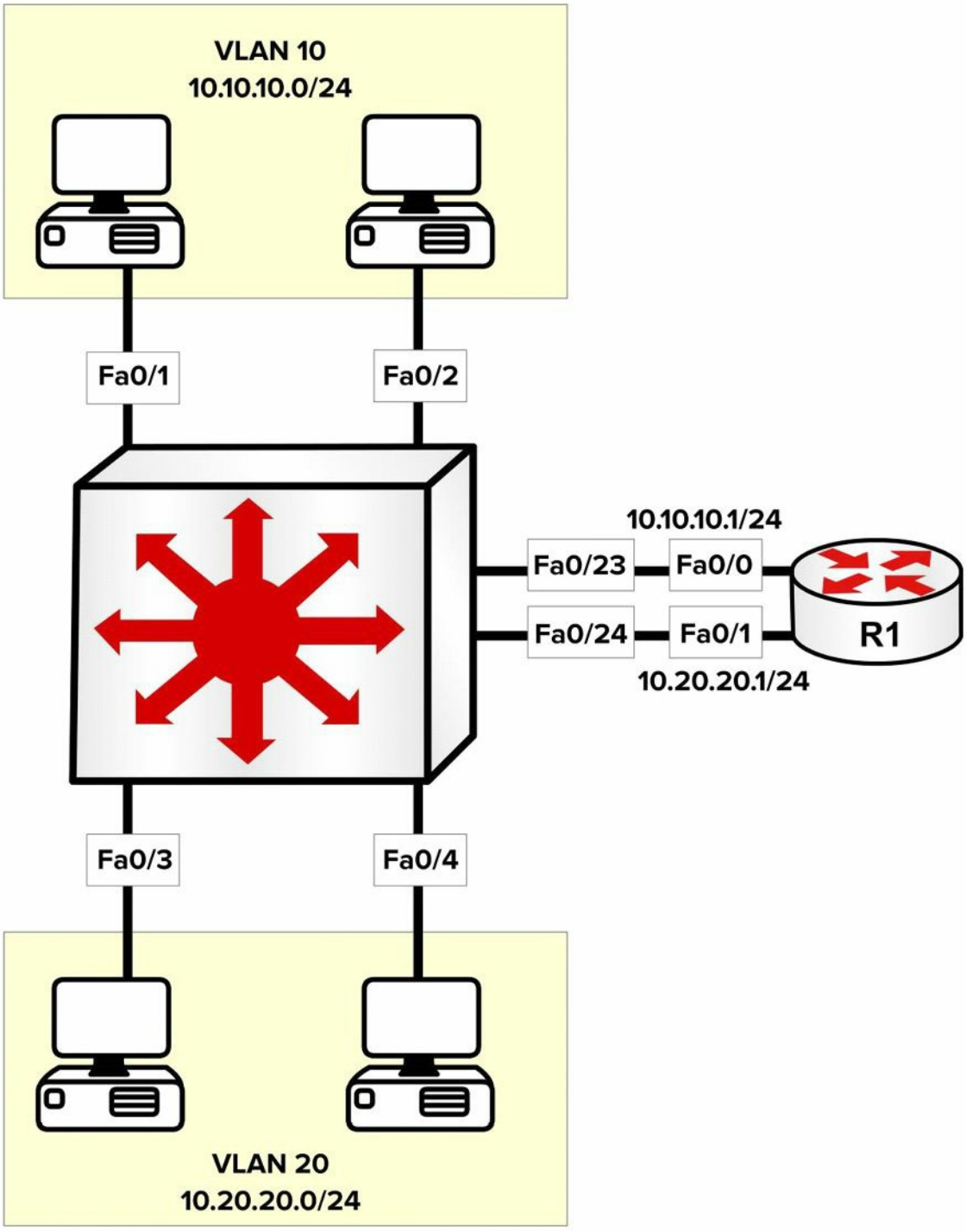


Figure 3.3 – Inter-VLAN Routing Using Multiple Physical Router Interfaces

Figure 3.3 illustrates a single LAN using two different VLANs, each with an assigned IP subnet. Although the network hosts depicted in the figure are connected to the same physical switch, because they reside in different VLANs, packets between hosts in VLAN 10 and those in VLAN 20 must be routed, while packets within the same VLAN are simply switched.

The primary advantage of using this solution is that it is simple and easy to implement. The primary disadvantage, however, is that it is not scalable. For example, if 5, 10, or even 20 additional VLANs were configured on the switch, the same number of physical interfaces as VLANs would also be needed on the router. In most cases, this is technically not feasible.

When using multiple physical router interfaces, each switch link connected to the router is configured as an access link in the desired VLAN. The physical interfaces on the router are then configured with the appropriate IP addresses, and the network hosts are either statically

https://t.me/learningnets

configured with IP addresses in the appropriate VLAN, using the physical router interface as the default gateway, or dynamically configured using DHCP. The configuration of the switch illustrated in Figure 3.3 is illustrated in the following output:

```
VTP-Server-1(config)#vlan 10
VTP-Server-1(config-vlan)#name Example-VLAN-10
VTP-Server-1(config-vlan)#exit
VTP-Server-1(config)#vlan 20
VTP-Server-1(config-vlan)#name Example-VLAN-20
VTP-Server-1(config-vlan)#exit
VTP-Server-1(config)#interface range FastEthernet0/1 - 2, 23
VTP-Server-1(config-if-range)#switchport
VTP-Server-1(config-if-range)#switchport access vlan 10
VTP-Server-1(config-if-range)#switchport mode access
VTP-Server-1(config-if-range)#exit
VTP-Server-1(config)#interface range FastEthernet0/3 - 4, 24
VTP-Server-1(config-if-range)#switchport
VTP-Server-1(config-if-range)#switchport access vlan 20
VTP-Server-1(config-if-range)#switchport mode access
VTP-Server-1(config-if-range)#exit
```

The `switchport` command isn't required on the 2960 switch because the interface is already running in Layer 2 mode.

The router illustrated in Figure 3.3 is configured as shown in the following output:

```
R1(config)#interface FastEthernet0/0
R1(config-if)#ip add 10.10.10.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface FastEthernet0/1
R1(config-if)#ip add 10.20.20.1 255.255.255.0
R1(config-if)#exit
```

Inter-VLAN Routing Using Router Subinterfaces

Implementing inter-VLAN routing using subinterfaces addresses the scalability issues that are possible when using multiple physical router interfaces. With subinterfaces, only a single physical interface is required on the router and subsequent subinterfaces are configured off that physical interface. This is illustrated below in Figure 3.4:

https://t.me/learningnets

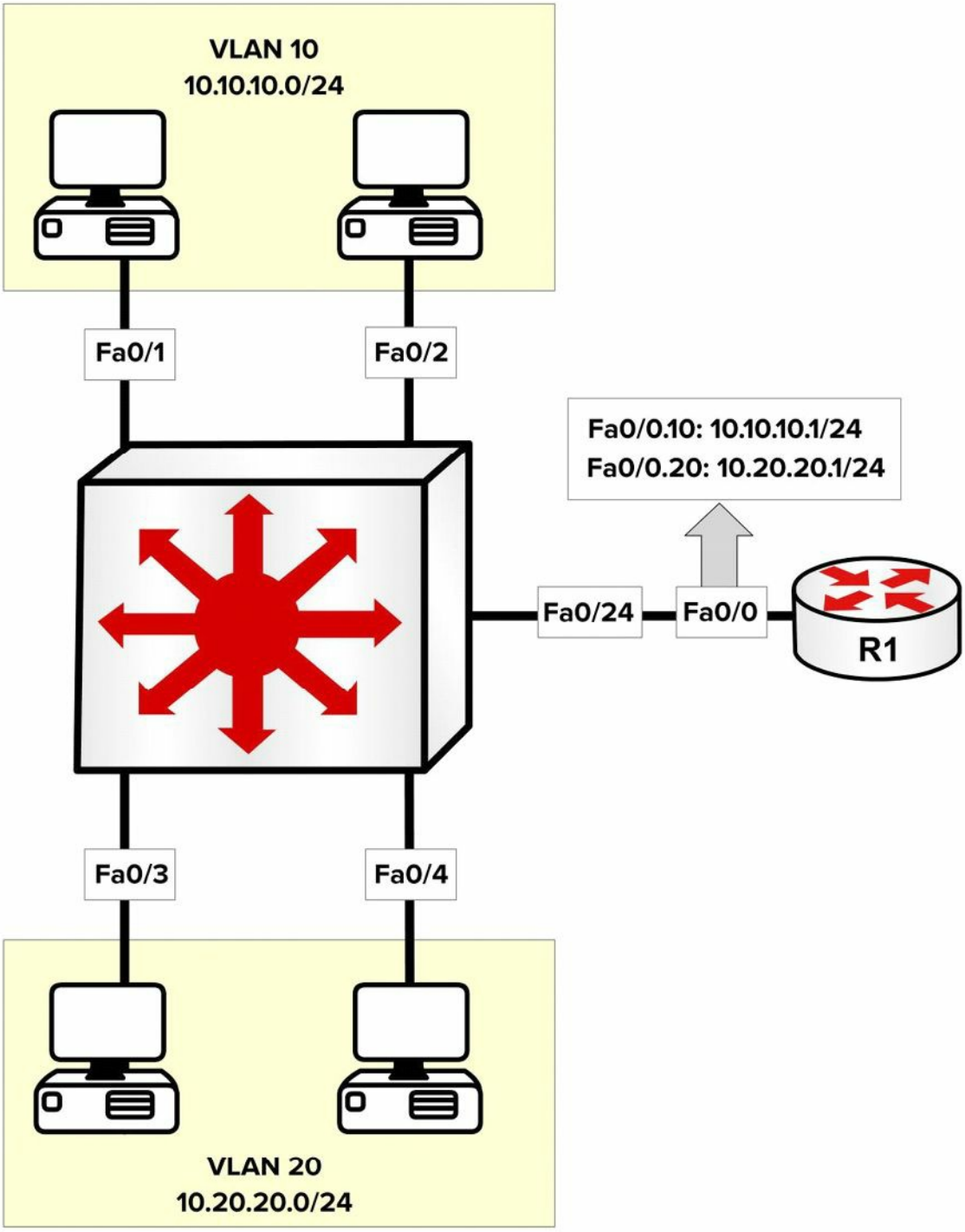


Figure 3.4 – Inter-VLAN Routing Using Router Subinterfaces

Figure 3.4 depicts the same LAN illustrated in Figure 3.3. In Figure 3.4, however, only a single physical router interface is being used. In order to implement an inter-VLAN routing solution, subinterfaces are configured off the main physical router interface using the `interface [name].[subinterface number]` global configuration command. Each subinterface is associated with a particular VLAN using the `encapsulation [isl|dot1Q] [vlan]` subinterface configuration command. The final step is to configure the desired IP address on the interface.

On the switch, the single link connected to the router must be configured as a trunk link because routers don't support DTP. If the trunk is configured as an 802.1Q trunk, a native VLAN must be defined if a VLAN other than the default will be used as the native VLAN. This native VLAN must also be configured on the respective router subinterface using the `encapsulation dot1Q [vlan] native` subinterface configuration command. The following output illustrates the

https://t.me/learningnets

configuration of inter-VLAN routing using a single physical interface (also referred to as “router-on-a-stick”). The two VLANs depicted in Figure 3.4 are shown in the following output, as is an additional VLAN used for Management; this VLAN will be configured as the native VLAN:

```
VTP-Server-1(config)#vlan 10
VTP-Server-1(config-vlan)#name Example-VLAN-10
VTP-Server-1(config-vlan)#exit
VTP-Server-1(config)#vlan 20
VTP-Server-1(config-vlan)#name Example-VLAN-20
VTP-Server-1(config-vlan)#exit
VTP-Server-1(config)#vlan 30
VTP-Server-1(config-vlan)#name Management-VLAN
VTP-Server-1(config-vlan)#exit
VTP-Server-1(config)#interface range FastEthernet0/1 - 2
VTP-Server-1(config-if-range)#switchport
VTP-Server-1(config-if-range)#switchport access vlan 10
VTP-Server-1(config-if-range)#switchport mode access
VTP-Server-1(config-if-range)#exit
VTP-Server-1(config)#interface range FastEthernet0/3 - 4
VTP-Server-1(config-if-range)#switchport
VTP-Server-1(config-if-range)#switchport access vlan 20
VTP-Server-1(config-if-range)#switchport mode access
VTP-Server-1(config-if-range)#exit
VTP-Server-1(config)#interface FastEthernet0/24
VTP-Server-1(config-if)#switchport
VTP-Server-1(config-if)#switchport trunk encapsulation dot1q
VTP-Server-1(config-if)#switchport mode trunk
VTP-Server-1(config-if)#switchport trunk native vlan 30
VTP-Server-1(config-if)#exit
VTP-Server-1(config)#interface vlan 30
VTP-Server-1(config-if)#description ‘This is the Management Subnet’
VTP-Server-1(config-if)#ip address 10.30.30.2 255.255.255.0
VTP-Server-1(config-if)#no shutdown
VTP-Server-1(config-if)#exit
VTP-Server-1(config)#ip default-gateway 10.30.30.1
```

The router illustrated in Figure 3.4 is configured as shown in the following output:

```
R1(config)#interface FastEthernet0/0
R1(config-if)#no ip address
R1(config-if)#exit
R1(config)#interface FastEthernet0/0.10
R1(config-subif)#description ‘Subinterface For VLAN 10’
```

https://t.me/learningnets

```
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip add 10.10.10.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface FastEthernet0/0.20
R1(config-subitf)#description 'Subinterface For VLAN 20'
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip add 10.20.20.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface FastEthernet0/0.30
R1(config-subitf)#description 'Subinterface For Management'
R1(config-subif)#encapsulation dot1Q 30 native
R1(config-subif)#ip add 10.30.30.1 255.255.255.0
R1(config-subif)#exit
```

The primary advantage of this solution is that only a single physical interface is required on the router. The primary disadvantage is that the bandwidth of the physical interface is shared between the various configured subinterfaces. Therefore, if there is a lot of inter-VLAN traffic, the router can quickly become a bottleneck in the network.

Inter-VLAN Routing Using Switched Virtual Interfaces

Multilayer switches support the configuration of IP addressing on physical interfaces. These interfaces, however, must be configured with the `no switchport` interface configuration command to allow administrators to configure IP addressing on them. In addition to using physical interfaces, Multilayer switches also support Switched Virtual Interfaces (SVIs).

SVIs are logical interfaces that represent a VLAN. Although the SVI represents a VLAN, it is not automatically configured when a Layer 2 VLAN is configured on the switch; it must be manually configured by the administrator using the `interface vlan [number]` global configuration command. The Layer 3 configuration parameters, such as IP addressing, are then configured on the SVI in the same manner as they would be on a physical interface.

The following output illustrates the configuration of SVIs to allow inter-VLAN routing on a single switch. This output references the VLANs used in the previous configuration outputs in this section:

```
VTP-Server-1(config)#vlan 10
VTP-Server-1(config-vlan)#name Example-VLAN-10
VTP-Server-1(config-vlan)#exit
VTP-Server-1(config)#vlan 20
VTP-Server-1(config-vlan)#name Example-VLAN-20
VTP-Server-1(config-vlan)#exit
VTP-Server-1(config)#interface range FastEthernet0/1 - 2
VTP-Server-1(config-if-range)#switchport
VTP-Server-1(config-if-range)#switchport mode access
VTP-Server-1(config-if-range)#switchport access vlan 10
```

https://t.me/learningnets

```
VTP-Server-1(config-if-range)#exit
VTP-Server-1(config)#interface range FastEthernet0/3 - 4
VTP-Server-1(config-if-range)#switchport
VTP-Server-1(config-if-range)#switchport mode access
VTP-Server-1(config-if-range)#switchport access vlan 20
VTP-Server-1(config-if-range)#exit
VTP-Server-1(config)#interface vlan 10
VTP-Server-1(config-if)#description "SVI for VLAN 10"
VTP-Server-1(config-if)#ip address 10.10.10.1 255.255.255.0
VTP-Server-1(config-if)#no shutdown
VTP-Server-1(config-if)#exit
VTP-Server-1(config)#interface vlan 20
VTP-Server-1(config-if)#description 'SVI for VLAN 10'
VTP-Server-1(config-if)#ip address 10.20.20.1 255.255.255.0
VTP-Server-1(config-if)#no shutdown
VTP-Server-1(config-if)#exit
```

When using Multilayer switches, SVIs are the recommended method for configuring and implementing an inter-VLAN routing solution.

You can verify that the SVI is properly configured (IP addressing, etc.) by using the `how interface vlan x` command. The output is identical to a `show interface x` command:

```
Switch#show interfaces vlan 100
Vlan100 is up, line protocol is down
  Hardware is EtherSVI, address is c200.06c8.0000 (bia c200.06c8.0000)
  Internet address is 10.10.10.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
```

If you wish to use a 2960 switch to route IP packets, it will require a configuration change and reload. The reason for this is the 2960 and newer model switches are tuned to allocate resources in a certain way. The resource management is called the Switch Database Management (SDM) template. Your choices include the following:

- Default – balances all functions
- Dual IPv4/IPv6 – for use in dual-stack environments
- Lanbase-routing – supports Unicast routes
- QoS – gives support for QoS features

Here are the options on my 3750 switch. They don't match the 2960 options exactly, but you get the idea. Also, bear in mind that your switch model and IOS will affect the configuration

https://t.me/learningnets

options, so check the configuration guide for your model:

```
Switch(config)#sdm prefer ?
  access              Access bias
  default             Default bias
  dual-ipv4-and-ipv6  Support both IPv4 and IPv6
  ipe                 IPe bias
  lanbase-routing     Unicast bias
  vlan                VLAN bias
```

Lanbase-routing will need to be enabled if you wish to configure inter-VLAN routing on your 2960 switch. You will also need to reload the switch before the change will take effect. Here is the output of the `show sdm prefer` command, which tells you the current SDM configuration and resource allocation:

```
Switch#show sdm prefer
The current template is "desktop default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.
  number of unicast mac addresses:                  6K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    8K
    number of directly-connected IPv4 hosts:        6K
    number of indirect IPv4 routes:                 2K
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      0.5K
  number of IPv4/MAC security aces:                 1K
Switch#
```

VTP

VLAN Trunking Protocol (VTP) is a Cisco proprietary Layer 2 messaging protocol that manages the addition, deletion, and renaming of VLANs on switches in the same VTP domain. VTP allows VLAN information to propagate through the switched network, which reduces administration overhead in a switched network, whilst enabling switches to exchange and maintain consistent VLAN information. This concept is illustrated in Figure 3.5 below:

https://t.me/learningnets

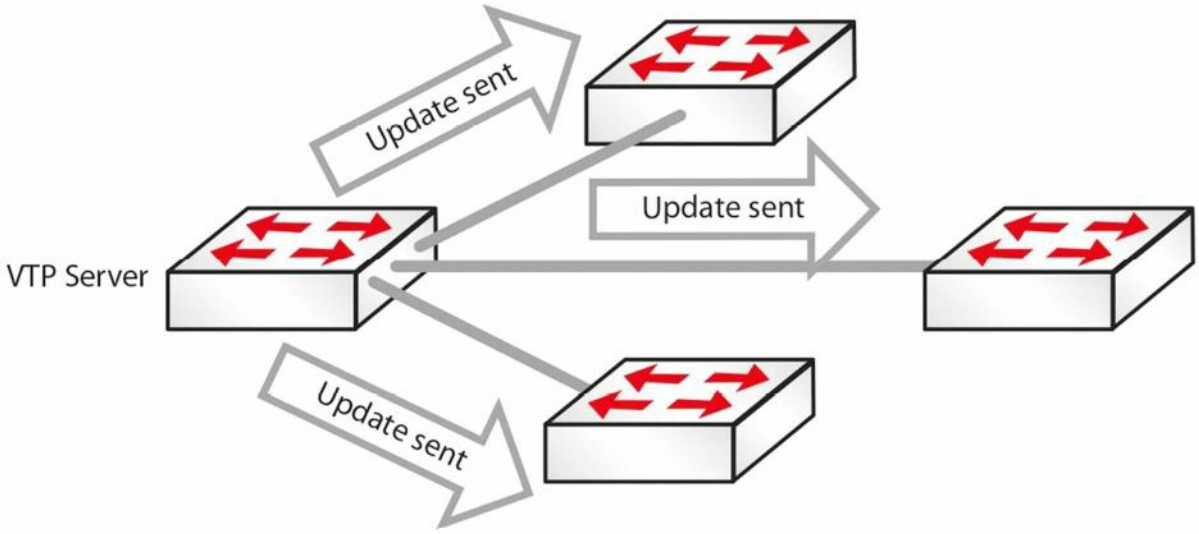


Figure 3.5 – VTP Updates

Some benefits to using VTP include the following:

- Accurate monitoring and reporting of VLANs
- VLAN consistency across the network
- Ease of adding and removing VLANs

Configuring VTP

All switches must be configured with the same VTP domain name if they are to exchange VLAN information, as illustrated in the output below:

```
Switch(config)#vtp mode server ←this is on by default
Switch(config)#vtp domain in60days
Changing VTP domain name from NULL to in60days
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs Supported Locally : 255
Number of Existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : in60days
```

If you want to secure your VTP updates, you can add a password, but it must match on each switch in the VTP domain:

```
Switch(config)#vtp password Cisco321
Setting device VLAN database password to Cisco321
```

VTP Modes

VTP runs in the following three modes:

- Server (default)

https://t.me/learningnets

- Client
- Transparent

You can see the server mode in the configuration and output above.

Server Mode

In Server mode, the switch is authorised to create, modify, and delete VLAN information for the entire VTP domain. Any changes you make to a server are propagated throughout the whole domain. VLAN configuration is stored in the VLAN database file “vlan.dat” located on the flash memory.

Client Mode

In Client mode, the switch will receive VTP information and apply any changes, but it does not allow adding, removing, or changing VLAN information on the switch. The client will also send the VTP packet received out of its trunk ports. Remember that you cannot add a switch port on a VTP client switch to a VLAN that does not exist on the VTP server. VLAN configuration is stored in the VLAN database file “vlan.dat” located on the flash memory.

Transparent Mode

In Transparent mode, the switch will forward the VTP information received out of its trunk ports, but it will not apply the changes. A VTP Transparent-mode switch can create, modify, and delete VLANs, but the changes are not propagated to other switches. VTP Transparent mode also requires configuration of domain information. A VTP transparent switch is needed when a switch separating a VTP server and client needs to have a different VLAN database. Transparent mode is needed to configure the extended VLAN range (1006 to 4096).

VTP Pruning

There will often be situations where you have VLANs 20 to 50, for example, on one side of your network and 60 to 80 on the other. It doesn’t make sense for VLAN information from the switches on one side to be passed to every switch on the other. For this reason, switches can prune unnecessary VLAN information on the switches, thus reducing the Broadcast traffic, as shown in Figure 3.6 below:

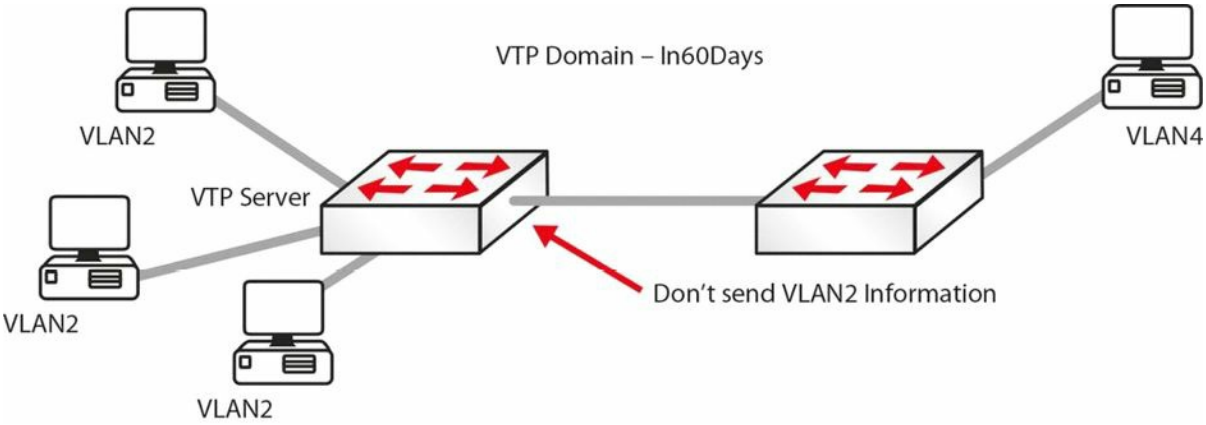


Figure 3.6 – VTP Pruning in Operation

The following line of configuration will add VTP pruning to your switch:

https://t.me/learningnets

```
Switch(config)#vtp pruning
```

It is worth noting that if you have a switch set to transparent mode in-between two other switches, then pruning will not work.

Configuration Revision Number

The configuration revision number is a 32-bit number that indicates the level of revision for a VTP packet (see the `show vtp status` output above). This information is used to determine whether the received information is more recent than the current version. Each time that you make a VLAN change on a switch in VTP Server mode, the configuration revision is incremented by one and change will be propagated to VTP clients (switches in VTP Transparent mode will have a revision number of 0 and will not increase with database changes). In order to reset the configuration revision of a switch, change the VTP domain name, and then change the name back to the original name.

IMPORTANT NOTE: If a switch configured as VTP Server or VTP Client with a matching domain name and a higher revision number connects to the network, its database will be propagated to all other switches, potentially replacing their existing VTP databases. This can bring the whole LAN network down, so be very careful (always check the VTP status) when connecting a new switch to the LAN network!

Basic VLAN Troubleshooting

VLANs are a fairly straightforward feature which rarely requires troubleshooting. A few of the problems that you will see are mostly configuration errors. We will cover Layer 2 troubleshooting in detail on Day 15. Common problems include the following:

1. Inter-VLAN routing not working: Check to ensure that the link between the switches and the routers is set up correctly, and the relevant VLANs are allowed and not pruned (see VTP pruning). The `show interface trunk` command will provide the required information. Also, check to ensure that the router's subinterfaces are configured with correct encapsulation and VLAN, and the subinterface's IP address is the default gateway for the hosts.
2. VLANs cannot be created: Check whether the VTP mode on the switch is set to "client." VLANs cannot be created if the VTP mode is client. Another important factor is the number of VLANs allowed on the switch. The `show vtp status` command will provide the information required (see the Troubleshooting Trunking and VTP section below).
3. Hosts within the same VLAN cannot reach each other: It is important that hosts in a VLAN have an IP address that belongs to the same subnet. If the subnet is different, then they will not be able to reach each other. Another factor to consider is whether the hosts are connected to the same switch. If they are not connected to the same switch, then ensure that the trunk link(s) between the switches is/are working correctly and that the VLAN is not excluded/not pruned from the allowed list. The `show interface trunk` command will show needed information regarding the trunk link.

Troubleshooting Trunking and VTP

https://t.me/learningnets

The following are examples of problems and possible solutions:

Trunk down?

- Interface must be up/up
- Encapsulation must match both sides

```
SwitchA#show interface fa1/1 switchport
Name: Fa1/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
```

VLAN information not passing?

- Is the VLAN blocked on the trunk?

```
Switch#show interface trunk
```

VTP information not reaching the client?

- Correct domain and VTP password?

```
show vtp status / show vtp password
```

Added a new switch and all VTP information has changed?

- Always add a new switch in Client mode (but check the above note on the configuration revision number)
- Server mode will propagate new information

VTP pruning not working?

- Is there a transparent switch in the middle?
- Is the VLAN allowed across the trunk?

Troubleshooting Inter-VLAN Routing

Inter-VLAN routing issues can come in many forms, especially considering that multiple devices are involved (switches, routers, etc.) in the process. By following a proper troubleshooting methodology, you should be able to isolate the problem to a particular device and then map it to a specific feature that has been misconfigured.

From a connectivity standpoint, some of the things that need to be checked include:

- Verfiying that the end-stations are connected in the proper switch ports
- Verifying that the proper switch ports are connected in the proper router ports (if a router is used for inter-VLAN routing)
- Verifying that each of the ports involved in this process carry the correct VLANs

https://t.me/learningnets

- The ports that connect the end-stations are usually access ports allocated to a particular VLAN
- The ports connecting the switch to the router are usually trunk ports

After confirming that the connectivity between the devices is correct, the next logical step is investigating Layer 2 configuration, starting with the configured encapsulation method on the trunk ports, which is usually 802.1Q, the preferred method. Next, make sure that the same encapsulation is configured on both ends of the trunk link.

Some of the commands that can be used to verify the encapsulation types are as follows:

- `show interface trunk`
- `show interface <number> switchport`

Here is an example output:

```
Cat-3550-1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/1       1,10,20,30,40,50
Fa0/2       1-99,201-4094
```

Another important detail that is offered by the `show interface trunk` command is the trunk status. This confirms whether the trunk is formed or not and it has to be checked at both ends of the link. If the interface is not in “trunking” mode, one of the most important things that has to be verified is the mode of operation (on, auto, etc.) to see whether it will allow a trunking state to form with the other end of the link.

The native VLAN is another important element that you should verify on the trunk ports. Misconfigured native VLANs can lead to a lack of functionality or security issues. The native VLAN should match at both ends of the trunk links.

If after verifying the Layer 2 verification tasks the inter-VLAN issue is still not resolved, you can proceed to verifying Layer 3 configuration. Depending upon the Layer 3 device used to ensure the actual inter-VLAN routing, this can be configured/verified on one of the following devices:

- Multilayer switch
- Router – physical interfaces
- Router – subinterfaces

On the Layer 3 device, you should verify that the correct subnet is assigned to each interface (or SVI), and you should also verify the routing protocol, if needed. Usually, a different subnet is assigned to each VLAN so you should make sure that you don’t misconfigure the interfaces. In order to verify this you can use the `show interface` command for the specific physical interface, subinterface, or SVI.

https://t.me/learningnets

Day 3 Questions

1. Name four advantages of using VLANs.
2. Hosts in the same VLAN can be in different subnets. True or false?
3. An access link is part of more than one VLAN. True or false?
4. Name the two trunk link encapsulation types.
5. Which commands will configure and name a VLAN?
6. A trunk link on a switch can be in which five possible modes?
7. Which command would put your interface into VLAN 5?
8. Which command will change the native VLAN?
9. VTP Client mode allows you to configure VLANs. True or false?
10. Name three benefits of using VTP.
11. Which command configures VTP pruning on your switch?

https://t.me/learningnets

Day 3 Answers

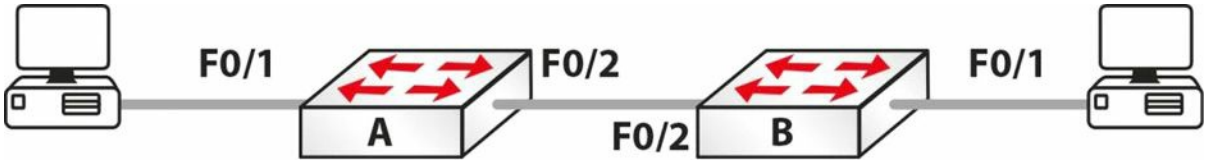
1. Containing Broadcasts within a smaller group of devices will make the network faster; saves resources on devices because they process less Broadcasts; added security by keeping devices in a certain group (or function) in a separate Broadcast domain; and flexibility in expanding a network across a geographical location of any size.
2. True, but not recommended.
3. False.
4. 802.1Q and ISL.
5. The `vlan x` and `name y` commands.
6. On, off, auto, desirable, and nonegotiate.
7. The `switchport access vlan 5` command.
8. The `switchport trunk native vlan x` command.
9. False.
10. Accurate monitoring and reporting of VLANs; VLAN consistency across the network; and ease of adding and removing VLANs.
11. The `vtp pruning` command.

https://t.me/learningnets

Day 3 Labs

VLAN and Trunking Lab

Topology



Purpose

Learn how to configure VLANs and trunk links.

Walkthrough

1. You will need to add IP addresses on each PC. Feel free to choose your own, as long as they are on the same subnet!
2. On Switch A, set the hostname, create VLAN 2, and put the interface to which your PC is connected into VLAN 2. You can also give the VLAN a name if you wish.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SwitchA
SwitchA(config)#vlan 2
SwitchA(config-vlan)#name 60days
SwitchA(config-vlan)#interface FastEthernet0/1
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 2
SwitchA(config-if)#^Z
SwitchA#show vlan brief
VLAN Name                Status    Ports
---- --------- -------------------------------
1    default             active    Fa0/2, Fa0/3, Fa0/4, Fa0/5,
                                   Fa0/6, Fa0/7, Fa0/8, Fa0/9,
                                   Fa0/10, Fa0/11, Fa0/12, Fa0/13,
                                   Fa0/14, Fa0/15, Fa0/16, Fa0/17,
                                   Fa0/18, Fa0/19, Fa0/20, Fa0/21,
                                   Fa0/22, Fa0/23, Fa0/24
2    60days              active    Fa0/1
1002 fddi-default        active
1003 token-ring-default  active
1004 fddinet-default     active
1005 trnet-default       active
```

https://t.me/learningnets

```
SwitchA#
```

3. Set your trunk link to trunk mode.

```
SwitchA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#int FastEthernet0/2
SwitchA(config-if)#switchport mode trunk
SwitchA#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/2       on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/2       1-1005
```

4. If you wish, permit only VLAN 2 on the trunk link.

```
SwitchA(config)#int FastEthernet0/2
SwitchA(config-if)#switchport trunk allowed vlan 2
SwitchA(config-if)#^Z
SwitchA#
%SYS-5-CONFIG_I: Configured from console by console
SwitchA#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/2       on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/2       2
```

5. At this point, if you ping from one PC to another, it should fail. This is because one side is in VLAN 1 and the other is in VLAN 2.

```
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Ping statistics for 192.168.1.1:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss)
```

6. Configure the same commands on Switch B now. For VLAN creation, put the PC port into VLAN 2, and set the interface to “access” and the trunk link to “trunk.”

7. Now you should be able to ping across the trunk link from PC to PC.

```
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=188ms TTL=128
Reply from 192.168.1.1: bytes=32 time=78ms TTL=128
Reply from 192.168.1.1: bytes=32 time=94ms TTL=128
Reply from 192.168.1.1: bytes=32 time=79ms TTL=128
Ping statistics for 192.168.1.1:
```

https://t.me/learningnets

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 78ms, Maximum = 188ms, Average = 109ms
```

VTP Lab

Test the VTP configuration commands presented in this module in a topology made up of two switches:

- ☐ Configure one of the switches as a VTP server
- ☐ Configure the other switch as a VTP client
- ☐ Configure the same VTP domain and password on both switches
- ☐ Create a series of VLANs on the server switch and see how they propagate to each other
- ☐ Configure VTP pruning on both switches
- ☐ Verify (show) the VTP configuration on both switches
- ☐ Configure a different VTP domain name and password and repeat the process; see how the results differ

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 4 – Router and Switch Security

Day 4 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's lab
- Read the ICND1 cram guide

Switches and routers do not come with any security configuration. You need to add this depending upon your business requirements. The commands and procedures to secure your switch are pretty much the same as those for your router. Now it's time to move on to the practical steps you can take to secure your router from attempts to log in and reconfigure, either accidentally or maliciously.

My first job at Cisco was on the core team. Our role involved helping customers with access control lists, IOS upgrades, disaster recovery, and related tasks. One of the first things which struck me was how many engineers didn't lock down their routers with a password. Many of those who did used the password "password" or "cisco" – probably two of the most easily guessed, I would imagine!

In this section of the guide, we will look at the basic steps you should take on every network to protect your routers.

Today you will learn about the following:

- Protecting physical access
- Telnet access
- Protecting Enable mode
- Router logging
- Securing the switch

This module maps to the following CCNA syllabus requirements:

- Configure and verify network device security features, such as:
  - Device password security
  - Enable secret versus enable
  - Transport
  - Disable Telnet
  - SSH
  - VTYs
  - Physical security

https://t.me/learningnets

- Service password

- Describe external authentication methods
- Configure and verify Switch Port Security features, such as:
  - Sticky MAC
  - MAC address limitation
  - Static/dynamic
  - Violation modes
  - Err disable
  - Shutdown
  - Protect restrict
  - Shut down unused ports
  - Err disable recovery
- Assign unused ports to an unused VLAN
- Set native VLAN to something other than VLAN 1
- Configure and verify NTP as a client

Protecting Physical Access

Strange that when you consider the disastrous consequences of losing network access for a business, you often find their router sitting underneath somebody's desk!

Network equipment should be stored in a secure room with keypad access, or at least lock and key access. Cisco routers can be very valuable pieces of equipment, and they are attractive targets to thieves. The larger the network, the more valuable the equipment, and the higher the need to protect the data and router configuration files.

Console Access

The console port is designed to give physical access to the router to permit initial configurations and disaster recovery. Anybody having console access can completely wipe or reconfigure the files, so, for this reason, the console port should be protected with a password by adding either a password or a local username and password, as illustrated below:

- Add a password

```
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
```

- Or add a local username and password

```
Router(config)#username paul password cisco
Router(config)#line console 0
```

https://t.me/learningnets

```
Router(config-line)#login local
```

You can also create a timeout on the console (and VTY) lines so that it disconnects after a certain period of time. The default is 5 minutes.

```
Router(config)#line console 0
Router(config-line)#exec-timeout ?
  <0-35791>  Timeout in minutes
Router(config-line)#exec-timeout 2 ?
  <0-2147483>  Timeout in seconds
  <cr>
Router(config-line)#exec-timeout 2 30
Router(config-line)#
```

Telnet Access

You can't actually Telnet into a router unless somebody adds a password to the Telnet or VTY lines. Again, you can add a password to the VTY lines or tell the router to look for a local username and password (in the configuration file or username and password stored on a RADIUS/TACACS server), as shown below:

```
Router(config-line)#line vty 0 15
Router(config-line)#password cisco
Router(config-line)#login ← or login local
```

The output below is a Telnet session from one router to another. You can see the hostname change when you get Telnet access. The password will not show as you type it:

```
Router1#telnet 192.168.1.2
Trying 192.168.1.2 ...Open
User Access Verification
Username: paul
Password:
Router2>
```

If you have a security IOS image, you can configure the router to permit only SSH access rather than Telnet. The benefit of this is that all data is encrypted. If you try to Telnet after SSH has been enabled, the connection will be terminated:

```
Router1(config)#line vty 0 15
Router1(config-line)#transport input ssh
Router2#telnet 192.168.1.2
Trying 192.168.1.2 ...Open
[Connection to 192.168.1.2 closed by foreign host]
```

Protecting Enable Mode

Enable mode gives configuration access to the router, so you will want to protect this also. You can configure an enable secret or an enable password. In fact, you could have both at the same

time, but this is a bad idea.

An enable password is unencrypted, so it can be seen in the router configuration. An enable secret is given level 5 (MD5) encryption, which is hard to break. Newer IOS releases (starting with 15.0(1)S) can also use level 4 (SHA256) encryption, which is superior to MD5 encryption (this level 5 encryption will be deprecated eventually). You can add the command `service password encryption` to your enable password, but this can be cracked easily because it is level 7 encryption (i.e., low security; Cisco calls it "over the shoulder security," as it only requires someone looking over your shoulder to memorise a slightly harder phrase and then crack it using password 7 decryption tools on the Internet). You can see level 7 and level 5 encryption in the output below:

```
Router(config)#enable password cisco
Router(config)#exit
Router#show run
enable password cisco
Router(config)#enable password cisco
Router(config)#service password-encryption
Router#show run
enable password 7 0822455D0A16
Router(config)#enable secret cisco
Router(config)#exit
Router#show run
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
```

Bear in mind that if you forget the enable password, you will have to perform a password recovery on the router or switch. Google the term for the particular model you are using because the process differs. For routers, it involves reloading the device, pressing the designated break key on your keyboard, setting the configuration register to skip the startup configuration file (usually to 0x2142), and then issuing a `copy start run` command so you can create a new password.

For switches, it is a bit more complicated (again, Google the term for the particular model you are using), but it can also be done using a little trick – hold down the MODE button for eight seconds while powering on the switch. The switch will boot up with a blank configuration, and the last startup configuration will be saved to the flash in the file named `config.text.renamed` so it can be copied back to running configuration and modified with another password.

Protecting User Access

Cisco IOS offers the ability to give users individual passwords and usernames, as well as access to a restricted list of commands. This would be useful if you have tiers of network support. An example of this is shown in the following output:

```
RouterA#config term
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#username paul password cisco
```

https://t.me/learningnets

```
RouterA(config)#username stuart password hello
RouterA(config)#username davie password football
RouterA(config)#line vty 0 4
RouterA(config-line)#login local
RouterA(config-line)#exit
RouterA(config)#exit
```

You can specify access levels for user accounts on the router. You may want, for example, junior network team members to be able to use only some basic troubleshooting commands. It is also worth remembering that Cisco routers have two modes of password security, User mode (Exec) and Privileged mode (Enable).

Cisco routers have 16 different privilege levels (0 to 15) available to configure, where 15 is full access, as illustrated below:

```
RouterA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#username support privilege 4 password soccer
    LINE Initial keywords of the command to modify
RouterA(config)#privilege exec level 4 ping
RouterA(config)#privilege exec level 4 traceroute
RouterA(config)#privilege exec level 4 show ip interface brief
RouterA(config)#line console 0
RouterA(config-line)#password basketball
RouterA(config-line)#login local ← password is needed
RouterA(config-line)#^z
```

The support person logs in to the router and tries to go into configuration mode, but this command and any other command not available are not valid and cannot be seen:

```
RouterA con0 is now available
Press RETURN to get started.
User Access Verification
Username: support
Password:
RouterA#config t ← not allowed to use this command
          ^
% Invalid input detected at '^' marker.
```

You can see the default privilege levels at the router prompts:

```
Router>show privilege
Current privilege level is 1
Router>en
Router#show priv
Router#show privilege
Current privilege level is 15
Router#
```

Updating the IOS

https://t.me/learningnets

Admittedly, updating the IOS can sometimes introduce new bugs or problems into your network, so it is best practice to do this on the advice of Cisco if you have a TAC support contract. In general, though, keeping your IOS up to date is highly recommended.

Updating your IOS:

- Fixes known bugs
- Closes security vulnerabilities
- Offers enhanced features and IOS capabilities

Router Logging

Routers offer the ability to log events. They can send the log messages to your screen or a server if you wish. You should log router messages, and there are eight levels of logging severity available (you need to know them for the exam), as shown in bold in the output below:

```
logging buffered ?
<0-7>Logging severity level
alerts—Immediate action needed (severity=1)
critical—Critical conditions (severity=2)
debugging—Debugging messages (severity=7)
emergencies—System is unusable (severity=0)
errors—Error conditions (severity=3)
informational—Informational messages (severity=6)
notifications—Normal but significant conditions (severity=5)
warnings—Warning conditions (severity=4)
```

You can send the logging messages to several places:

```
Router(config)#logging ?
  A.B.C.D   IP address of the logging host
  buffered  Set buffered logging parameters
  console   Set console logging parameters
  host      Set syslog server IP address and parameters
  on        Enable logging to all enabled destinations
  trap      Set syslog server logging level
  userinfo  Enable logging of user info on privileged mode enabling
```

Logging messages will usually be displayed on the screen when you are consoled into the router. This can prove somewhat annoying if you are typing configuration commands. Here, I'm typing a command (underlined) when it's interruped by a console logging message:

```
Router(config)#int f0/1
Router(config-if)#no shut
Router(config-if)#end
Router#
*Jun 27 02:06:59.951: %SYS-5-CONFIG_I: Configured from console by console show ver
*Jun 27 02:07:01.151: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
```

You can either turn off logging messages with the `no logging console` command or you can set

https://theelearningfield

them to not interrupt as you type with the `logging synchronous` command, which re-enters the line you were typing before being interrupted by the logging message (also available on VTY lines).

```
Router(config)#line con 0
Router(config-line)#logging synchronous
Router(config-line)#
Router(config-line)#exit
Router(config)#int f0/1
Router(config-if)#shut
Router(config-if)#exit
Router(config)#
*Jun 27 02:12:46.143: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
Router(config)#exit
```

It's worth mentioning here that you won't see console output when you are Telnetted (or using SSH) into the router. If you want to see logging messages when Telnetted in, then issue the `terminal monitor` command.

Simple Network Management Protocol (SNMP)

SNMP is a service you can use to manage your network remotely. It consists of a central station maintained by an administrator running the SNMP management software and smaller files (agents) on each of your network devices, including routers, switches, and servers.

Several vendors have designed SNMP software, including HP, Cisco, IBM, and SolarWinds. There are also open source versions available. This software allows you to monitor bandwidth and activity on devices, such as logins and port status.

You can remotely configure or shut down ports and devices using SNMP. You can also configure it to send alerts when certain conditions are met, such as high bandwidth or ports going down. We will cover SNMP in more detail on Day 40 because it is part of the ICND2 syllabus.

Securing the Switch

Prevent Telnet Access

Telnet traffic sends the password in clear text, which means that it could easily be read on the configuration or by a network sniffer, if one was attached to your network.

Telnet is actually disabled by default (i.e., you need to set a password and, optionally, a username to get it working). However, if you still want to have remote access to the management ports, you can enable SSH traffic to the switch with the `transport input ssh` command, which was discussed earlier.

> Farai says – "The command `transport input all` is enabled by default for all VTY lines, while `transport input none` is enabled by default for other lines."

https://t.me/learningnets

Enable SSH

When possible, you should always use SSH instead of Telnet and SNMP to access your switches. SSH stands for secure shell and allows a secure exchange of information between two devices on a network. SSH uses public-key cryptography to authenticate the connecting device. Telnet and SNMP versions 1 and 2 are unencrypted and susceptible to packet sniffing (SNMP version 3 offers confidentiality – encryption of packets to prevent snooping by an unauthorised source). SSH, on the other hand, is encrypted.

To enable SSH you must have a version of IOS that supports encryption. A quick way to find this out is the `show version` command. Look for `K9` in the file name and/or the security statement of Cisco Systems.

```
Switch#sh version
Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICES K9-M), Version
12.2(35)SE1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 19-Dec-06 10:54 by antonio
Image text-base: 0x00003000, data-base: 0x01362CA0
ROM: Bootstrap program is C3560 boot loader
BOOTLDR: C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE
SOFTWARE (fc4)
Switch uptime is 1 hour, 8 minutes
System returned to ROM by power-on
System image file is "flash:/c3560-advipservicesk9-mz.122-35.SE1.bin"

This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately. A summary of U.S. laws governing Cisco cryptographic
products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
--More-
```

NOTE: If you do not have a security version of IOS, you must purchase a license for it.

For an encrypted connection , you will need to create a private/public key on the switch (see below). When you connect, use the public key to encrypt the data and the switch will use its private key to decrypt the data. For authentication, use your chosen username/password combination. Next, set the switch hostname and domain name because the private/public keys will be created using the hostname.domainname nomenclature. Obviously, it makes sense for the key to be named something representing the system.

Firstly, make sure that you have a hostname other than the default one, which is Switch. Next, add your domain name (this typically matches your FQDN in Windows Active Directory). Then, create the crypto key that will be used for encryption. The modulus will be the length of the keys you want to use, in the range from 360 to 2048, with the latter being the most secure; 1024 and above is considered secure. At this point, SSH is enabled on the switch. There are a few maintenance commands you should enter as well. The `ip ssh time-out 60` will time out

https://t.me/learningnets

any SSH connection that has been idle for 60 seconds. The `ip ssh authentication-retries 2` will reset the initial SSH connection if authentication fails two times. This will not prevent the user from establishing a new connection and retrying authentication. This process is illustrated in the output below:

```
Switch(config)#hostname SwitchOne
SwitchOne(config)#ip domain-name mydomain.com
SwitchOne(config)#crypto key generate rsa
Enter modulus: 1024
SwitchOne(config)#ip ssh time-out 60
SwitchOne(config)#ip ssh authentication-retries 2
```

You can optionally enable SSH version 2 with the `ip ssh version 2` command. Let's take a look at one of the keys. In this example, the key was generated for HTTPS. Because the key was automatically generated when enabling HTTPS, the name will also be auto-generated.

```
firewall#show crypto key mypubkey rsa
Key name: HTTPS_SS_CERT_KEYPAIR.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
306C300D 06092A86 4886F70D 01010105 00035B00 30580251 00C41B63 8EF294A1
DC0F7378 7EF410F6 6254750F 475DAD71 4E1CD15E 1D9086A8 BD175433 1302F403
2FD22F82 C311769F 9C75B7D2 1E50D315 EFA0E940 DF44AD5A F717BF17 A3CEDBE1
A6A2D601 45F313B6 6B020301 0001
```

To verify that SSH is enabled on the switch, enter the following command:

```
Switch#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 2
Switch#
```

If you have SSH enabled, you should probably disable Telnet and HTTP. When you enter the `transport input` command, any protocol entered after it is allowed. Any protocol not entered is not allowed. In the output below, you can see that only SSH is allowed:

```
line vty 0 15
transport input ssh
```

The following output shows that both SSH and Telnet are allowed:

```
line vty 0 15
transport input ssh telnet
```

You can disable HTTP access with one simple command:

```
Switch(config)#no ip http server
```

To view the status of the HTTP server on the switch:

```
Switch#show ip http server status
HTTP server status: Disabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path: flash:html
Maximum number of concurrent server connections allowed: 16
Server idle time-out: 180 seconds
```

https://t.me/learningnets

```
Server life time-out: 180 seconds
Maximum number of requests allowed on a connection: 25
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
HTTP secure server active session modules: ALL
```

You could also apply an access control list to the VTY lines and permit only SSH. We will cover access control lists on Day 9.

Set an Enable Secret Password

Global Configuration mode will permit a user to configure the switch or router and erase configurations, as well as reset passwords. You must protect this mode by setting a password or a secret password (which actually prevents the user from getting past User mode). The secret password will be displayed on the routers running the configuration file, whereas the `enable secret` password will be encrypted.

I've already mentioned that you can actually have both a password and an enable secret password on your router and switch, but this can cause confusion. Just set the enable secret password. The configuration file below illustrates how to issue a command without dropping back to Privileged mode by typing `do` before the command:

```
Switch1(config)#enable password cisco
Switch1(config)#do show run
Building configuration...
Current configuration: 1144 bytes
hostname Switch1
enable password cisco
```

Farai says – "You can encrypt the `enable secret` password with the `service password-encryption` command."

You can erase most lines of configuration by issuing it again with the word `no` before the command. It is also worth noting that, as Farai says, you can issue a `service password-encryption` command, but this only offers weak (level 7) encryption, whereas below, the secret password has strong (MD5) encryption :

```
Switch1(config)#no enable password
Switch1(config)#enable secret cisco
Switch1(config)#do show run
Building configuration...
Current configuration: 1169 bytes
hostname Switch1
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0 [strong level 5 password]
```

Services

You should always disable the services you are not going to use. Cisco has done a good job by not enabling insecure or rarely used services/protocols; however, you might want to disable

https://t.me/learningnets

them just to make sure. There are some services that are helpful as well. The majority of services are found under the command `service` in Global Configuration mode.

```
Switch(config)# service ?
compress-config  Compress the configuration file
config  TFTP load config files
counters  Control aging of interface counters
dhcp  Enable DHCP server and relay agent
disable-ip-fast-frag  Disable IP particle-based fast fragmentation
exec-callback  Enable EXEC callback
exec-wait  Delay EXEC startup on noisy lines
finger  Allow responses to finger requests
hide-telnet-addresses  Hide destination addresses in telnet command
linenumber  enable line number banner for each exec
nagle  Enable Nagle's congestion control algorithm
old-slip-prompts  Allow old scripts to operate with slip/ppp
pad  Enable PAD commands
password-encryption  Encrypt system passwords
password-recovery  Disable password recovery
prompt  Enable mode specific prompt
pt-vty-logging  Log significant VTY-Async events
sequence-numbers  Stamp logger messages with a sequence number
slave-log   Enable log capability of slave IPs
tcp-keepalives-in   Generate keepalives on idle incoming network
  connections
tcp-keepalives-out   Generate keepalives on idle outgoing network
  connections
tcp-small-servers   Enable small TCP servers (e.g., ECHO)
telnet-zeroidle  Set TCP window 0 when connection is idle
timestamps   Timestamp debug/log messages
udp-small-servers  Enable small UDP servers (e.g., ECHO)
```

Generally speaking, the most common services to enable/disable are listed below. The description of the service is in brackets [ ].

- ☐ `no service pad` [packet assembler/disassembler, used in asynchronous networking; rarely used]
- ☐ `no service config` [prevents the switch from getting its config file from the network]
- ☐ `no service finger` [disables the finger server; rarely used]
- ☐ `no ip icmp redirect` [prevents ICMP redirects, which can be used for router poisoning]
- ☐ `no ip finger` [another way to disable the finger service]

- ☐ `no ip gratuitous-arps` [disable to prevent man-in-the-middle attacks]
- ☐ `no ip source-route` [disables user-provided hop-by-hop routing to destination]
- ☐ `service sequence-numbers` [in each log entry, gives it a number and increases sequentially]
- ☐ `service tcp-keepalives-in` [prevents the router from keeping hung management sessions open]
- ☐ `service tcp-keepalives-out` [same as `service tcp-keepalives-in`]
- ☐ `no service udp-small-servers` [disables echo, chargen, discard, daytime; rarely used]
- ☐ `no service tcp-small-servers` [disables echo, chargen, discard; rarely used]
- ☐ `service timestamps debug datetime localtime show-timezone` [timestamps each logged packet (in debug mode) with the date and time, using local time, and shows the timezone]
- ☐ `service timestamps log datetime localtime show-timezone` [timestamps each logged packet (not in debug mode) with the date and time, using local time, and shows the timezone – very useful for observing the log file (especially if the clock is set up correctly)]

Change the Native VLAN

The native VLAN is used by the switch to carry specific protocol traffic, such as Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), Port Aggregation Protocol (PAgP), and Dynamic Trunking Protocol (DTP) information. The default native VLAN is always VLAN 1; however, the native VLAN can be manually changed to any valid VLAN number (except for 0 and 4096, because these are in the reserved range of VLANs).

You can verify the native VLAN with the commands (issued per interface) illustrated in the output below:

```
Switch#show interfaces FastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Having ports in VLAN 1 is considered a security vulnerability which allows hackers to gain access to network resources. To mitigate this problem, it is advisable to avoid putting any hosts into VLAN 1. You can also change the native VLAN on all trunk ports to an unused VLAN:

```
Switch(config-if)#switchport trunk native vlan 888
```

NOTE: This is one of the key objectives in the CCNA syllabus, so bear it in mind.

You can also prevent native VLAN data from passing on the trunk with the command below:

https://t.me/learningnets

```
Switch(config-if)#switchport trunk allowed vlan remove 888
```

Change the Management VLAN

You can also add an IP address to the switch to allow you to Telnet to it for management purposes. This is referred to as a Switch Virtual Interface (SVI). It is a wise precaution to have this management access in a VLAN other than VLAN 1, as shown in the output below:

```
Switch(config)#vlan 3

Switch(config-vlan)#interface vlan3

%LINK-5-CHANGED: Interface Vlan3, changed state to up

Switch(config-if)#ip address 192.168.1.1 255.255.255.0
```

Turn Off CDP

Cisco Discovery Protocol (CDP) will be covered later, but for now, you just need to know that it is turned on by default on most routers and switches universally and per interface, and its function is to discover attached Cisco devices. You may not want other Cisco devices to see information about your network devices, so you can turn this off, at least on the devices at the edge of your network which connect to other companies or your ISP.

Farai says – "CDP is not enabled by default on all platforms, such as ASR routers, for example."

In the output below, you can see how a router connected to my switch is able to see basic information when I issue the `show cdp neighbor detail` command:

```
Router#show cdp neighbor detail

Device ID: Switch1
Entry address(es):
Platform: Cisco 2960, Capabilities: Switch
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/2
Holdtime: 176
Version :

Cisco Internetwork Operating System Software
IOS (tm) C2960 Software (C2960-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
advertisement version: 2
Duplex: full

Router#
```

The command below will turn off CDP for the entire device:

```
Switch1(config)#no cdp run
```

To turn off CDP for a particular interface, issue the following command:

```
Switch1(config)#int FastEthernet0/2

Switch1(config-if)#no cdp enable
```

Add a Banner Message

A banner message will show when a user logs in to your router or switch. It won't offer any

https://t.me/learningnets

actual security but it will display a warning message of your choice. In the configuration below, I chose the letter Y as my delimiting character, which tells the router that I've finished typing my message:

```
Switch1(config)#banner motd Y
Enter TEXT message.  End with the character 'Y'.

KEEP OUT OR YOU WILL REGRET IT Y

Switch1(config)#
```

When I Telnet to the switch from my router, I can see the banner message. The mistake was choosing Y as the delimiting character because it cuts off my message:

```
Router#telnet 192.168.1.3

Trying 192.168.1.3 ...Open

KEEP OUT OR
```

Banner messages can be:

- Shown before the user sees the login prompt – MOTD (message of the day)
- Shown before the user sees the login prompt – Login
- Shown to the user after the login prompt – Exec (used when you want to hide information from unauthorised users)

Banner inputs as part of the labs in this book. I suggest that you learn to configure all three types and test them by logging in to the router. You will have different choices depending upon your platform and IOS:

```
Router(config)#banner ?
  LINE            c banner-text c, where 'c' is a delimiting character
  exec            Set EXEC process creation banner
  incoming        Set incoming terminal line banner
  login           Set login banner
  motd            Set Message of the Day banner
  prompt-timeout Set Message for login authentication timeout
  slip-ppp        Set Message for SLIP/PPP
```

Set a VTP Password

VTP ensures that accurate VLAN information is passed between the switches on your network. In order to protect these updates, you should add a VTP password on your switch (it should match on all switches in the VTP domain), as illustrated in the output below:

```
Switch1(config)#vtp domain 60days
Changing VTP domain name from NULL to 60days
Switch1(config)#vtp password cisco
Setting device VLAN database password to cisco
Switch1(config)#
```

Restrict VLAN Information

By default, switches permit all VLANs across the trunk links. You can change this by specifying

https://t.me/learningnets

which VLANs can pass, as illustrated in the following output:

```
Switch1(config)#int FastEthernet0/4
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#switchport trunk allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  none    no VLANs
  remove  remove VLANs from the current list

Switch1(config-if)#switchport trunk allowed vlan 7-12

Switch1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/4       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/4       7-12
```

Error Disable Recovery

A series of events can cause Cisco switches to put their ports into a special disabled mode called err-disabled. This basically means that a particular port has been disabled (shut down) due to an error. This error can have multiple causes, one of the most common being a violation of a port security policy. This is a normal behaviour when an unauthorised user tries to connect to a switch port and it prevents rogue devices from accessing the network.

An err-disabled port might look something like this:

```
Switch# show interface f0/1

FastEthernet0/1 is down, line protocol is down [err-disabled]

.....
```

In order to re-activate an err-disabled interface, manual intervention is necessary via issuing the `shutdown` and `no shutdown` commands on the interface (referred to a bouncing the port by network engineers). However, some situations might require automatic recovery of the original port state instead of waiting for an administrator to manually enable the port. The err-disable recovery mode functions by configuring the switch to automatically re-enable an err-disabled port after a certain period, based on the event that generated the failure. This provides granularity in deciding which events can be monitored by the err-disable recovery function.

The command to do this is the `errdisable recovery cause`, entered under Global Router Configuration mode:

```
Switch(config)#errdisable recovery cause ?
  all         Enable timer to recover from all causes
  bpduguard   Enable timer to recover from bpdu-guard error disable state
  dtp-flap    Enable timer to recover from dtp-flap error disable state
  link-flap   Enable timer to recover from link-flap error disable state
  pagp-flap   Enable timer to recover from pagp-flap error disable state
  rootguard   Enable timer to recover from root-guard error disable state
```

https://t.me/learningnets

```
  udld       Enable timer to recover from udld error disable state
......
```

The `errdisable recovery cause` command can vary based on the device model, but the most common parameters are:

- ☐ all
- ☐ arp-inspection
- ☐ bpduguard
- ☐ dhcp-rate-limit
- ☐ link-flap
- ☐ psecure-violation
- ☐ security-violation
- ☐ storm-control
- ☐ udld

The time after which the port is automatically restored is 300 seconds by default on most platforms, but this can be manually configured with the `errdisable recovery interval` global configuration command:

```
Switch(config)#errdisable recovery interval ?
  <30-86400>  timer-interval(sec)
```

The `show errdisable recovery` command will provide information about the active features monitored by the err-disable recovery function and about the interfaces being monitored, including the time left until the interface is enabled.

```
Switch#show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
arp-inspection               Disabled
bpduguard                    Disabled
channel-misconfig            Disabled
dhcp-rate-limit              Disabled
dtp-flap                     Disabled
gbic-invalid                 Disabled
inline-power                 Disabled
l2ptguard                    Disabled
link-flap                    Disabled
mac-limit                    Disabled
link-monitor-failure         Disabled
loopback                     Disabled
oam-remote-failure           Disabled
```

https://t.me/learningnets

```
pagp-flap                   Disabled
port-mode-failure           Disabled
psecure-violation           Enabled
security-violation          Disabled
sfp-config-mismatch         Disabled
storm-control               Disabled
udld                        Disabled
unicast-flood               Disabled
vmps                        Disabled
Timer interval: 300 seconds
Interfaces that will be enabled at the next timeout:
Interface       Errdisable reason       Time left(sec)
---------       -----------------       --------------
Fa0/0           psecure-violation       193
```

External Authentication Methods

Rather than store usernames and passwords locally, you can use a server which typically runs either AAA or TACACS+. The advantage to this method is not having to manually enter usernames and passwords on each individual router and switch. Instead, they are stored on the server database.

TACACS+ stands for Terminal Access Controller Access Control System Plus. It is a Cisco proprietary protocol that uses TCP port 49. TACACS+ provides access control for network devices, including routers, and network access servers via one or more centralised servers.

RADIUS stands for Remote Authentication Dial-In User Service. It is a system of distributed network security that secures remote access to the network and a client/server protocol that uses UDP. RADIUS is open standard.

If you have TACACS+ or RADIUS, you may wish to enable Authentication, Authorization, and Accounting (AAA). AAA is installed on a server and monitors a database of user accounts for the network. Users' access, protocols, connections, and disconnect reasons, as well as many other features, can be monitored.

Routers and switches can be configured to query the server when a user attempts to log in. The server then validates the user. You should not be expected to configure these protocols for the CCNA exam.

Router Clock and NTP

The time on a switch is often overlooked; however, it is very important. When you encounter security violations, SNMP traps, or logging of events, it uses a timestamp. If the time on your switch is incorrect, it will be difficult figuring out when the event happened. For example, let's take a look at the switch below and check the time:

```
Switch#show clock
*23:09:45.773 UTC Tue Mar 2 1993
```

https://t.me/learningnets

The time is not accurate, so let's change it. But first, let's set some attributes:

```
clock timezone CST -6
clock summer-time CDT recurring
clock summer-time CST recurring 2 Sun Mar 2:00 1 Sun Nov 2:00
```

First, let's set the time zone. I'm in the Central time zone and I'm 6 hours off of GMT. Next, tell the switch that summertime (the time change) is recurring. Finally, set what the summertime time really is. Now, let's set the time and date:

```
Switch#clock set 14:55:05 June 19 2007
Switch#
1d23h: %SYS-6-CLOCKUPDATE: System clock has been updated from 17:26:01 CST
Tue Mar 2 1993 to 14:55:05 CST Tue Jun 19 2007, configured from console by console.
Switch#show clock
14:55:13.858 CST Tue Jun 19 2007
```

Notice that the clock was set in Enable mode, not Configuration mode. Alternatively, you can use NTP. NTP stands for Network Time Protocol and it allows you to synchronise your switch's clock to an atomic clock, ensuring very accurate time.

```
Switch(config)#ntp server 134.84.84.84 prefer
Switch(config)#ntp server 209.184.112.199
```

You can see whether your clock has synchronised with your NTP sources with the following two commands:

```
Switch#show ntp associations
Switch#show ntp status
```

We will cover NTP in more detail on Day 40.

Shut Down Unused Ports

Unused or "empty" ports within any network device pose a security risk, as someone might plug a cable into them and connect an unauthorised device to the network. This can lead to a number of issues, including:

- Network not functioning as it should
- Network information vulnerable to outsiders

This is why you should shut down every port that is not used on routers, switches, and other network devices. Depending upon the device, the shutdown state might be the default, but you should always verify this.

Shutting down a port is done with the `shutdown` command under the Interface Configuration mode:

```
Switch#conf t
Switch(config)#int fa0/0

Switch(config-if)#shutdown
```

You can verify a port is in the shutdown state in multiple ways, one of which is using the `show ip interface brief` command:

```
Router(config-if)#do show ip interface brief
```

https://t.me/learningnets

```
Interface              IP-Address      OK? Method Status                Protocol
```

```
FastEthernet0/0      unassigned      YES unset  administratively down down
FastEthernet0/1      unassigned      YES unset  administratively down down
```

Note that the administratively down status means that the port has been manually shut down.

Another way to verify the shutdown state is using the `show interface` command:

```
Router#show interface fa0/0
FastEthernet0/0 is administratively down, line protocol is down
  Hardware is Gt96k FE, address is c200.27c8.0000 (bia c200.27c8.0000)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
```

.....

Cisco Discovery Protocol (CDP)

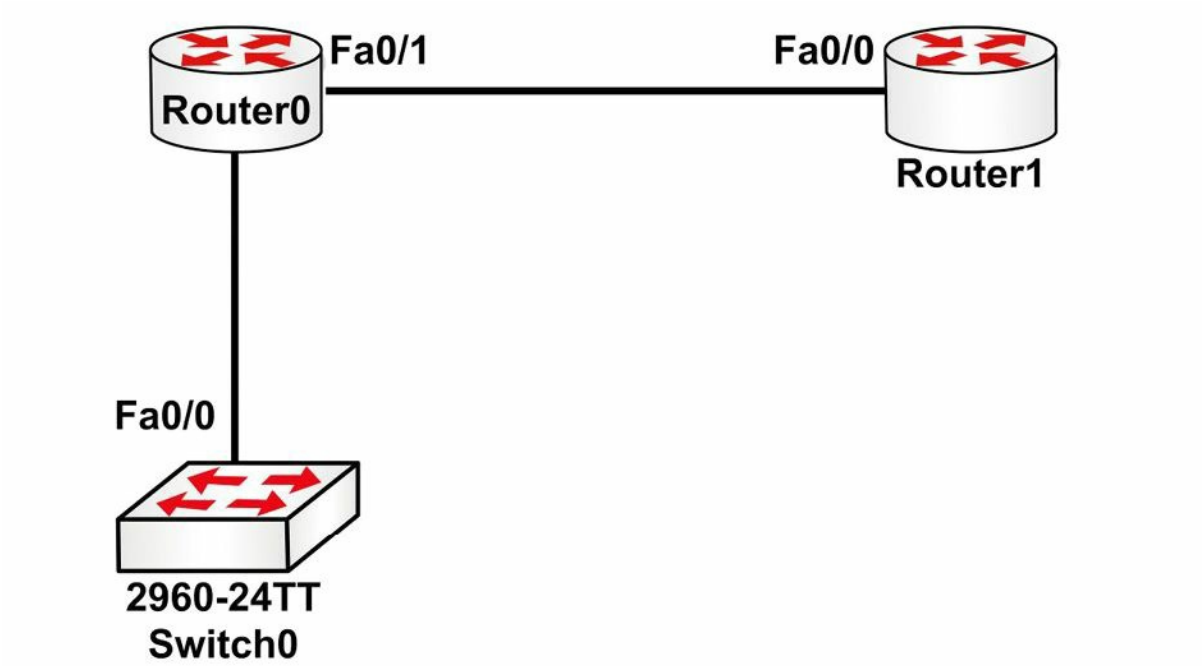
Now is as good a time as any to discuss Cisco Discovery Protocol.

CDP is a hot exam topic because it provides a means to discover information about network devices before any configuration has been applied. This is a very useful troubleshooting tool; however, it also presents a security risk.

CDP is Cisco proprietary, which means it will only work on Cisco devices. It is a Layer 2 service used by devices to advertise and discover basic information about directly connected neighbours. The IEEE version of CDP is Link Layer Discovery Protocol (LLDP), but this is not included in the CCNA syllabus.

Because CDP is a Layer 2 service it does not require IP addresses to be conifigured in order to exchange information. The interface need only be enabled. If an IP address is configured, then this will be included in the CDP message.

CDP is a very powerful troubleshooting tool and you will be expected to understand how to use it in the exam. Figure 4.1 below shows CDP outputs from Router 0. Imagine if you were asked to troubleshoot this network but had no topology diagram to work from.



https://t.me/learningnets

Figure 4.1 – CDP Outputs from Router 0

The following configuration outputs correspond to Figure 4.1:

```
Router0#show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H -
Host, I - IGMP, r - Repeater, P - Phone

Device ID  Local Interface  Holdtime  Capability  Platform   Port

Switch     Fas 0/0          165       S           2960       Fas 0/1

Router     Fas 0/1          169       R           C1841      Fas 0/0

Router0#
```

You can see more information by adding the `detail` command to the end:

```
Router0#show cdp neighbors detail

Device ID: Switch

Entry address(es):

Platform: cisco 2960, Capabilities: Switch

Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/1

Holdtime: 178

Version :

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE
SOFTWARE (fc1)

Copyright (c) 1986-2005 by Cisco Systems, Inc.

Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2

Duplex: full

---------------------------

Device ID: Router

Entry address(es):

  IP address : 192.168.1.2

Platform: cisco C1841, Capabilities: Router

Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/0

Holdtime: 122

Version :

Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2007 by Cisco Systems, Inc.

Compiled Wed 18-Jul-07 04:52 by pt_team

advertisement version: 2

Duplex: full
```

Now you can see the IOS release, model, IP address, and other information. Remember that you still haven't configured an IP address on Router 0 yet.

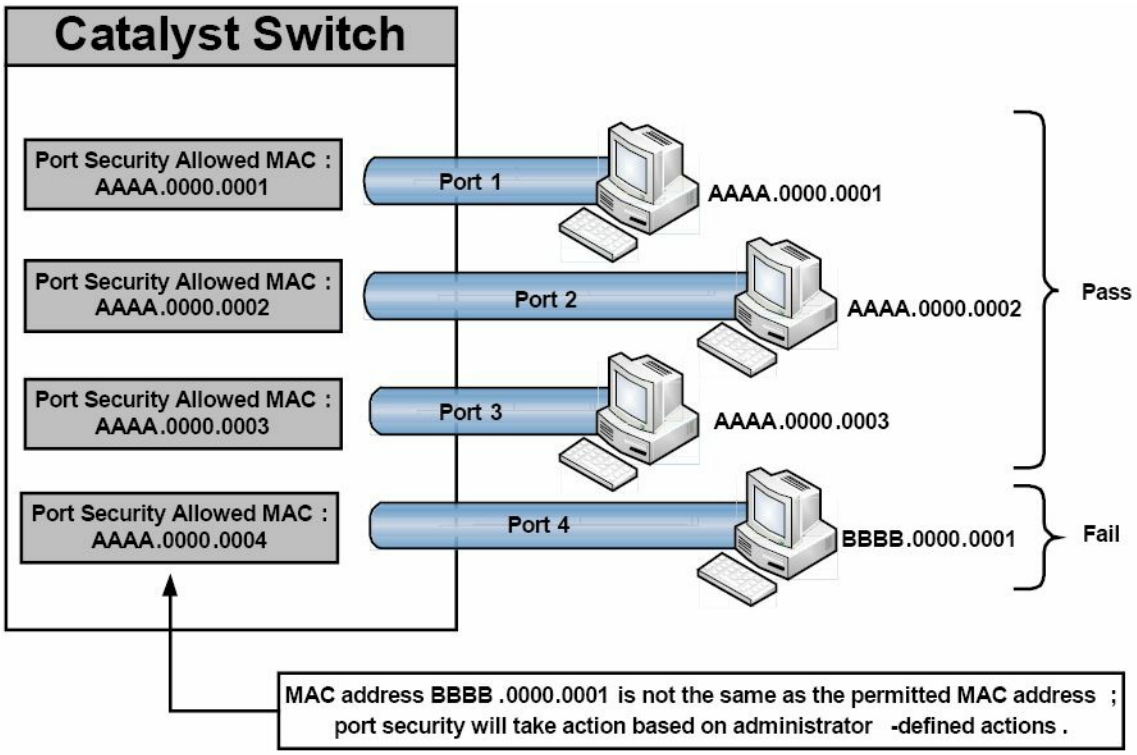
https://t.me/learningnets

We've already covered how to disable CDP on the device or interface only. Two other commands are `show cdp`, which displays protocol information for the device, and `show cdp entry <Router>`, which shows information about a specific device by imputting the name. I recommend that you spend some time checking CDP outputs during the labs you will configure in this guide.

```
Router0#show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
Router0#show cdp ?
  entry      Information for specific neighbor entry
  interface  CDP interface status and configuration
  neighbors  CDP neighbor entries
  traffic    CDP statistics
  |          Output modifiers
  <cr>
```

Switch Port Security

The port security feature is a dynamic Catalyst switch feature that secures switch ports, and ultimately the CAM table, by limiting the number of MAC addresses that can be learned on a particular port or interface. With the port security feature, the switch maintains a table that is used to identify which MAC address (or addresses) can access which local switch port. Additionally, the switch can also be configured to allow only a certain number of MAC addresses to be learned on any given switch port. Port security is illustrated below in Figure 4.2:



https://t.me/learningnets

Figure 4.2 – Port Security Operation

Figure 4.2 shows four ports on a Catalyst switch configured to allow a single MAC address via the port security feature. Ports 1 through 3 are connected to hosts whose MAC address matches the address permitted by port security. Assuming no other filtering is in place, these hosts are able to forward frames through their respective switch ports. Port 4, however, has been configured to allow a host with MAC address AAAA.0000.0004, but instead a host with MAC address BBBB.0000.0001 has been connected to this port. Because the host MAC and the permitted MAC are not the same, port security will take appropriate action on the port as defined by the administrator. The valid port security actions will be described in detail in a subsequent section.

The port security feature is designed to protect the switched LAN from two primary methods of attack. These attack methods, which will be described in the following sections, are:

- CAM table overflow attacks
- MAC spoofing attacks

CAM Table Overflow Attacks

Switch CAM tables are storage locations that contain lists of known MAC addresses on physical ports, as well as their VLAN parameters. Dynamically learned contents of the switch CAM table, or MAC address table, can be viewed by issuing the `show mac-address-table dynamic` command, as illustrated in the following output:

```
VTP-Server-1#show mac-address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   2    000c.cea7.f3a0    DYNAMIC     Fa0/1
   2    0013.1986.0a20    DYNAMIC     Fa0/2
   6    0004.c16f.8741    DYNAMIC     Fa0/3
   6    0030.803f.ea81    DYNAMIC     Fa0/4
   8    0004.c16f.8742    DYNAMIC     Fa0/5
   8    0030.803f.ea82    DYNAMIC     Fa0/6
Total Mac Addresses for this criterion: 6
```

Switches, like all computing devices, have finite memory resources. This means that the CAM table has a fixed, allocated memory space. CAM table overflow attacks target this limitation by flooding the switch with a large number of randomly generated invalid source and destination MAC addresses until the CAM table fills up and the switch is no longer able to accept new entries. In such situations, the switch effectively turns into a hub and simply begins to broadcast all newly received frames to all ports (within the same VLAN) on the switch, essentially turning the VLAN into one big Broadcast domain.

CAM table attacks are easy to perform because common tools, such as MACOF and DSNIFF, are

https://t.me/learningeasy

readily available to perform these activities. While increasing the number of VLANs (which reduces the size of Broadcast domains) can assist in reducing the effects of CAM table attacks, the recommended security solution is to configure the port security feature on the switch.

MAC Spoofing Attacks

MAC address spoofing is used to spoof a source MAC address in order to impersonate other hosts or devices on the network. Spoofing is simply a term that means masquerading or pretending to be someone you are not. The primary objective of MAC spoofing is to confuse the switch and cause it to believe that the same host is connected to two ports, which causes the switch to attempt to forward frames destined to the trusted host to the attacker as well. Figure 4.3 below shows the CAM table of a switch connected to four different network hosts:

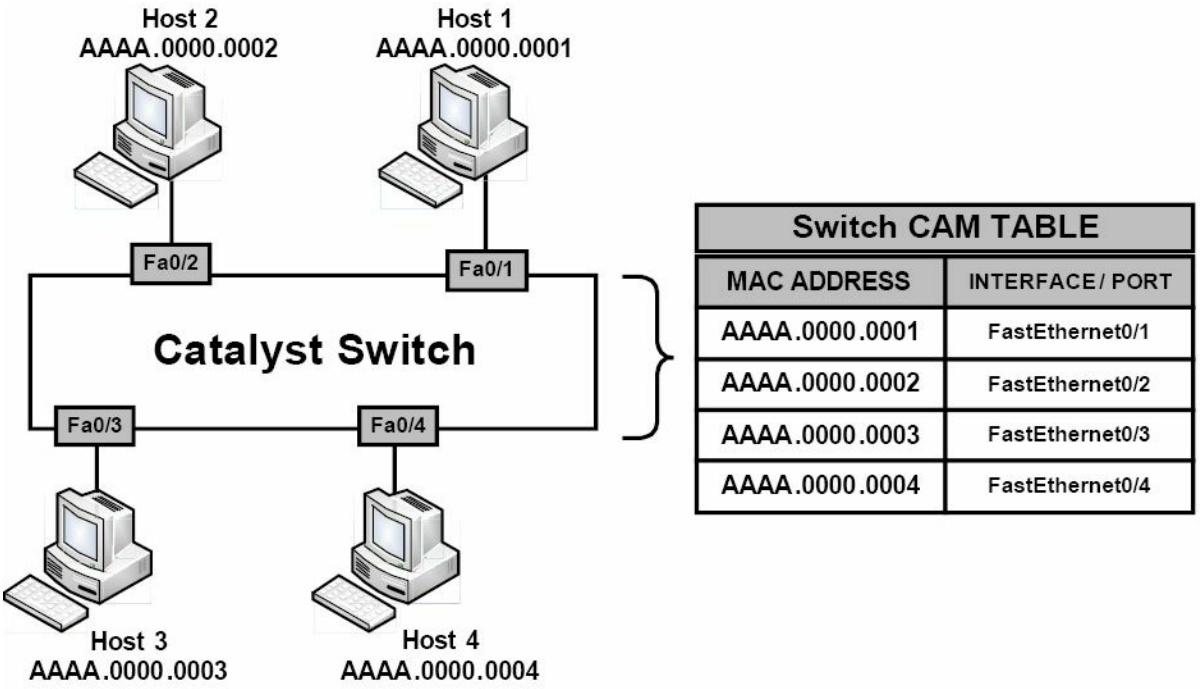


Figure 4.3 – Building the Switch CAM Table

In Figure 4.3, the switch is operating normally and, based on the CAM table entries, knows the MAC addresses for all the devices connected to its ports. Based on the current CAM table, if Host 4 wanted to send a frame to Host 2, the switch would simply forward the frame out of its FastEthernet0/2 interface toward Host 2.

Now, assume that Host 1 has been compromised by an attacker who wants to receive all traffic destined for Host 2. By using MAC address spoofing, the attacker crafts an Ethernet frame using the source address of Host 2. When the switch receives this frame, it notes the source MAC address and overwrites the CAM table entry for the MAC address of Host 2, and points it to port FastEthernet0/1 instead of FastEthernet0/2, where the real Host 2 is connected. This concept is illustrated below in Figure 4.4:

https://t.me/learningnets

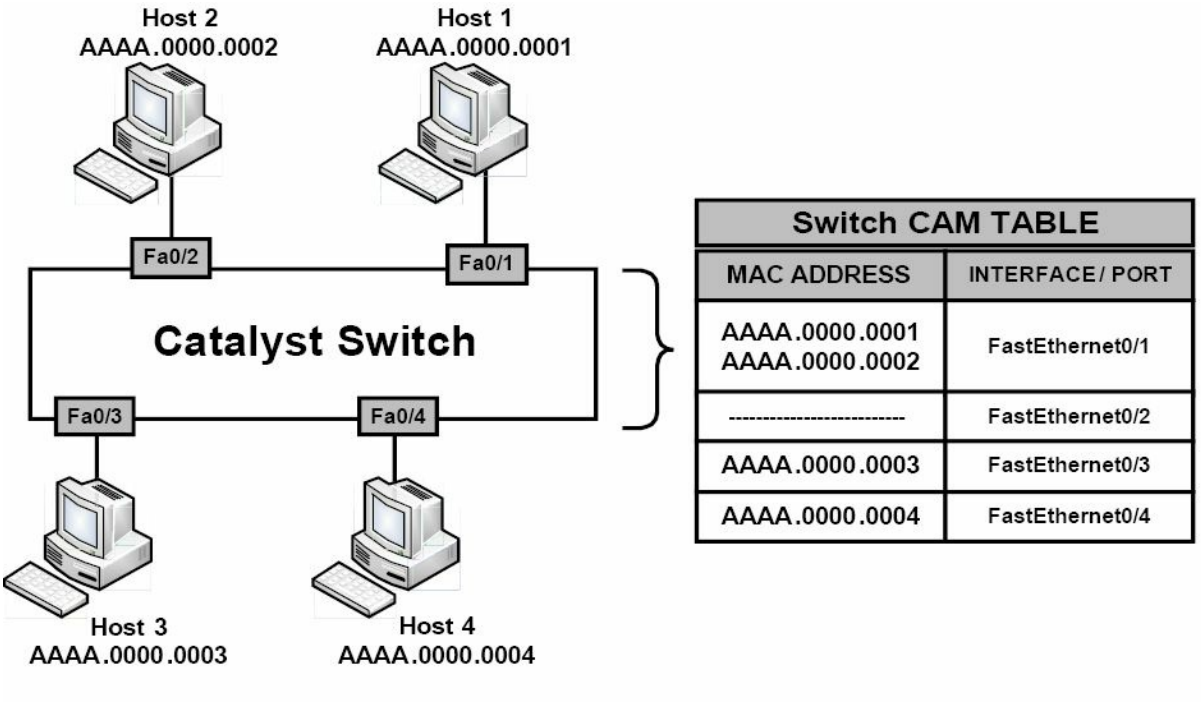


Figure 4.4 – MAC Address Spoofing

Referencing Figure 4.4, when Host 3 or Host 4 attempts to send frames to Host 2, the switch will forward them out of FastEthernet0/1 to Host 1 because the CAM table has been poisoned by a MAC spoofing attack. When Host 2 sends another frame, the switch relearns its MAC address from FastEthernet0/2 and rewrites the CAM table entry once again to reflect this change. The result is a tug-of-war between Host 2 and Host 1 as to which host owns this MAC address.

In addition, this confuses the switch and causes repetitive rewrites of MAC address table entries, causing a Denial of Service (DoS) attack on the legitimate host (i.e., Host 2). If the number of spoofed MAC addresses used is high, this attack could have serious performance consequences for the switch that is constantly rewriting its CAM table. MAC address spoofing attacks can be mitigated by implementing port security.

Port Security Secure Addresses

The port security feature can be used to specify which specific MAC address is permitted access to a switch port, as well as to limit the number of MAC addresses that can be supported on a single switch port. The methods of port security implementation described in this section are as follows:

- Static secure MAC addresses
- Dynamic secure MAC addresses
- Sticky secure MAC addresses

Static secure MAC addresses are statically configured by network administrators and are stored in the MAC address table, as well as in the switch configuration. When static secure MAC addresses are assigned to a secure port, the switch will not forward frames that do not have a source MAC address that matches the configured static secure MAC address or addresses.

Dynamic secure MAC addresses are dynamically learned by the switch and are stored in the MAC address table. However, unlike static secure MAC addresses, dynamic secure MAC address

https://t.me/learningnets

entries are removed from the switch when the switch is reloaded or powered down. These addresses must then be relearned by the switch when it boots up again.

Sticky secure MAC addresses are a mix of static secure MAC addresses and dynamic secure MAC addresses. These addresses can be learned dynamically or configured statically and are stored in the MAC address table, as well as in the switch running configuration. This means that when the switch is powered down or rebooted, it will not need to dynamically discover the MAC addresses again because they are already saved in the configuration file (if you save the running configuration).

Port Security Actions

Once port security has been enabled, administrators can define the actions the switch will take in the event of a port security violation. Cisco IOS software allows administrators to specify four different actions to take when a violation occurs, as follows:

- Protect
- Shutdown (default)
- Restrict
- Shutdown VLAN (outside of the CCNA syllabus)

The protect option forces the port into Protected Port mode. In this mode, the switch will simply discard all Unicast or Multicast frames with unknown source MAC addresses. When the switch is configured to protect a port, it will not send out a notification when operating in Protected Port mode, meaning that administrators would never know when any traffic was prevented by the switch port operating in this mode.

The shutdown option places a port in an err-disabled state when a port security violation occurs. The corresponding port LED on the switch is also turned off when this configured action mode is used. In Shutdown mode, the switch sends out an SNMP trap and a syslog message, and the violation counter is incremented. This is the default action taken when port security is enabled on an interface.

The restrict option is used to drop packets with unknown MAC addresses when the number of secure MAC addresses reaches the administrator-defined maximum limit for the port. In this mode, the switch will continue to restrict additional MAC addresses from sending frames until a sufficient number of secure MAC addresses is removed, or the number of maximum allowable addresses is increased. As is the case with the shutdown option, the switch sends out an SNMP trap and a syslog message, and the violation counter is incremented.

The shutdown VLAN option is similar to the shutdown option; however, this option shuts down a VLAN instead of the entire switch port. This configuration could be applied to ports that have more than one single VLAN assigned to them, such as a voice VLAN and a data VLAN, as well as to trunk links on the switches.

Configuring Port Security

Before configuring port security, it is recommended that the switch port be statically configured

https://t.me/learningnets

as a Layer 2 access port (it can only be configured on static access or trunk ports, not on dynamic ports). This configuration is illustrated in the following output:

```
VTP-Server-1(config)#interface FastEthernet0/1
VTP-Server-1(config-if)#switchport
VTP-Server-1(config-if)#switchport mode access
```

NOTE: The `switchport` command is not required in Layer 2-only switches, such as the Catalyst 2950 and Catalyst 2960 series switches. However, it must be used on Multilayer switches, such as the Catalyst 3750, Catalyst 4500, and Catalyst 6500 series switches.

By default, port security is disabled; however, this feature can be enabled using the `switchport port-security [mac-address {mac-address} [vlan {vlan-id | {access | voice}}] | mac-address {sticky} [mac-address | vlan {vlan-id | {access | voice}}] [maximum {value} [vlan {vlan-list | {access | voice}}]]` interface configuration command. The options that are available with this command are described below in Table 4.1:

Table 4.1 – Port Security Configuration Keywords

Keyword	Description
mac-address {mac-address}	This keyword is used to specify a static secure MAC address. You can add additional secure MAC addresses up to the maximum value configured.
vlan {vlan id}	This keyword should be used on a trunk port only to specify the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used.
vlan {access}	This keyword should be used on an access port only to specify the VLAN as an access VLAN.
vlan {voice}	This keyword should be used on an access port only to specify the VLAN as a voice VLAN. This option is only available if a voice VLAN is configured on the specified port.
mac-address {sticky} [mac-address]	This keyword is used to enable dynamic or sticky learning on the specified interface or to configure a static secure MAC address.
maximum {value}	This keyword is used to specify the maximum number of secure addresses that can be learned on an interface. The default is 1.

Configuring Static Secure MAC Addresses

The following output illustrates how to enable port security on an interface and to configure a static secure MAC address of 001f:3c59:d63b on a switch access port:

```
VTP-Server-1(config)#interface GigabitEthernet0/2
VTP-Server-1(config-if)#switchport
VTP-Server-1(config-if)#switchport mode access
VTP-Server-1(config-if)#switchport port-security
VTP-Server-1(config-if)#switchport port-security mac-address 001f.3c59.d63b
```

The following output illustrates how to enable port security on an interface and to configure a static secure MAC address of 001f:3c59:d63b in VLAN 5 on a switch trunk port:

```
VTP-Server-1(config)#interface GigabitEthernet0/2
VTP-Server-1(config-if)#switchport
VTP-Server-1(config-if)#switchport trunk encapsulation dot1q
VTP-Server-1(config-if)#switchport mode trunk
```

https://t.me/learningnets

```
VTP-Server-1(config-if)#switchport port-security
VTP-Server-1(config-if)#switchport port-security mac-address 001f.3c59.d63b  vlan 5
```

The following output illustrates how to enable port security on an interface and to configure a static secure MAC address of 001f:3c59:5555 for VLAN 5 (the data VLAN) and a static secure MAC address of 001f:3c59:7777 for VLAN 7 (the voice VLAN) on a switch access port:

```
VTP-Server-1(config)#interface GigabitEthernet0/2
VTP-Server-1(config-if)#switchport
VTP-Server-1(config-if)#switchport mode access
VTP-Server-1(config-if)#switchport access vlan 5
VTP-Server-1(config-if)#switchport voice vlan 7
VTP-Server-1(config-if)#switchport port-security
VTP-Server-1(config-if)#switchport port-security maximum 2
VTP-Server-1(config-if)#switchport port-security mac-address 001f.3c59.5555  vlan access
VTP-Server-1(config-if)#switchport port-security mac-address 001f.3c59.7777 vlan voice
```

It is very important to remember that when enabling port security on an interface that is also configured with a voice VLAN in conjunction with the data VLAN, the maximum allowed secure addresses on the port should be set to 2. This is performed via the `switchport port-security maximum 2` interface configuration command, which is included in the output above.

One of the two MAC addresses is used by the IP phone and the switch learns about this address on the voice VLAN. The other MAC address is used by a host (such as a PC) that may be connected to the IP phone. This MAC address will be learned by the switch on the data VLAN.

Verifying Static Secure MAC Address Configuration

Global port security configuration parameters can be validated by issuing the `show port-security` command. The following shows the output printed by this command based on default values:

```
VTP-Server-1#show port-security
Secure Port MaxSecureAddr  CurrentAddr SecurityViolation  Security Action
            (Count)        (Count)       (Count)
-----------------------------------------------------
Gi0/2       1               1             0              Shutdown
-----------------------------------------------------------------
Total Addresses in System : 1
Max Addresses limit in System : 1024
```

As seen in the output above, by default, only a single secure MAC address is permitted per port. In addition, the default action in the event of a violation is to shut down the port. The text in bold indicates that only a single secured address is known, which is the static address configured on the interface. The same can also be confirmed by issuing the `show port-security interface [name]` command, as illustrated in the following output:

```
VTP-Server-1#show port-security interface gi0/2
```

https://t.me/learningnets

```
Port Security : Enabled
Port status : SecureUp
Violation mode : Shutdown
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Aging time : 0 mins
Aging type : Absolute
SecureStatic address aging : Disabled
Security Violation count : 0
```

NOTE: The modification of the other default parameters in the output above will be described in detail as we progress through this section.

To see the actual configured static secure MAC address on the port, the `show port-security address` or the `show running-config interface [name]` command must be used. The following output illustrates the `show port-security address` command:

```
VTP-Server-1#show port-security address
          Secure Mac Address Table
-----------------------------------------------------------------
Vlan    Mac Address       Type                  Ports   Remaining Age
                                                          (mins)
----    -----------       ----                  -----   -----------
   1    001f.3c59.d63b    SecureConfigured      Gi0/2       -
-----------------------------------------------------------------
Total Addresses in System : 1
Max Addresses limit in System : 1024
```

Configuring Dynamic Secure MAC Addresses

By default, when port security is enabled on a port, the port will dynamically learn and secure one MAC address without any further configuration from the administrator. To allow the port to learn and secure more than a single MAC address, the `switchport port-security maximum [number]` command must be used. Keep in mind that the `[number]` keyword is platform-dependent and will vary on different Cisco Catalyst switch models.



Real-World Implementation

In production networks with Cisco Catalyst 3750 switches, it is always a good idea to determine what the switch will be used for, and then select the appropriate Switch Database Management

https://t.me/learningnets

(SDM) template via the `sdm prefer {access | default | dual-ipv4-and-ipv6 {default | routing | vlan} | routing | vlan} [desktop]` global configuration command.

Each template allocates system resources to best support the features being used or that will be used. By default, the switch attempts to provide a balance between all features. However, this may impose a limit on the maximum possible values for other available features and functions. An example would be the maximum possible number of secure MAC addresses that can be learned or configured when using port security.

The following output illustrates how to configure a switch port to dynamically learn and secure up to two MAC addresses on interface GigabitEthernet0/2:

```
VTP-Server-1(config)#interface GigabitEthernet0/2
VTP-Server-1(config-if)#switchport
VTP-Server-1(config-if)#switchport mode access
VTP-Server-1(config-if)#switchport port-security
VTP-Server-1(config-if)#switchport port-security maximum 2
```

Verifying Dynamic Secure MAC Addresses

Dynamic secure MAC address configuration can be verified using the same commands as those illustrated in the static secure address configuration examples, with the exception of the `show running-config` command. This is because, unlike static or sticky secure MAC addresses, all dynamically learned addresses are not saved in the switch configuration and are removed if the port is shut down. These same addresses must then be relearned when the port comes back up. The following output illustrates the `show port-security address` command, which shows an interface configured for secure dynamic MAC address learning:

```
VTP-Server-1#show port-security address
          Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                          (mins)
----    -----------       ----                -----   ------------
   1    001d.09d4.0238    SecureDynamic       Gi0/2       -
   1    001f.3c59.d63b    SecureDynamic       Gi0/2       -
------------------------------------------------------------------
Total Addresses in System : 2
Max Addresses limit in System : 1024
```

Configuring Sticky Secure MAC Addresses

The following output illustrates how to configure dynamic sticky learning on a port and restrict the port to dynamically learn up to a maximum of 10 MAC addresses:

```
VTP-Server-1(config)#interface GigabitEthernet0/2
VTP-Server-1(config-if)#switchport
VTP-Server-1(config-if)#switchport mode access
```

https://t.me/learningnets

```
VTP-Server-1(config-if)#switchport port-security
VTP-Server-1(config-if)#switchport port-security mac-address sticky
VTP-Server-1(config-if)#switchport port-security maximum 10
```

Based on the configuration above, by default, up to 10 addresses will be dynamically learned on interface GigabitEthernet0/2 and will be added to the current switch configuration. When sticky address learning is enabled, MAC addresses learned on each port are automatically saved to the current switch configuration and added to the address table. The following output shows the dynamically learned MAC addresses (in bold font) on interface GigabitEthernet0/2:

```
VTP-Server-1#show running-config interface GigabitEthernet0/2
Building configuration...
Current configuration : 550 bytes
!
interface GigabitEthernet0/2
switchport
switchport mode access
switchport port-security
switchport port-security maximum 10
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0004.c16f.8741
switchport port-security mac-address sticky 000c.cea7.f3a0
switchport port-security mac-address sticky 0013.1986.0a20
switchport port-security mac-address sticky 001d.09d4.0238
switchport port-security mac-address sticky 0030.803f.ea81
...
```

The MAC addresses in bold text in the output above are dynamically learned and added to the current configuration. No manual administrator configuration is required to add these addresses to the configuration. By default, sticky secure MAC addresses are not automatically added to the startup configuration (NVRAM). To ensure that this information is saved to NVRAM, which means that these addresses are not relearned when the switch is restarted, it is important to remember to issue the `copy running-config startup-config` command, or the `copy system:running-config nvram:startup-config` command, depending upon the IOS version of the switch on which this feature is implemented. The following output illustrates the `show port-security address` command on a port configured for sticky address learning:

```
VTP-Server-1#show port-security address
          Secure Mac Address Table
------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                          (mins)
----    -----------       ----                -----   -----------
   1    0004.c16f.8741    SecureSticky        Gi0/2       -
```

https://t.me/learningnets

```
   1    000c.cea7.f3a0    SecureSticky        Gi0/2       -
   1    0013.1986.0a20    SecureSticky        Gi0/2       -
   1    001d.09d4.0238    SecureSticky        Gi0/2       -
   1    0030.803f.ea81    SecureSticky        Gi0/2       -
------------------------------------------------------------------

Total Addresses in System : 5
Max Addresses limit in System : 1024
```

You can also set an aging time and type on the switch, but this is going beyond the CCNA-level requirements. (Have a try on your own time if you wish.)

Configuring the Port Security Violation Action

As stated earlier, Cisco IOS software allows administrators to specify four different actions to take when a violation occurs, as follows:

- Protect
- Shutdown (default)
- Restrict
- Shutdown VLAN (this is outside the CCNA syllabus)

These options are configured using the `switchport port-security [violation {protect | restrict | shutdown | shutdown vlan}]` interface configuration command. If a port is shut down due to a security violation, it will show as `errdisabled`, and the `shutdown` and then `no shutdown` command will need to be applied to bring it back up.

```
Switch#show interfaces FastEthernet0/1 status
Port     Name          Status       Vlan      Duplex  Speed  Type
Fa0/1                  errdisabled  100       full    100    100BaseSX
```

Cisco do want you to know which violation action triggers an SNMP message for the network administrator and a logging message, so here is that information for you in Table 4.2 below:

Table 4.2 – Port Security Violation Actions

Mode	Port Action	Traffic	Syslog	Violation Counter
Protect	Protected	Unknown MACs discarded	No	No
Shutdown	Errdisabled	Disabled	Yes and SNMP trap	Incremented
Restrict	Open	# of excess MAC traffic denied	Yes and SNMP trap	Incremented

Make sure that you memorise the table above for the exam!

The following output illustrates how to enable sticky learning on a port for a maximum of 10 MAC addresses. In the event that an unknown MAC address (e.g., an eleventh MAC address) is

https://t.me/learningnets

detected on the port, the port will be configured to drop the received frames:

```
VTP-Server-1(config)#interface GigabitEthernet0/2
VTP-Server-1(config-if)#switchport port-security
VTP-Server-1(config-if)#switchport port-security mac-address sticky
VTP-Server-1(config-if)#switchport port-security maximum 10
VTP-Server-1(config-if)#switchport port-security violation restrict
```

Verifying the Port Security Violation Action

The configured port security violation action is validated via the `show port-security` command, as shown in the following output:

```
VTP-Server-1#show port-security
Secure Port  MaxSecureAddr CurrentAddr SecurityViolation  Security Action
                (Count)        (Count)      (Count)
Gi0/2           10              5             0         Restrict
Total Addresses in System : 5
Max Addresses limit in System : 1024
```

If logging is enabled and either the Restrict mode or the Shutdown Violation mode is configured on the switch, messages similar to those shown in the following output will be printed on the switch console, logged into the local buffer, or sent to a syslog server:

```
VTP-Server-1#show logging
...
[Truncated Output]
...
04:23:21: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0013.1986.0a20 on port Gi0/2.
04:23:31: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 000c.cea7.f3a0 on port Gi0/2.
04:23:46: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0004.c16f.8741 on port Gi0/2.
```

One final point is that switch security can be configured on Packet Tracer, but many of the commands and `show` commands don’t work.

https://t.me/learningnets

Day 4 Questions

1. Write out the two ways of configuring console passwords. Write the actual commands.
2. Which command will permit only SSH traffic into the VTY lines?
3. Which command will encrypt a password with level 7 encryption?
4. Name the eight levels of logging available on the router.
5. Why would you choose SSH access over Telnet?
6. Your three options upon violation of your port security are protect, _____, and _____.
7. How would you hard set a port to accept only MAC 0001.c74a.0a01?
8. Which command turns off CDP for a particular interface?
9. Which command turns off CDP for the entire router or switch?
10. Which command adds a password to your VTP domain?
11. Which command would permit only VLANs 10 to 20 over your interface?

https://t.me/learningnets

Day 4 Answers

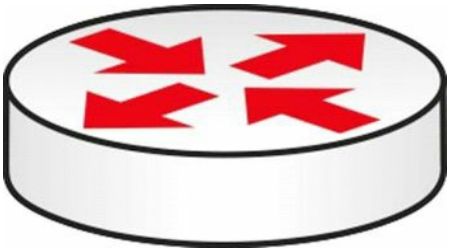
1. The `password xxx` and `login local` commands (username and password previously configured).
2. The `transport input ssh` command.
3. The `service password-encryption` command.
4. Alerts, critical, debugging, emergencies, errors, informational, notifications, and warnings.
5. SSH offers secure, encrypted traffic.
6. Shutdown and restrict.
7. Issue the `switchport port-security mac-address x.x.x.x` command.
8. The `no cdp enable` command.
9. The `no cdp run` command.
10. The `vtp password xxx` command.
11. The `switchport trunk allowed vlan 10-20` command.

https://t.me/learningnets

Day 4 Labs

Basic Router Security Lab

Topology



Purpose

Learn some basic steps to take to lock down your router.

Walkthrough

1. Log in using Protect Enable mode with an enable secret password. Test this by logging out of Privileged mode and then logging back in.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret cisco
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#exi
Router con0 is now available
Press RETURN to get started.
Router>en
Password:
Router#
```

2. Set an enable password and then add service password encryption. This is rarely done on live routers because it is not secure.

```
Router(config)#no enable secret
Router(config)#enable password cisco
Router(config)#service pass
Router(config)#service password-encryption
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show run
Building configuration...
Current configuration: 480 bytes
!
```

https://t.me/learningnets

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router
!
enable password 7 0822455D0A16
```

3. Protect the Telnet lines. Set a local username and password and have users enter this when connecting to the router.

```
Router(config)#line vty 0 ?
  <1-15>  Last Line number
  <cr>
Router(config)#line vty 0 15
Router(config-line)#login local
Router(config-line)#exit
Router(config)#username in60days password cisco
Router(config)#
```

You have tested Telnet before, but feel free to add a PC and Telnet into the router so you are prompted for a username and password.

4. Protect the console port with a password. Set one directly on the console port.

```
Router(config)#line console 0
Router(config-line)#password cisco
```

You can test this by unplugging and plugging your console lead back into the router. You can also protect the auxiliary port on your router if you have one:

```
Router(config)#line aux 0
Router(config-line)#password cisco
```

5. Protect the Telnet lines by permitting only SSH traffic in. You can also permit only SSH traffic outbound. You will need a security image for this command to work.

```
Router(config)#line vty 0 15
Router(config-line)#transport input ssh
Router(config-line)#transport output ssh
```

6. Add a banner message of the day (MOTD). Set the character which tells the router you have finished your message as “X” (the delimiting character).

```
Router(config)#banner motd X
Enter TEXT message.  End with the character 'X'.
Do not use this router without authorization. X
Router(config)#
Router(config)#exit
```

https://t.me/learningnets

```
Router#
%SYS-5-CONFIG_I: Configured from console by console
Exit
Router con0 is now available
Press RETURN to get started.
Do not use this router without authorization.
Router>
```

7. Turn off CDP on the entire router. You could disable it on an interface only with the `no cdp enable interface` command.

```
Router(config)#no cdp run
```

You can test whether this is working by connecting a switch or router to your router before you turn off CDP and issuing the `show cdp neighbor (detail)` command.

8. Set the router to send logging messages to a host on the network.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#logging ?
  A.B.C.D   IP address of the logging host
  buffered  Set buffered logging parameters
  console   Set console logging parameters
  host      Set syslog server IP address and parameters
  on        Enable logging to all enabled destinations
  trap      Set syslog server logging level
  userinfo  Enable logging of user info on privileged mode enabling
Router(config)#logging 10.1.1.1
```

Basic Switch Security Lab

Topology



Please note that your switch will need to have a security image which permits basic security settings.

Purpose

Learn how to apply basic security settings to a Cisco switch.

Walkthrough

1. Connect a PC or laptop to your switch. In addition, set up a console connection for your configuration. The port to which you connect your PC will be the one you configure

https://t.me/learningnets

security settings on in this lab. I have chosen FastEthernet 0/1 on my switch.

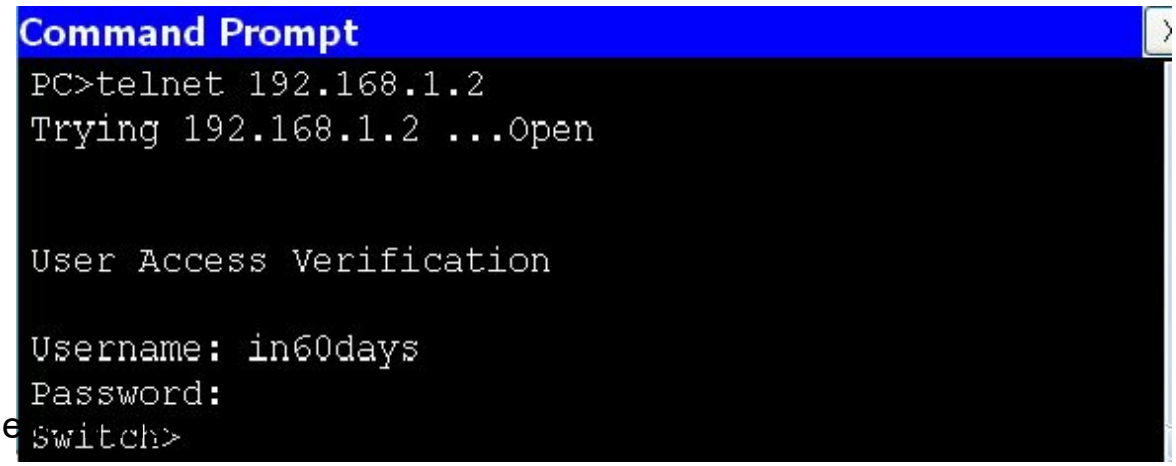
2. Log in to the VTY lines and set up Telnet access referring to a local username and password.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line vty 0 ?
  <1-15>  Last Line number
  <cr>
Switch(config)#line vty 0 15
Switch(config-line)#?
Switch(config-line)#login local
Switch(config-line)#exit
Switch(config)#username in60days password cisco
Switch(config)#
```

3. Add an IP address to VLAN 1 on the switch (all ports are in VLAN 1 automatically). Additionally, add the IP address 192.168.1.1 to your PC's FastEthernet interface.

```
Switch(config)#interface vlan1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#no shut
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
Switch(config-if)#^Z ← press Ctrl+Z keys
Switch#
Switch#ping 192.168.1.1 ← test connection from switch to PC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 31/31/32 ms
Switch#
```

4. Test Telnet by Telnetting from your PC to your switch.

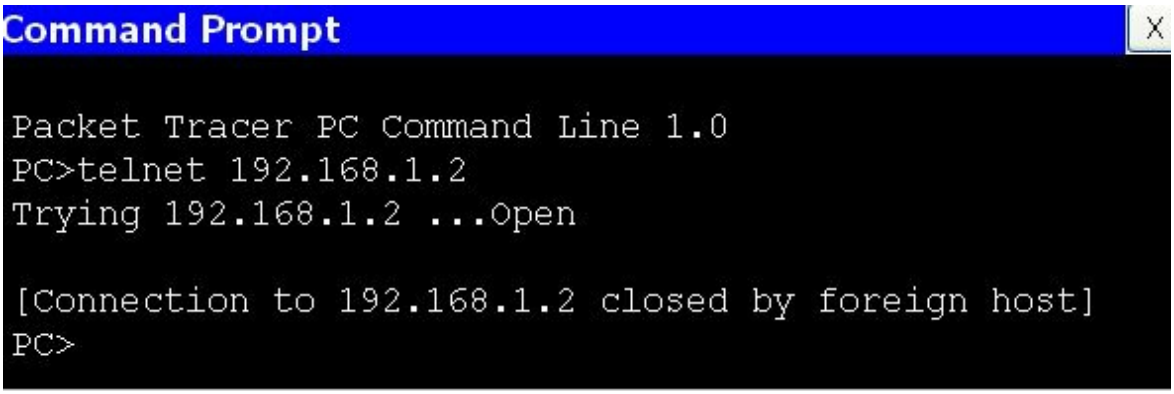


https://t.me

5. Your IT manager changes his mind and wants only SSH access, so change this on your VTY lines. Only certain models and IOS versions will support the `SSH` command.

```
Switch(config)#line vty 0 15
Switch(config-line)#transport input ssh
```

6. Now Telnet from your PC to the switch. Because only SSH is permitted, the connection should fail.



7. Set port security on your switch for the FastEthernet port. It will fail if you have not hard set the port to access (as opposed to dynamic or trunk).

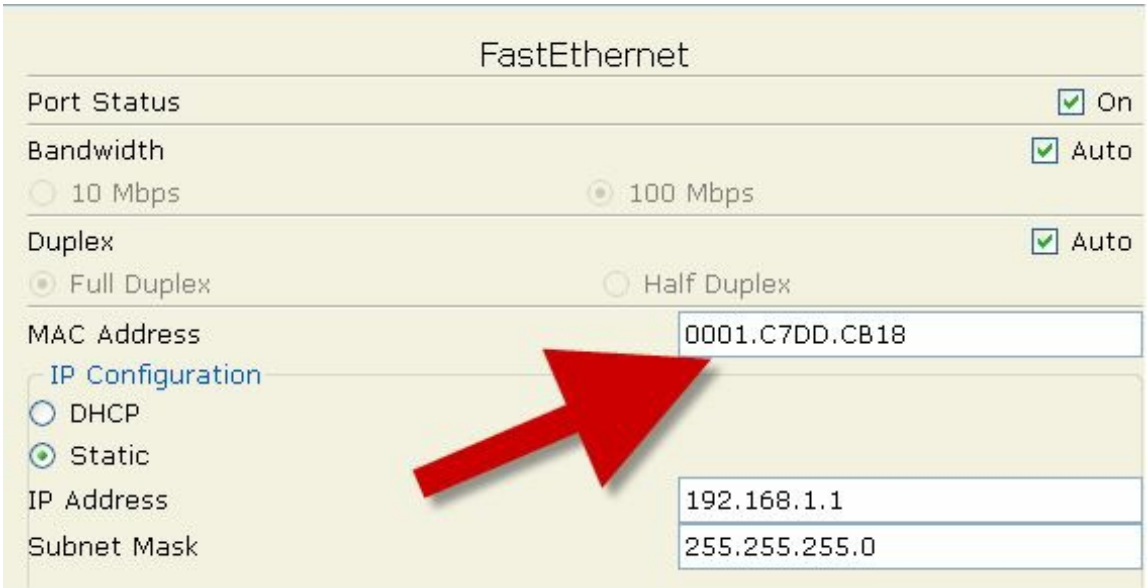
```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#
```

8. Hard set the MAC address from your PC to be permitted on this port. You can check this with the `ipconfig/all` command on your PC command line. Then check the port security status and settings.

```
Switch(config-if)#switchport port-security mac-address 0001.C7DD.CB18
Switch(config-if)#^Z
Switch#show port-security int FastEthernet0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses    : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0001.C7DD.CB18:1
Security Violation Count   : 0
```

https://t.me/learningnets

9. Change the MAC address on your PC, or if you can't do this, plug another device into the switch port. This should make the port shut down due to a breach in the security settings. The screenshot below shows where you would change the MAC address in Packet Tracer.



10. You should see your FastEthernet port go down immediately.

```
Switch#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#show port-security interface FastEthernet0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses    : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0001.C7DD.CB19:1
Security Violation Count   : 1
```

NOTE: Please repeat this lab until you understand the commands and can type them without looking at the Walkthrough section (and do the same for all the other labs in this book).

https://t.me/learningnets

Day 5 – IP Addressing

Day 5 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's lab
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website

Welcome to what many people find to be one of the hardest areas of the CCNA syllabus to understand. In order to understand IP addressing for the CCNA exam, we must cover binary mathematics and the hexadecimal numbering system, classes of addresses, powers of two and rules such as subnet zero, and Broadcast and network addresses, as well as formulas to work out subnets and host addresses.

Don't worry, though; this is a process, not a one-off event, so follow my notes and then feel assured that we will be coming back to review these concepts many times.

Today you will learn about the following:

- IP addressing (using binary and hexadecimal)
- Using IP addresses
- Subnetting
- Easy subnetting
- Network design
- Using VLSM
- Slicing down networks

This module maps to the following CCNA syllabus requirements:

- Describe the operation and necessity of using private and public IP addresses for IPv4 addressing
- Identify the appropriate IPv4 addressing scheme using VLSM and summarisation to satisfy addressing requirements in a LAN/WAN environment
- Troubleshoot and correct common problems associated with IP addressing and host configurations

Cisco have put some VLSM requirements into the ICND1 and the ICND2 exams. More emphasis on this seems to be in the ICND2 exam, but you need to prepare yourself for questions in both exams equally. VLSM will be covered, but you need to understand IP addressing and subnetting first.

https://t.me/learningnets

IP Addressing

All devices on a network need some way to identify themselves as a specific host. Early networks simply used a naming format, and a server on the network kept a map of MAC addresses to host names. Tables quickly grew very large and with this grew issues such as consistency and accuracy (see Figure 5.1 below). IP addressing effectively resolved this issue.

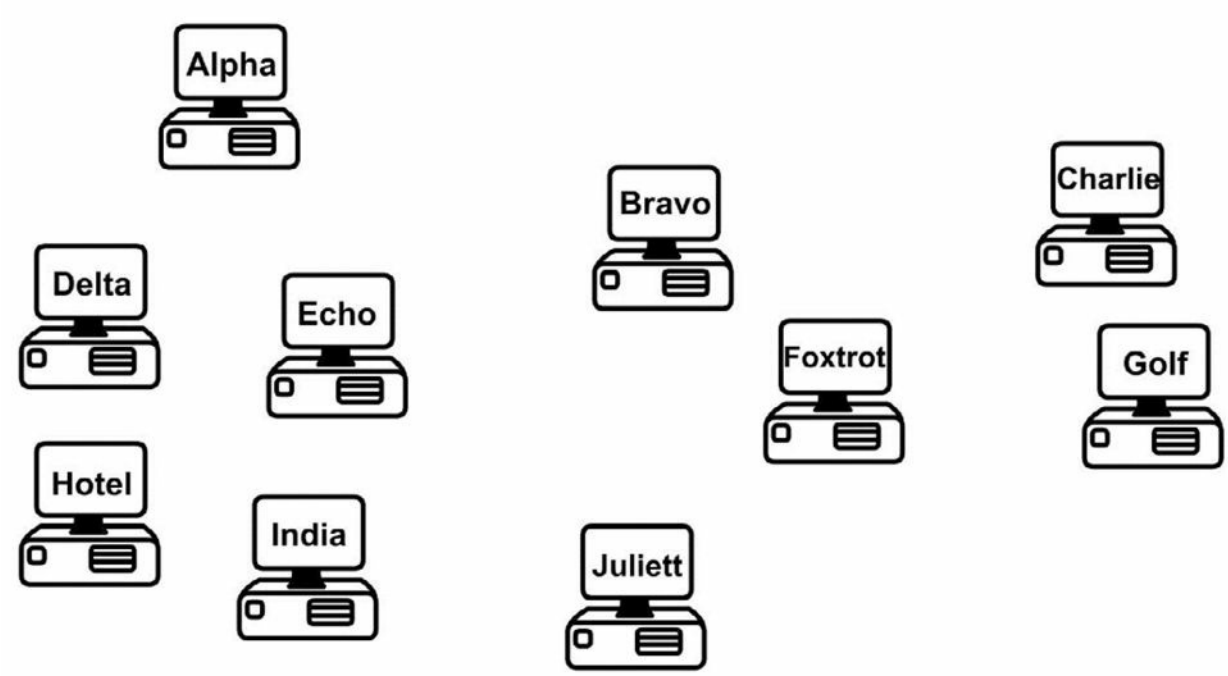


Figure 5.1 – Device Naming Tables Became Too Cumbersome

IP Version 4

IP version 4 (IPv4) was devised to resolve the device naming issue. IPv4 uses binary to apply an address to network devices. IPv4 addresses use 32 binary bits divided into four groups of eight (octets). The following is an example of an IPv4 address in binary:

11000000.10100011.11110000.10101011

which you would see in decimal as:

192.163.240.171

Each binary bit represents a decimal number, and you can use or not use the number by placing a 1 or a 0, respectively, in the relevant column. The eight columns are as follows:

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

In the chart above, you can see that only the first two decimal numbers are used (those with 1s beneath them), which produces the value 128 + 64 = 192.

Binary

In order to understand how IP addressing works, you need to understand binary mathematics (sorry). Computers and networking equipment do not understand decimal. We use decimal

https://t.me/learningnets

because it is a numbering system using 10 digits, invented by a caveman millenia ago when he realised he had 10 digits on his hands that could be used for counting dinosaurs as they walked past his cave.

Computers and networking equipment can only understand electrical signals. Since an electrical signal is either on or off, the only numbering system that will work is binary. Binary uses only two numbers, a 0 or a 1. A 0 means there is no electrical pulse on the wire and a 1 means that there is a pulse on the wire.

Any number can be made up using binary values. The more binary values you add, the larger the number becomes. For every binary value you add, you double the next number (e.g., 1 to 2 to 4 to 8 to 16, and so on into infinity), starting at the right and moving left. With two binary digits, you can count up to 3. Just place a 0 or a 1 in the column to decide whether you want to use that value.

Let's start with only two binary values in columns 1 and 2:

2	1
0	0

0 + 0 = 0

2	1
0	1

0 + 1 = 1

2	1
1	0

2 + 0 = 2

2	1
1	1

2 + 1 = 3

If you use eight binary bit places (an octet), you can get any number from 0 up to 255. You can see that the numbers start from the right and move across to the left:

128	64	32	16	8	4	2	1

If you add a 0 to each of these columns, you have a value of 0 in decimal:

128	64	32	16	8	4	2	1

https://t.me/learningnets

0	0	0	0	0	0	0	0

If you add a 1 to each of these columns, you have a value of 255 in decimal:

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

Don't believe me?

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

So logic dictates that you can actually make any number from 0 to 255 by placing a 0 or a 1 in various columns, for example:

128	64	32	16	8	4	2	1
0	0	1	0	1	1	0	0

32 + 8 + 4 = 44

IP addressing and subnetting are based on the fundamentals above. Table 5.1 below summarises what you know so far. Pay special attention to this table because the values can be used for any subnet mask (more on that later).

Table 5.1 – Binary Values

Binary	Decimal
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

Make up some of your own binary numbers to ensure that you understand this concept fully.

Hexadecimal

Hexadecimal (or hex) is an alternative numbering system. Rather than counting in 2s or by 10, 16 numbers or characters are used. Hex starts at 0 and goes all the way up to F, as illustrated below:

0 1 2 3 4 5 6 7 8 9 A B C D E F

Each hexadecimal digit actually represents four binary digits, as shown below in Table 5.2:

https://t.me/learningnets

Table 5.2 – Decimal, Hex, and Binary Digits

Decimal	0	1	2	3	4	5	6	7
Hex	0	1	2	3	4	5	6	7
Binary	0000	0001	0010	0011	0100	0101	0110	0111

Decimal	8	9	10	11	12	13	14	15
Hex	8	9	A	B	C	D	E	F
Binary	1000	1001	1010	1011	1100	1101	1110	1111

Converting from binary to hex to decimal is fairly simple, as shown in Table 5.3 below:

Table 5.3 – Conversion of Binary to Hex to Decimal

Decimal	13	6	2	12
Hex	D	6	2	C
Binary	1101	0110	0010	1100

Hex is a more manageable counting system for humans than binary, but it's close enough to binary to be used by computers and networking equipment. Any number can be made using hex, as it can use binary or decimal; just count in multiples of 16 instead, for example:

1 x 16 = 16

16 x 16 = 256

256 x 16 = 4096

…and so on.

Hex	4096	256	16	1
			1	A

Counting in hex, therefore, goes 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22, etc., to infinity. 1A (above), for example, is an A in the 1 column and a 1 in the 16 column: A = 10 + 16 = 26.

When converting binary to hex, it makes the task easier if you break the octet into two groups of four bits. So 11110011 becomes 1111 0011. 1111 is 8 + 4 + 2 + 1 = 15, and 0011 is 2 + 1 = 3. 15 is F in hex and 3 is 3 in hex, giving us the answer F3. You can check Table 5.2 to confirm this.

Hex to binary is carried out using the same process. For example, 7C can be split into 7, which is 0111 in binary, and C (12 in decimal), which is 1100 in binary. The answer, then, is 01111100.

Converting Exercise

Here are some examples for you to try. Write out the charts above for working out hex and

https://t.me/learningnets

binary (i.e., for hex, a 1 column, then a 16 column, then a 256 column, and so on):

1. Convert 1111 to hex and decimal.
2. Convert 11010 to hex and decimal.
3. Convert 10000 to hex and decimal.
4. Convert 20 to binary and hex.
5. Convert 32 to binary and hex.
6. Convert 101 to binary and hex.
7. Convert A6 from hex to binary and decimal.
8. Convert 15 from hex to binary and decimal
9. Convert B5 from hex to binary and decimal.

It would be useful in the exam to write out Table 5.2 to help you work out any binary to hex to decimal conversions.

The rule for using IP addressing is that each address on the network must be unique to that host (i.e., it can't be shared). Some addresses can't be used for hosts. This will be covered in more detail later, but for now, know that you can't use an address which is reserved for the entire network, a Broadcast address, or addresses reserved for testing. In addition, three groups are reserved for use on internal networks to save addresses.

Because of the rapid growth of network sizes, each IP address must be used in conjunction with a subnet mask. The subnet mask is there to tell the network devices how to use the numbers in the IP address. The reason for this is that some of the addresses available for hosts on your network can actually be used to chop down the network into smaller chunks or subnets.

An example of an IP address with a subnet mask is 192.168.1.1 255.255.255.240.

Address Classes

You need to know this and you don't! I know, I'm not helping much, but address classes are actually only significant historically, so as a new Cisco engineer, you might become confused when you look at the old rules and try to apply them to new methods of network design.

We still refer to groups of IP addresses as classes, but with the introduction of subnet masking and VLSM, they are actually no longer applicable to network design. Address classes are useful to know, though, because they show us which parts of the IP address we can and can't use for our mini-networks (subnets).

When IPv4 was first invented, addresses were divided into classes. The classes of addresses were then allocated to companies on an as-needed basis. The bigger the company, the bigger the address class. The address classes were assigned letters, A through E. A Class A address was reserved for the biggest networks. A Class A address can be numbered from 1 to 126 in the first octet. The reason for this is that the first bit on the first octet must be 0. If you have 0 in the first octet, then the remaining values can only go from 1 to 126, for example:

https://t.me/learningnets
00000001 = 1

01111111= 126

You can't have an address of all 0s on a network. If you actually add the other three octets, then you can see Class A addresses in full, for example:

10.1.1.1

120.2.3.4

126.200.133.1

These are all Class A addresses because they are within the range of 1 to 126. 127 is not a permitted number for IP addresses; 127.0.0.1 is actually an address used to test whether TCP/IP is working on your device.

A Class B address must have the first two bits of the first octet set to 10. This means that the first octet can only use the numbers 128 to 191, for example:

10000000 = 128

10111111 = 191

For Class C addresses, the first three bits on the first octet must be set to 110, giving us addresses 192 to 223, for example:

11000000 = 192

11011111 = 223

Class D addresses are used for multicasting (directed broadcasts), and Class E addresses are for experimental use only.

Subnet Mask Primer

I mentioned earlier that part of the address identifies the network and part of it identifies the host on the network. Subnet masks establish which parts are which. The difficulty is that it isn't always easy to establish which is which by just looking at the subnet mask. This requires practise, and for the more difficult addresses, you must work them out by hand (or cheat by using a subnet calculator).

Even if you are not chopping your network into smaller parts, you must still apply a subnet mask to every address used. Each network class comes with a default subnet mask, for example:

Class A = 255.0.0.0

Class B = 255.255.0.0

Class C = 255.255.255.0

When the binary bits are turned on, the network knows that this number is to be used for the network, not for a host on the network, as illustrated below:

192	168	12	2
255	255	255	0
Network	Network	Network	Host

https://t.me/learningnets

The address above means that 192.168.12 is the network and 2 is a host on that network. Furthermore, any address starting with 192.168.12 is on the same network. You can see from the number in the first octet and the default subnet mask that this is a Class C network.

Remember the rule I mentioned earlier: You can't use the network numbers for hosts, so the numbers below cannot be used on devices:

10.0.0.0

192.168.2.0

174.12.0.0

The other rule is that you can't use the Broadcast address on each network or subnet. A Broadcast address goes to all devices on the network, so, logically, it can't be used for devices. A Broadcast address is one in which all the host bits are active, or turned on:

10.255.255.255

192.168.1.255

In the examples above, each binary bit is turned on for the host portion.

Using IP Addresses

Next up, the practicalities of using IP addresses – which ones can be used and which ones can't be used?

You know that there has been a huge explosion in the use of computers over the past two decades. A PC used to be a very expensive item which few people could afford; therefore, they were reserved for use by well-funded companies only. Today, nearly every house contains one or more computers.

The problem, of course, is that IPv4 was devised when only a limited number of devices were being used and there was no anticipation of this situation changing. As addresses were being allocated, it was realised that at the current rate of growth, we would quickly run out of available addresses.

Private IP Addresses

One of several solutions was to reserve some classes of addresses for anybody to use, as long as that address wasn't used over the Internet. This range of addresses is known as private IP addresses, and this solution was created by two RFCs, 1918 and 4193. As a refresher, RFC stands for Request for Comments and is a means for engineers to submit ideas for networking methods, protocols, and technology advancements.

The ranges of private addresses are as follows:

10.x.x.x – any address starting with a 10

172.16.x.x to 172.31.x.x – any address starting with 172.16 to 172.31, inclusive

192.168.x.x – any address starting with 192.168

https://t.me/learningnets

Subnetting

Subnetting allows you to steal bits of an IP address which were traditionally used for hosts on the network. You can now carve smaller networks from your larger network space, and these smaller networks are referred to as subnetworks, or subnets for short.

If you apply the default subnet masks to the three usable address classes, you will see the portions of the address you can't use for carving out subnets, as illustrated in the chart below:

A – 255	0	0	0
Can't Use	Can Use	Can Use	Can Use
B – 255	255	0	0
Can't Use	Can't Use	Can Use	Can Use
C – 255	255	255	0
Can't Use	Can't Use	Can't Use	Can Use

For example, if you take a Class C network with the default subnet mask

IP Address	192	168	1	0
Subnet Mask	255	255	255	0
In Binary	11111111	11111111	11111111	00000000

and steal some of the available host bits on the last octet

IP Address	192	168	1	0
Subnet Mask	255	255	255	192
In Binary	11111111	11111111	11111111	**11**000000

you get two stolen bits on the last octet. This gives you the following subnets, each with 62 hosts:

Network	Network	Network	Subnet	Hosts	Broadcast Address
192	168	1	0	1–62	63
192	168	1	64	65–126	127
192	168	1	128	129–190	191
192	168	1	192	193–254	255

With a bigger network, you could have used host numbers 1 to 254, so you have less available host numbers to use here but the trade-off is more networks. The chart below shows how the four subnets were determined:

128	64	32	16	8	4	2	1	**Subnet**

https://t.me/learningnets

0	0	0	0	0	0	0	0	**0**
0	1	0	0	0	0	0	0	**64**
1	0	0	0	0	0	0	0	**128**
1	1	0	0	0	0	0	0	**192**

Delving into binary math, you can see that using the first two bits of the host address lets you use the binary combinations 00, 01, 10, and 11, and writing these out in full, as you see in the subnets column, gives you the subnets 0, 64, 128, and 192. To clarify this further, the first two rows in grey are subnet numbers and the remaining six rows are for use by host numbers on each subnet.

If you feel your head spinning right about now, this is normal. It takes a while for all of this to finally click, I'm afraid.

Easy Subnetting

Come exam day, or when troubleshooting a subnetting issue on a live network, you will want to get to your answer quickly and accurately. For these reasons, I devised an easy way to subnet, which is the subject of my *Subnetting Secrets* Amazon Kindle book. You won't need to read it though to be honest, as I cover what you need to know in this book.

A very useful resource I've created is www.subnetting.org, which gives you free challenge questions to solve around subnetting and network design.

Classless Inter-Domain Routing

Classless Inter-Domain Routing (CIDR) was created by the Internet Engineering Task Force as a method to allocate blocks of IP addresses and to route IP packets. The main feature of CIDR we will examine here is using slash address notation to represent subnet masks. This is important because it saves time, it is used in the real world, and, if that isn't enough, you will be given exam questions involving CIDR addresses.

With CIDR, instead of using the full subnet mask, you write down the number of binary bits used. For 255.255.0.0, for example, there are two lots of eight binary bits used, so this would be represented with a /16. For 255.255.240.0, there are 8 + 8 + 4 bits used, giving you /20.

When you refer to subnet masks or network masks in the context of internetworking, you would say "slash sixteen" or "slash twenty" to work colleagues and they would know that you are referring to a CIDR mask.

The Subnetting Secrets Chart

I'm about to save you many weeks of subnetting frustration. My Subnetting Secrets cheat chart has been used by thousands of CCNA and CCNP students all over the world to pass exams and ace technical interviews for networking roles.

Seriously. Until I stumbled across the easy way while studying for my CCNA several years ago, students were forced to write out network addresses in binary or go through painful calculations in order to get to the correct answer.

https://t.me/learningnets

In order to write out the Subnetting Secrets chart, you will need a pencil and paper. You need to be able to write it out from memory because in your exam you will be given a whiteboard to use for any working out. You can also use pen and paper in any technical interviews.

On the top right side of your paper, write the number 1, and then to the left of that double it to 2, then 4, then 8, and keep doubling up to number 128. This is one binary octet:

128	64	32	16	8	4	2	1

Under the 128 and going down, write out the number you would get if you put a tick in the first box (the 128 box). Then the next number below that will be what you would get if you ticked the next box (64), and the next (32), and the next (16), and so on until you had ticked all eight boxes:

128
192
224
240
248
252
254
255

If you put together both parts, you will have the upper portion of the Subnetting Secrets cheat sheet:

Bits	128	64	32	16	8	4	2	1
Subnets								
128								
192								
224								
240								
248								
252								
254								
255								

The top row represents your subnet increment and the left column your subnet mask. Using this part of the chart, you could answer any subnetting question in a few seconds. If you want to add the part of the chart which tells you how to answer any design question, such as “How many subnets and hosts will subnet mask ‘X’ give you,” just add a “powers of two” section.

https://t.me/learningnets

One column will be “powers of two” and another will be “powers of two minus two.” The minus two is meant to cover the two addresses you can’t use, which are the subnet and the Broadcast addresses on the subnet. You start with the number 2 and double it as many times as you need to in order to answer the question.

Bits	128	64	32	16	8	4	2	1
Subnets								
128								
192								
224								
240			**For working out which subnet a host is in**					
248								
252								
254								
255								
	Subnets	Hosts -2						
2			**For working out how many subnets and how many hosts per subnet**					
4								
8								
16								
32								
64								

You will probably learn best by jumping straight into an exam-style question:

Which subnet is host 192.168.1.100/26 in?

Well, you know that this is a Class C address and the default mask is 24 binary bits, or 255.255.255.0. You can see that instead of 24 there are 26 bits, so 2 bits have been stolen to make the subnet. Simply write down your Subnetting Secrets cheat sheet and tick two places (from the left) along the top row. This will reveal in what amount your subnets go up. You can then tick down two places in the subnets column to reveal the actual subnet mask.

Bits	128	64	32	16	8	4	2	1
Subnets	✔	✔						

https://t.me/learningnets

128	✔							
192	✔							
224								
240								
248								
252								
254								
255								
	Subnets	Hosts -2						
2								
4								
8								
16								
32								
64								

Now you know two things: subnets will go up in increments of 64 (you can use 0 as the first subnet value) and your subnet mask for /26 ends in 192, so, in full, it is 255.255.255.192:

192.168.100.0 is your first subnet
192.168.100.64 is your second subnet
192.168.100.128 is your third subnet
192.168.100.192 is your last subnet

You can't go any further than your actual subnet value, which is 192 in this example. But remember that the question is asking you to find host 100. You can easily see that the subnet ending in 64 is where host 100 would lie because the next subnet is 128, which is too high.

Just for completeness, I will add the host addresses and the Broadcast addresses. You can quickly work out the Broadcast address by taking the next subnet value and subtracting 1:

Subnet	First Host	Last Host	Broadcast
192.168.100.0	192.168.100.1	192.168.100.62	192.168.100.63
192.168.100.64	192.168.100.65	192.168.100.126	192.168.100.127
192.168.100.128	192.168.100.129	192.168.100.190	192.168.100.191
192.168.100.192	192.168.100.193	192.168.100.254	192.168.100.255

Consider the IP addresses to be values of anything from 0 to 255. Much like an odometer in a car, each number rolls up until it rolls back to 0 again, but the next box rolls over 1. Below are two sample octets. I jump up when we get to 0 2 to save space:

Octet 1	Octet 2

https://t.me/learningnets

0	0
0	1
0	2 (jump up)
0	255
1	0
1	1
1	2

If you wanted to use the design part of the chart, you could. There is no need to for this question, but to see how it works, you just tick down two places in the subnets column because you stole 2 bits. From 8 bits in the last octet, that leaves you 6 bits for hosts, so tick down six places in the Hosts -2 column to reveal that you get 64 minus 2 bits per subnet, or 4 subnets, and 62 hosts per subnet:

Bits	128	64	32	16	8	4	2	1
Subnets	✔	✔						
128	✔							
192	✔							
224								
240								
248								
252								
254								
255								
	Subnets	Hosts -2						
2	✔	✔						
4	✔	✔						
8		✔						
16		✔						
32		✔						
64		✔						

Ready for another question? Of course you are.

Which subnet is host 200.100.2.210/25 in?

Same drill as before. You know this is a Class C address, and that to get from 24 to 25 bits, you need to steal 1 bit. Tick one across in the top row and then one down in the left column:

Bits	128	64	32	16	8	4	2	1
Subnets	✔							

https://t.me/learningnets

128	✔							
192								
224								
240								
248								
252								
254								
255								

Therefore, your mask will be 255.255.255.128, and your subnets will go up in increments of 128. You can't actually steal less than 1 bit for a Class C address; this will give you only two subnets:

200.100.2.0

and

200.100.2.128

You can already answer the question because you can see that host 210 will be in the second subnet. Just to demonstrate, I will write out the host and Broadcast addresses again:

Subnet	First Host	Last Host	Broadcast
200.100.2.0	200.100.2.1	200.100.2.126	200.100.2.127
200.100.2.128	200.100.2.129	200.100.2.254	200.100.2.255

Next question: Which subnet is 172.16.100.11/19 in?

You need to add 3 to 16 (the default Class B mask) to get to 19. Tick across three places in the top row of the chart to get the subnet increment, and then down three in the left column to get the subnet mask. You don't need the lower portion of the chart for these types of questions.

Bits	128	64	32	16	8	4	2	1
Subnets	✔	✔	✔					
128	✔							
192	✔							
224	✔							
240								
248								
252								
254								
255								

https://t.me/learningnets

Your subnet mask is 255.255.224.0, and you are subnetting on the third octet because the first two are reserved for the network address/default subnet mask.

Your subnets will be as follows:

172.16.0.0
172.16.32.0
172.16.64.0
172.16.96.0*
172.16.128.0
172.16.160.0
172.16.192.0
172.16.224.0

In the exam, please stop once you get to one subnet past the one your host is in, because going one past will make sure you have the right subnet. You are looking for host 100.11 on the 172.16 network; the asterisk in the list of subnets above denotes the subnet that the host number resides in.

If, for some reason, in the exam they asked you to identify the host addresses and Broadcast address (for extra points), you can easily add these. I will put them in for the first few subnets:

Subnet	First Host	Last Host	Broadcast
172.16.0.0	172.16.0.1	172.16.31.254	172.16.31.255
172.16.32.0	172.16.32.1	172.16.63.254	172.16.63.255
172.16.64.0	172.16.64.1	172.16.95.254	172.16.95.255
172.16.96.0	172.16.96.1	172.16.127.254	172.16.127.255

In the exam, they may well try to trick you by adding Broadcast addresses as options for host addresses, or even subnet addresses for host addresses. This is why you need to be able to identify which is which. You will also come across the same issue on live networks, where other engineers have tried to add the wrong address to an interface.

Next question: Which subnet is host 172.16.100.11/29 in?

As you can see by now, you can use any mask you wish with most any subnet. I could have asked you about the address 10.100.100.1/29, so don't let the fact that you have a Class A address with subnet bits going into the second, third, or fourth octet put you off.

You need to steal 13 bits for the subnet mask but the subnetting chart has only eight places. Since you are looking at the easy way to subnet, just focus on the part of the chart which the remaining numbers spill over into. If you drew another chart next to the one you had just filled up, you would have five places filled up (8 + 5 = 13 bits):

Bits	128	64	32	16	8	4	2	1
Subnets	✔	✔	✔	✔	✔			
128	✔							

https://t.me/learningnets

192	✔							
224	✔							
240	✔							
248	✔							
252								
254								
255								

From the chart above, you can see that the subnet mask is 255.255.255.248. The 255 in the third octet is there because you filled it up whilst moving over into the fourth octet. The subnets are also going up in increments of 8.

You could start off with 172.16.0.0, but the problem with that is it would take quite some time to count up in multiples of 8 before you got to 172.16.100.11 this way, and the exam is a timed one. Therefore, you need to fast track the counting process.

If you start counting up in increments of 8, you would get the following:

172.16.0.0
172.16.0.8
172.16.0.16, and you could keep counting up to
172.16.1.0
172.16.1.8, and keep counting up to
172.16.20.0
172.16.20.8

This would take a very long time because there are over 8000 subnets (2 to the power of 13 gives you 8192, and you can check this using the design section of the Subnetting Secrets cheat sheet).

Let's presume that each third octet is going up one digit at a time (which it is). Why not jump up to 172.16.100.x to start with?

172.16.100.0
172.16.100.8*
172.16.100.16

From the above, you can see which subnet host 11 is in, and if you were asked to work out the Broadcast address, it would look like the chart below:

Subnet	First Host	Last Host	Broadcast
172.16.100.0	172.16.100.1	172.16.100.6	172.16.100.7
172.16.100.8	172.16.100.9	172.16.100.14	172.16.100.15
172.16.100.16	172.16.100.17	172.16.100.22	172.16.100.23

https://howtonetwork.com

That's it for now. We will revisit this subject many times over. For some

network design examples using the lower part of the chart, please check out www.in60days.com.

Remember also that there are a few subnetting resources available for you to use:

www.subnetting.org – subnetting question generator
www.youtube.com/user/paulwbrowning – my YouTube channel with free videos

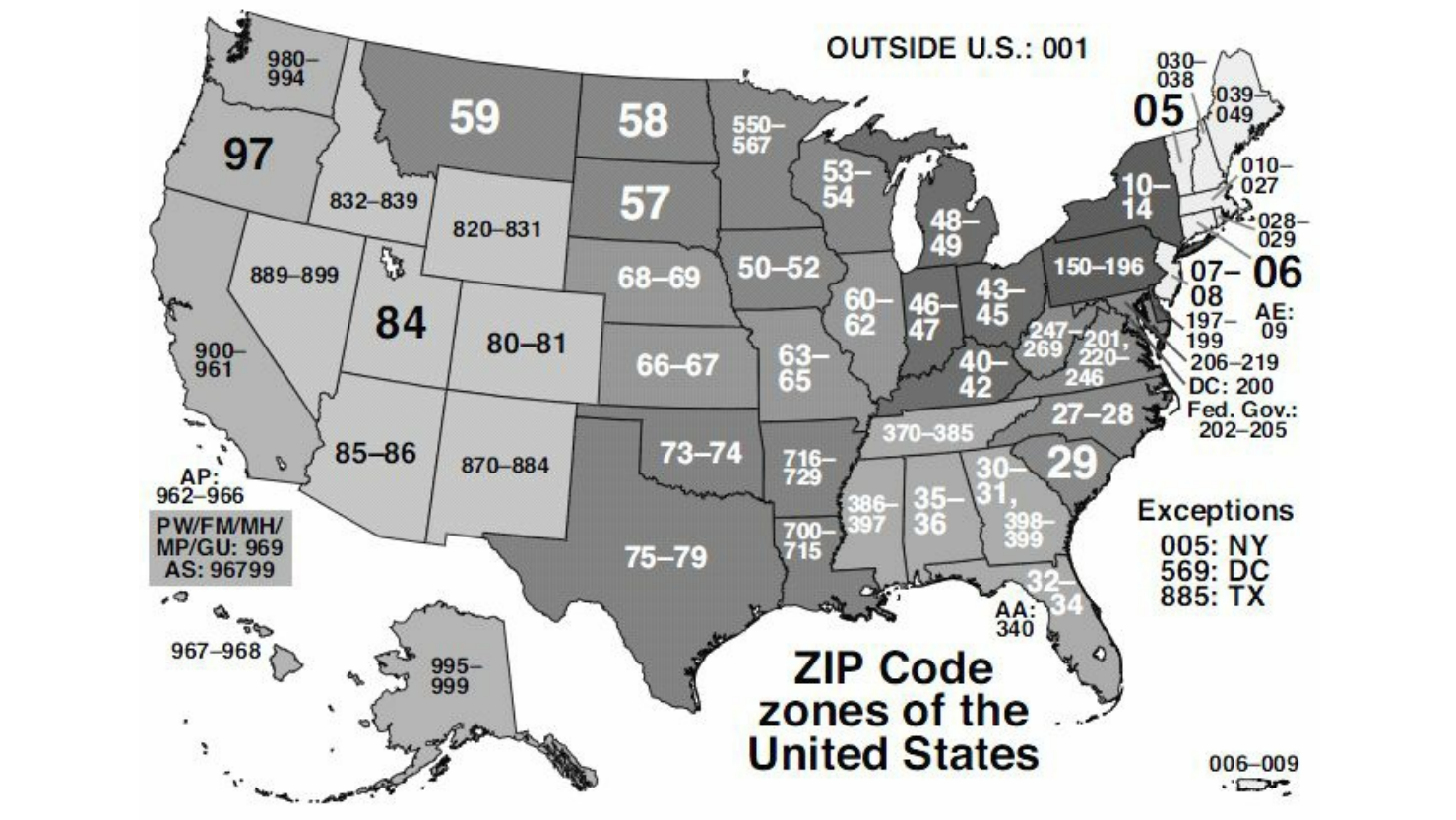
Route Summarisation

There are many millions of routes on the Internet. If these routes all had to be stored individually, the Internet would have come to a stop many years ago. Route summarisation, also known as supernetting, was proposed in RFC 1338, which you can read online by clicking on the RFC - www.faqs.org/rfcs/rfc1338.html.

If you want to read a very comprehensive guide to route summarisation, then please grab a hold of Jeff Doyle's excelling Cisco book *Routing TCP/IP Volume 1*, which is now in its second edition.

ZIP Codes

ZIP codes are used by the United States Postal Service to improve routing of letters to addresses within the USA (see Figure 5.2). The first digit represents a group of US states, and the second and third digits represent a region inside that group. The idea is that letters and parcels can be quickly routed by machine or by hand into the correct state and then forwarded to that state. When it reaches the state, it can be routed to the correct region. From there, it can be routed to the correct city and so on, until it is sorted into the correct mailbag for the local postal delivery person.



https://t.me/learningnets

Figure 5.2 – US ZIP Codes

The ZIP code system was devised to make the routing of mail more accurate and efficient. For example, the sorting office in Atlanta doesn't need to know which street in San Francisco the packet is destined for. Having to store that information would make the sorting process unworkable.

Route Summarisation Prerequisites

In order to use route summarisation on your network, you need to use a classless protocol (covered later), such as RIPv2, EIGRP, or OSPF. You also need to design your network in a hierarchical order, which will require careful planning and design. This means that you can't randomly assign networks to various routers or LANs within your network.

Applying Route Summarisation

Let's move on to an example of a network and what the problem will look like on your network if you don't use route summarisation. In this example, this is how summarisation would work with a range of IP addresses on a network. The router in Figure 5.3 below has several networks attached. The first choice is to advertise all of these networks to the next-hop router. The alternative is to summarise these eight networks down to one route and send that summary to the next-hop router, which will cut down on bandwidth, CPU, and memory requirements.

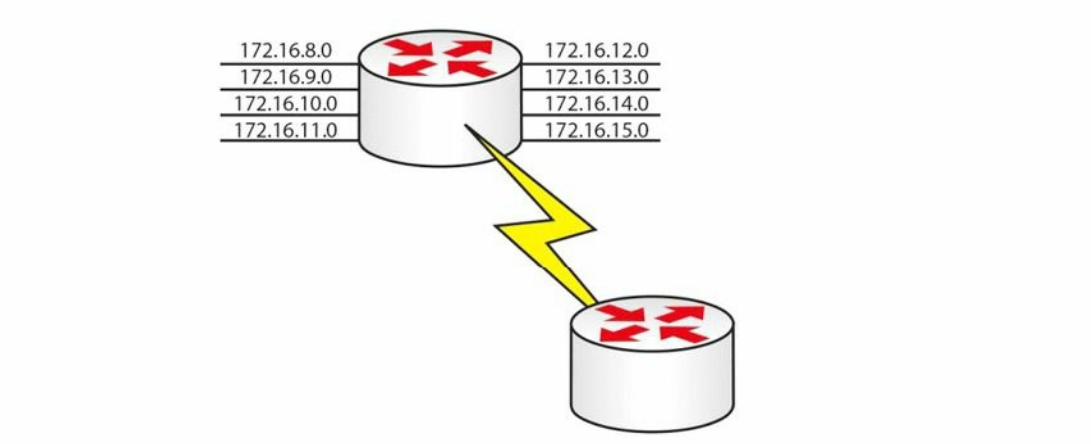


Figure 5.3 – An Example of Route Summarisation

The only way to work out a summary route is by converting the IP address into binary (sorry). If you don't do this, then you will have no way of knowing whether you are advertising the correct summary route, which will lead to problems on your network.

Firstly, write out all of the network addresses in full and then the binary versions to the right of that, as illustrated below:

172.16.8.0	*10101100.00010000.00001*000.00000000
172.16.9.0	*10101100.00010000.00001*001.00000000
172.16.10.0	*10101100.00010000.00001*010.00000000
172.16.11.0	*10101100.00010000.00001*011.00000000
172.16.12.0	*10101100.00010000.00001*100.00000000

https://t.me/learningnets

172.16.13.0	*10101100.00010000.00001*101.00000000
172.16.14.0	*10101100.00010000.00001*110.00000000
172.16.15.0	*10101100.00010000.00001*111.00000000
Matching Bits	*10101100.00010000.00001* = 21 bits

I have italicised and underlined the bits in each address that match. You can see that the first 21 bits match in every address, so your summarised route can reflect the following 21 bits:

172.16.8.0 255.255.248.0

One other significant advantage of using route summarisation is that if a local network on your router goes down, the summary network will still be advertised out. This means that the rest of the network will not need to update its routing tables or, worse still, have to deal with a flapping route (rapidly going up and down). I have chosen two exercises dealing with route summarisation for you to work out.

Exercise 1: Write out the binary equivalents for the addresses below, and then determine which bits match. I have written the first two octets for you to save time.

172.16.50.0	*10101100.00010000.*
172.16.60.0	*10101100.00010000.*
172.16.70.0	*10101100.00010000.*
172.16.80.0	*10101100.00010000.*
172.16.90.0	*10101100.00010000.*
172.16.100.0	*10101100.00010000.*
172.16.110.0	*10101100.00010000.*
172.16.120.0	*10101100.00010000.*

What summarised address would you advertise?

I would make it 172.16.50.0 255.255.128.0, or /17.

Exercise 2: The company below has three routers connected to their HQ router. They need to summarise the routes advertised from London 1, 2, and 3:

https://t.me/learningnets

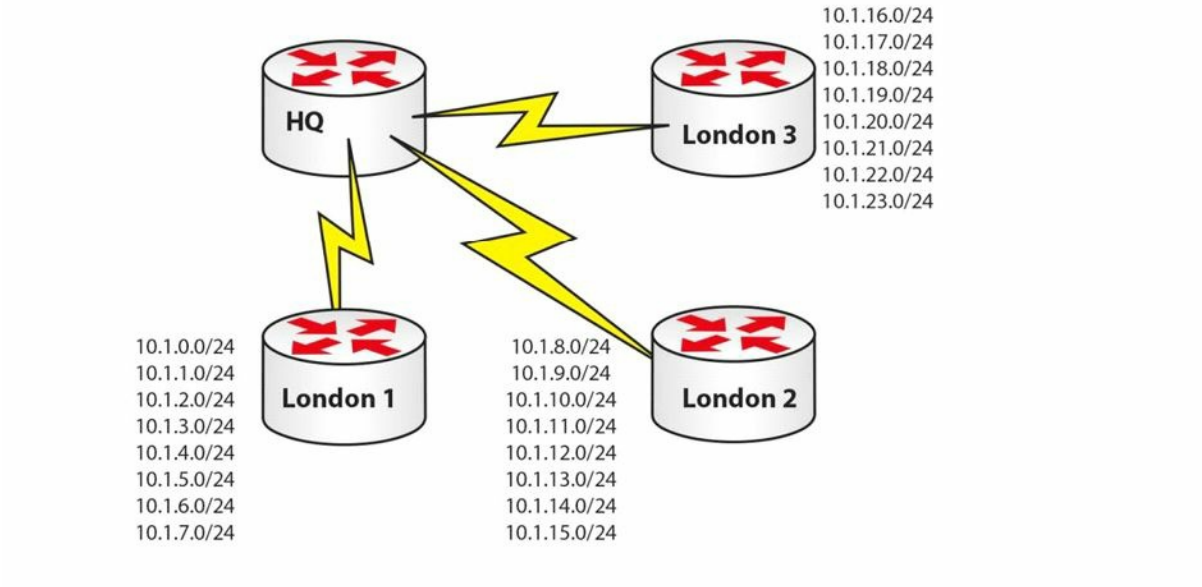


Figure 5.4 – Summarised Routes Advertised from London 1, 2, and 3

Let's start with London 1:

10.1.0.0	*00001010.00000001.00000*000.00000000
10.1.1.0	*00001010.00000001.00000*001.00000000
10.1.2.0	*00001010.00000001.00000*010.00000000
10.1.3.0	*00001010.00000001.00000*011.00000000
10.1.4.0	*00001010.00000001.00000*100.00000000
10.1.5.0	*00001010.00000001.00000*101.00000000
10.1.6.0	*00001010.00000001.00000*110.00000000
10.1.7.0	*00001010.00000001.00000*111.00000000

There are 21 common bits, so London 1 can advertise 10.1.0.0/21 to the HQ router.

And for London 2:

10.1.8.0	*00001010.00000001.00001000.*00000000
10.1.9.0	*00001010.00000001.00001*001.00000000
10.1.10.0	*00001010.00000001.00001*010.00000000
10.1.11.0	*00001010.00000001.00001*011.00000000
10.1.12.0	*00001010.00000001.00001*100.00000000
10.1.13.0	*00001010.00000001.00001*101.00000000
10.1.14.0	*00001010.00000001.00001*110.00000000
10.1.15.0	*00001010.00000001.00001*111.00000000

London 2 also has 21 common bits, so it can advertise 10.1.8.0/21 to the HQ router.

https://t.me/learningnets

And on to London 3:

10.1.16.0	*00001010.00000001.0001*0000.00000000
10.1.17.0	*00001010.00000001.0001*0001.00000000
10.1.18.0	*00001010.00000001.0001*0010.00000000
10.1.19.0	*00001010.00000001.0001*0011.00000000
10.1.20.0	0*0001010.00000001.0001*0100.00000000
10.1.21.0	*00001010.00000001.0001*0101.00000000
10.1.22.0	*00001010.00000001.0001*0110.00000000
10.1.23.0	*00001010.00000001.0001*0111.00000000

London 3 has 21 common bits also, so it can advertise 10.1.16.0/21 upstream to the HQ router.

You will be expected to understand route summarisation for the CCNA exam. If you can quickly work out the common bits, then you should be able to answer the questions quickly and accurately.

Here is the answer to Exercise 1:

00110010.00000000
00111100.00000000
01000110.00000000
01010000.00000000
01011010.00000000
01100100.00000000
01101110.00000000
01111000.00000000

Variable Length Subnet Masking

Using VLSM

Look at the following network:

- 192.168.1.0/24 = 1 network with 254 hosts

While this may work fine, what if your network requires more than one subnet? What if your subnets have less than 254 hosts in them? Either situation requires some changes to be made. If you applied a /26 mask to your network instead, you would get this:

- 192.168.1.0/26 = 4 subnets with 62 hosts

If that wasn't suitable, what about a /28 mask?

- 192.168.1.0/28 = 16 subnets with 14 hosts

https://t.me/learningnets

You can refer back to the Subnetting Secrets cheat sheet design section to help you work out

how to apply VLSM to your network or to an exam question. With the /26 mask, you can see how many subnets and hosts you will get:

Bits	128	64	32	16	8	4	2	1
Subnets	✔	✔						
128	✔							
192	✔							
224								
240								
248								
252								
254								
255								
	Subnets	Hosts -2						
2	✔	✔						
4	✔	✔						
8		✔						
16		✔						
32		✔						
64		✔						

You have to take away 2 bits for the hosts, so you get four subnets, each with 62 hosts.

Slicing Down Networks

The point of VLSM is to take your network block and make it work for your particular network needs. Taking the typical network address of 192.168.1.0/24, with VLSM, you can use a /26 mask and now do this:

192.168.1.0/26	Subnet	Hosts
192.168.1.0	1	62
192.168.1.64 – IN USE	2	62
192.168.1.128 – IN USE	3	62
192.168.1.192 – IN USE	4	62

This may work fine until you realise that you have two smaller networks on your infrastructure which require 30 hosts each. What if three of your smaller subnets are taken (marked as IN USE above) and you have only one left (i.e., 192.168.1.0)? VLSM lets you take any of your chopped down subnets and chop them down even further. The only rule is that any IP address can be used only once, no matter which mask it has.

https://t.me/learningnets

If you use the design section of the Subnetting Secrets cheat sheet, you will see which mask gives you 30 hosts:

	Subnets	Hosts -2						
2	✔	✔						
4	✔	✔						
8	✔	✔						
16		✔						
32		✔						
64								

The upper section of the chart (not shown here) tells us that three ticks down in the left column gives you a mask of 224 or /27 (3 stolen bits).

192.168.1.0/27	Subnet	Hosts
192.168.1.0	1	30
192.168.1.32	2	30
192.168.1.64	CAN'T USE	CAN'T USE

You can't use the .64 subnet because this is already in use. You are now free to use either of the other two subnets. If you needed only one, you could chop down the remaining one to give you more subnets, each with fewer hosts.

Please also read bonus stuff on VLSM on the in60days.com website.

Troubleshooting IP Addressing Issues

Troubleshooting Subnet Mask and Gateway Issues

You may see a number of symptoms occurring whenever you have a problem with IP addressing, the subnet mask, or gateway issues. Some of the problems that might occur include the following:

- Network devices can communicate within their local subnet but are unable to communicate with devices outside the local network. This usually indicates that you have some type of issue with the gateway configuration or operation.
- Not having any type of IP communication, either internally or remote. This usually points to a major issue which might involve a lack of functionality on certain devices.
- Situations in which you can communicate with some IP addresses but not all of those that are available. This is usually the most difficult problem to troubleshoot because it has many possible causes.

One of the first things you should always do during the troubleshooting process for such situations is to double-check the IP address, the subnet mask, and the default gateway

configuration on your devices. You should also check the documentation in order to verify this information. A great many issues stem from misconfigurations.

If you are installing network devices for the first time, very often you will manually type in the IP address information, along with the subnet mask and the default gateway. The recommendation is to verify this information before submitting it because human errors are rife in this area. Most enterprise networks have procedures for introducing new devices to the network, including testing the gateway and SNMP server reachablility.

If you need to gather information during the troubleshooting process, you might want to perform some packet capturing to see exactly which packets are sent between devices. If you see packets from hosts that are not on your network, you may have some kind of VLAN misconfiguration issue. If you suspect that your subnet mask is incorrect, you should check the parameters of other devices on your network. If the other machines work properly, you should use the same subnet mask on the device that is not working as expected and start testing again.

When using dynamic IP addressing (DHCP) to allocate IP address information to devices in your network, including the subnet mask and the default gateway, you should investigate the DHCP server configuration because that might be another area where problems may occur. Perhaps the DHCP server is misconfigured or the DHCP service is jammed, so you should include this step in your troubleshooting process. You must also remember to exclude reserved addresses from the DHCP pool because these addresses will usually be allocated to servers and router interfaces.

Other useful troubleshooting tools that will help you identify the point in the network where problems occur are traceroute and ping. We will cover these throughout the book and in labs.

https://t.me/learningnets

Day 5 Questions

1. Convert 192.160.210.177 into binary (without using a calculator).
2. Convert 10010011 into decimal.
3. What is the private range of IP addresses?
4. Write out the subnet mask from CIDR /20.
5. Write out the subnet mask from CIDR /13.
6. 192.168.1.128/26 gives you how many available addresses?
7. What is the last host of the 172.16.96.0/19 network?
8. Starting with 192.168.1.0/24, with VLSM, you can use a /26 mask and generate which subnets?
9. In order to use route summarisation on your network, you need to use what?
10. Write down the subnets 172.16.8.0 to 172.16.15.0, and work out the common bits and what subnet mask you should use as a summary. Don't look in the book before working this out.

https://t.me/learningnets

Day 5 Answers

1. 11000000.10100000.11010010.10110001.
2. 147.
3. 10.x.x.x – any address starting with a 10.
   172.16.x.x to 172.31.x.x – any address starting with 172.16 to 172.31, inclusive.
   192.168.x.x – any address starting with 192.168.
4. 255.255.240.0.
5. 255.248.0.0.
6. 62.
7. 172.16.127.254.
8. 192.168.1.0/26, 192.168.1.0.64/26, 192.168.1.0.128/26, and 192.168.1.0.192/26.
9. A classless protocol.
10. 172.16.8.0/21 (mask: 255.255.248.0).

Answers for the conversion exercises

1. Convert 1111 to hex and decimal

Hex = F

Decimal = 15

2. Convert 11010 to hex and decimal

Hex = 1A

Decimal = 26

3. Convert 10000 to hex and decimal

Hex = 10

Decimal = 16

4. Convert 20 to binary and hex

Binary = 10100

Hex = 14

5. Convert 32 to binary and hex

Binary = 100000

Hex = 20

6. Convert 101 to binary and hex

Binary = 1100101

Hex = 65

https://t.me/learningnets

7. Convert A6 from hex to binary and decimal

Binary = 10100110

Decimal = 166

8. Convert 15 from hex to binary and decimal

Binary = 10101

Decimal = 21

9. Convert B5 from hex to binary and decimal

Binary = 10110101

Decimal = 181

https://t.me/learningnets

Day 5 Lab

IP Addressing on Routers Lab

Topology



Purpose

Learn how to get used to configuring IP addresses on routers and pinging across a Serial interface.

Walkthrough

1. Start off by establishing your Serial interface numbers, as they may differ from mine in the diagram above. Also, please establish which side has the DCE cable attached because this side will require the `clock rate` command.

```
Router>en
Router#sh ip interface brief
Interface        IP-Address  OK? Method Status                Protocol
FastEthernet0/0 unassigned  YES unset  administratively down down
FastEthernet0/1 unassigned  YES unset  administratively down down
Serial0/1/0     unassigned  YES unset  administratively down down
Vlan1           unassigned  YES unset  administratively down down
Router#
Router#show controllers Serial0/1/0
M1T-E3 pa: show controller:
PAS unit 0, subunit 0, f/w version 2-55, rev ID 0x2800001, version 2
idb = 0x6080D54C, ds = 0x6080F304, ssb=0x6080F4F4
Clock mux=0x30, ucmd_ctrl=0x0, port_status=0x1
line state: down
DCE cable, no clock rate
```

2. Add a hostname and IP address to one side. If this side is the DCE, add the clock rate.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterA
RouterA(config)#interface s0/1/0
RouterA(config-if)#ip add 192.168.1.1 255.255.255.0
RouterA(config-if)#clock rate 64000
RouterA(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
```

https://t.me/learningnets

```
RouterA(config-if)#
```

3. Add an IP address and hostname to the other router. Also, bring the interface up with the `no shut` command.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterB
RouterB(config)#int s0/1/0
RouterB(config-if)#ip address 192.168.1.2 255.255.255.0
RouterB(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
RouterB(config-if)#^Z
RouterB#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
```

4. Test the connection with a ping.

```
RouterB#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/31/32 ms
```

NOTE: If the ping doesn't work, then double-check to make sure that you have added the `clock rate` command to the correct router. Ensure that the cable is inserted correctly and use the `show controllers serial x/x/x` command, inputting your own interface number.

Visit www.in60days.com and watch me do this lab for free.

Binary Conversion and Subnetting Practice

Please spend the rest of this day's lesson practising these critical topics:

- ☐ Conversion from decimal to binary (random numbers)
- ☐ Conversion from binary to decimal (random numbers)
- ☐ Subnetting IPv4 (random networks and scenarios)

https://t.me/learningnets

Day 6 – Network Address Translation

Day 6 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's labs
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website

Network Address Translation (NAT) is another strange subject, because Cisco has broken down NAT requirements between the ICND1 and the ICND2 syllabuses.

Today you will learn about the following:

- NAT basics
- Configuring and verifying NAT
- NAT troubleshooting

This module maps to the following ICND1 syllabus requirements:

- Identify the basic operation of NAT
  - Purpose
  - Pool
  - Static
  - One-to-one
  - Overloading
  - Source addressing
  - One-way NAT
- Configure and verify NAT for given network requirements

NAT Basics

Imagine for a moment that networks run on colours instead of using IP addresses. There is an unlimited supply of the colours blue and yellow but the other colours are in short supply. Your network is divided into many users using the colours blue and yellow because they are free to use. The blue users need to get out to the web fairly regularly, so you buy a few green tokens which your router can use to swap for the blue users' tokens when they need to reach hosts on the web. Your router would be doing this:

https://t.me/learningnets

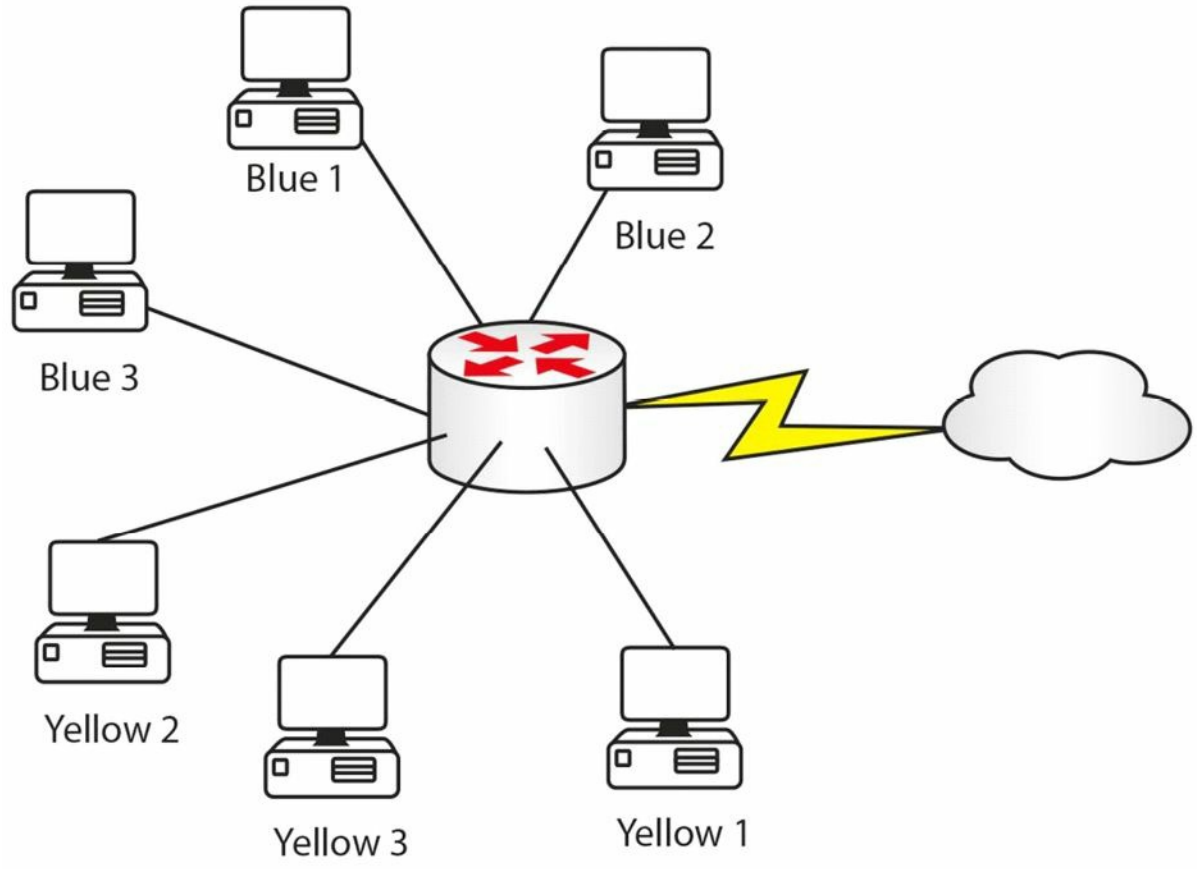


Figure 6.1 – Inside Tokens Swapped for Outside Tokens

Inside Tokens	Outside Tokens
Blue 1	Green 1
Blue 2	Green 2
Blue 3	Green 3

When each of the blue devices has finished with the outside connection, the green token can be released for use by another blue device. The benefits to this are outside devices can't see your internal token IDs and you are helping conserve the limited amount of green tokens available for use on the Internet.

As you can see, NAT not only protects your network IP addresses but also is another method of address conservation. NAT is performed on routers or firewalls, so, instead of colours, you would see something like this:

https://t.me/learningnets

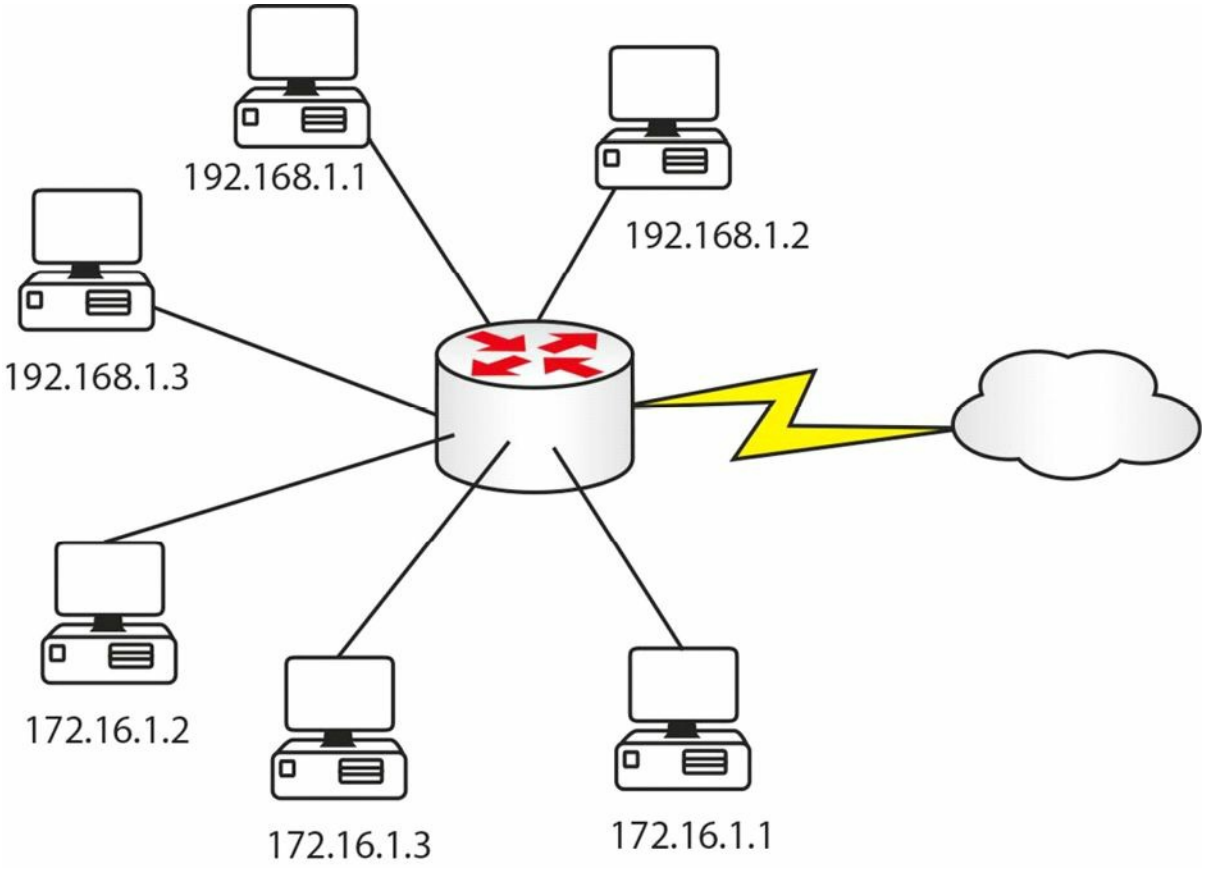


Figure 6.2 – Inside Addresses Swapped for Outside Addresses

Inside Addresses	Outside Addresses
192.168.1.1	200.100.1.5
192.168.1.3	200.100.1.7

There are three ways to configure NAT on your router, depending upon your particular requirements. You will need to know all three for the CCNA exam.

In order to configure NAT, you need to tell the router which interfaces are on the inside and outside of your NAT network. This is because you could actually swap internal addresses for a pool of NAT addresses, or, at the very least, a single NAT address, and perform NAT between two Ethernet interfaces on your router.

Having said that, for the exam and in the real world, you will usually translate private Internet addresses into routable addresses on the Internet. You will see this on your home broadband router, which will usually give your laptop an IP in the 192.168.1 range but then have a routable address on the interface to the ISP.

NAT enables hosts on private networks to access resources on the Internet or other public networks. NAT is an IETF standard that enables a LAN to use one set of IP addresses for internal traffic, typically private address space as defined in RFC 1918, and another set of addresses for external traffic, typically publicly registered IP address space.

NAT converts the packet headers for incoming and outgoing traffic and keeps track of each session. The key to understanding NAT and, ultimately, troubleshooting NAT problems is having a solid understanding of NAT terminology. You should be familiar with the following

https://t.me/learningnets

NAT terms:

- The NAT inside interface
- Inside local address
- Inside global address
- The NAT outside interface
- Outside local address
- Outside global address

In NAT terminology, the inside interface is the border interface of the administrative domain controlled by the organisation. This does not necessarily have to be the default gateway used by hosts that reside within the internal network.

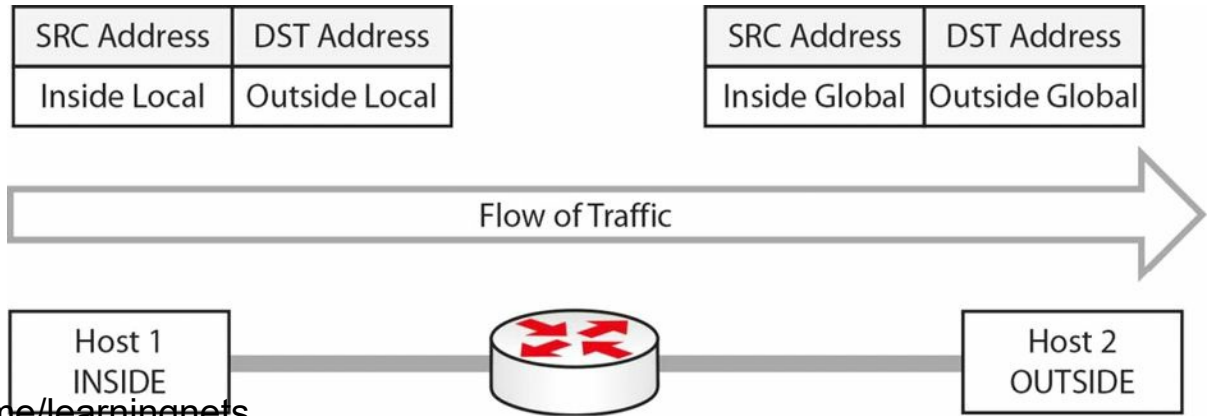
The inside local address is the IP address of a host residing on the inside network. In most cases, the inside local address is an RFC 1918 address (i.e., non-routable**,** such as 192.168.x.x or 172.16.x.x). This address is translated to the outside global address, which is typically an IP address from a publically assigned or registered pool. It is important to remember, however, that the inside local address could also be a public address.

The inside global address is the IP address of an internal host as it appears to the outside world. Once the inside IP address has been translated, it will appear as an inside global address to the Internet public or to any other external network or host.

The outside interface is the boundary for the administrative domain that is not controlled by the organisation. In other words, the outside interface is connected to the external network, which may be the Internet or any other external network, such as a partner network, for example. Any hosts residing beyond the outside interface fall outside the local organisation's administration.

The outside local address is the IP address of an outside, or external, host as it appears to inside hosts. Finally, the outside global address is an address that is legal and can be used on the Internet. Both outside local addresses and outside global addresses are typically allocated from a globally routable address or network space.

To clarify these concepts further, Figure 6.3 below shows the use of the addresses in a session between two hosts. NAT is enabled on the intermediate gateway:



https://t.me/learningnets

Figure 6.3 – Understanding NAT Inside and Outside Addresses

NAT inside and outside addressing is a classic exam question, so come back to this concept a few times.

Configuring and Verifying NAT

The configuration and verification of Network Address Translation with Cisco IOS software is a straightforward task. When configuring NAT, perform the following:

- Designate one or more interfaces as the internal (inside) interface(s) using the `ip nat inside` interface configuration command.
- Designate an interface as the external (outside) interface using the `ip nat outside` interface configuration command.
- Configure an access control list (ACL) that will match all traffic for translation. This can be a standard or an extended named or numbered ACL.
- Optionally, configure a pool of global addresses using the `ip nat pool <name> <start-ip> <end-ip> [netmask <mask> | prefix-length <length>]` global configuration command. This defines a pool of inside global addresses to which inside local addresses will be translated.
- Configure NAT globally using the `ip nat inside source list <ACL> [interface|pool] <name> [overload]` global configuration command.

> Farai says – "Please also check out the `ip nat inside source static` command, which you can review for free at www.howtonetwork.net/public/698.cfm."

The following output shows you one way to configure NAT (dynamic NAT) with Cisco IOS software. You can see that the configuration has used the `description` and `remark` features available to help administrators more easily manage and troubleshoot their networks:

```
R1(config)#interface FastEthernet0/0
R1(config-if)#description 'Connected To The Internal LAN'
R1(config-if)#ip address 10.5.5.1 255.255.255.248
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface Serial0/0
R1(config-if)#description 'Connected To The ISP'
R1(config-if)#ip address 150.1.1.1 255.255.255.248
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#access-list 100 remark 'Translate Internal Addresses Only'
R1(config)#access-list 100 permit ip 10.5.5.0 0.0.0.7 any
R1(config)#ip nat pool INSIDE-POOL 150.1.1.3 150.1.1.6 prefix-length 24
```

https://t.me/learningnets

```
R1(config)#ip nat inside source list 100 pool INSIDE-POOL
R1(config)#exit
```

Following this configuration, the `show ip nat translations` command can be used to verify that translations are actually taking place on the router, as illustrated below:

```
R1#show ip nat translations
Pro  Inside global  Inside local   Outside local  Outside global
icmp 150.1.1.4:4    10.5.5.1:4     200.1.1.1:4    200.1.1.1:4
icmp 150.1.1.3:1    10.5.5.2:1     200.1.1.1:1    200.1.1.1:1
tcp  150.1.1.5:159  10.5.5.3:159   200.1.1.1:23   200.1.1.1:23
```

You actually have three choices when it comes to configuring NAT on your router:

- Swap one internal address for one external address (static NAT)
- Swap many internal addresses for two or more external addresses (dynamic NAT)
- Swap many internal addresses for many external ports (Port Address Translation or one-way NAT)

Static NAT

You would want to swap one specific address for another address when you have a web server (for example) on the inside of your network. If you keep using dynamic addressing, then there is no way to reach the destination address because it keeps changing.

> Farai says – "You would use static NAT (see Figure 6.4 below) for any server that needs to be reachable via the Internet, such as e-mail or FTP."

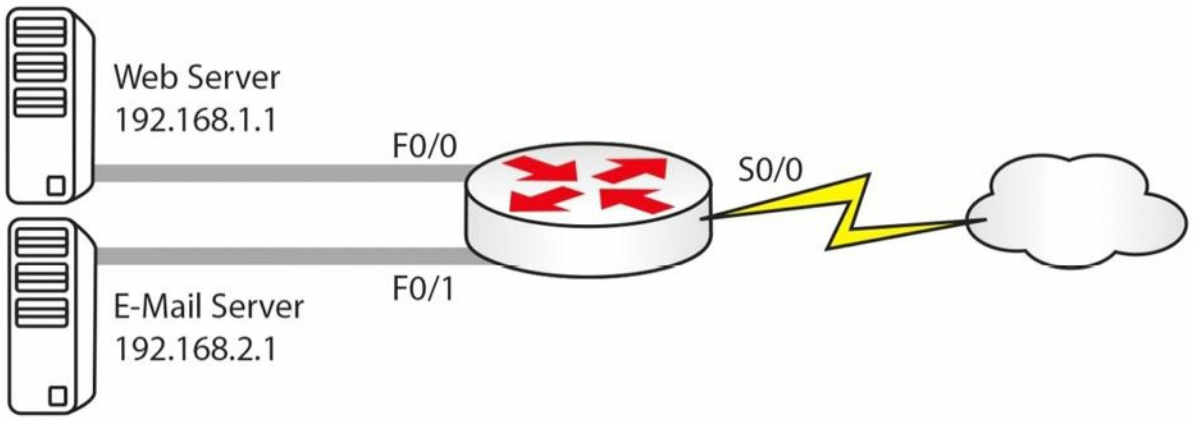


Figure 6.4 – Static NAT in Use

Inside Addresses	Outside NAT Addresses
192.168.1.1	200.1.1.1
192.168.2.1	200.1.1.2

For the network above, your configuration would be as follows:

https://t.me/learningnets

```
Router(config)#interface f0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config)#interface f0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config)#interface s0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat inside source static 192.168.1.1 200.1.1.1
Router(config)#ip nat inside source static 192.168.2.1 200.1.1.2
```

The `ip nat inside` and `ip nat outside` commands tell the router which are the inside NAT interfaces and which are the outside NAT interfaces. The `ip nat inside source` command defines the static translations, of which you could have as many as you wish, so long as you paid for the public IP addresses. The vast majority of configuration mistakes I fixed whilst at Cisco were missing `ip nat inside` and `ip nat outside` statements! You might see questions in the exam where you have to spot configuration mistakes.

I strongly recommend that you type the commands above onto a router. You will do many NAT labs in this book, but the more you type whilst you read the theory section, the better the information will stick in your head.

Dynamic NAT or NAT Pool

You will often need to use a group, or pool, of routable addresses. One-to-one NAT mapping has its limitations, of course, expense and extensive lines of configuration on your router to name two. Dynamic NAT allows you to configure one or more groups of addresses to be used by your internal hosts.

Your router will keep a list of the internal addresses to external addresses, and eventually the translation in the table will time out. You can alter the timeout values but please do so on the advice of a Cisco TAC engineer.

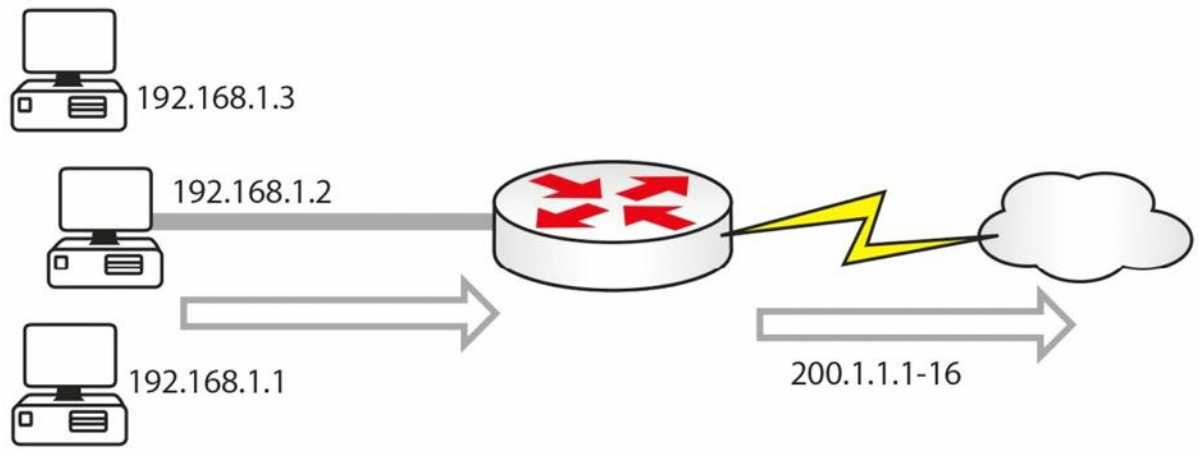


Figure 6.5 – Internal Addresses to a NAT Pool of Routable Addresses

If you issued a `show ip nat translations` command on the router when the inside hosts have made outside connections, you would see a chart containing something like this:

Inside Addresses	Outside NAT Addresses
192.168.1.3	200.1.1.11

https://t.me/learningnets

192.168.1.2	200.1.1.14

In Figure 6.5 above, you have internal addresses using a pool of addresses from 200.1.1.1 to 200.1.1.16. Here is the configuration file to achieve it. I have left off the router interface addresses for now:

```
Router(config)#interface f0/0
Router(config-if)#ip nat inside
Router(config)#interface s0/1
Router(config-if)#ip nat outside

Router(config)#ip nat pool poolname 200.1.1.1 200.1.1.16 netmask 255.255.255.0

Router(config)#ip nat inside source list 1 pool poolname

Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

The ACL is used to tell the router which addresses it can and cannot translate. The subnet mask is actually reversed and is called a wildcard mask, which will be covered later. All NAT pools need a name, and in this example, it is simply called “poolname.” The source list refers to the ACL.

NAT Overload/Port Address Translation/One-Way NAT

IP addresses are in short supply, and if you have hundreds or thousands of addresses which need to be routed, it could cost you a lot of money. In this instance, you can use NAT overload (see Figure 6.6), also referred to as Port Address Translation (PAT) or one-way NAT by Cisco. PAT cleverly allows a port number to be added to the IP address as a way of uniquely identifying it from another translation using the same IP address. There are over 65,000 ports available per IP address.

Although this is beyond the scope of the CCNA exam, it could be useful to know how PAT handles port numbers. Per Cisco documentation, it divides the available ports per global IP address into three ranges: 0–511, 512–1023, and 1024–65535. PAT assigns a unique source port to each UDP or TCP session. It will attempt to assign the same port value of the original request, but if the original source port has already been used, it will start scanning from the beginning of the particular port range to find the first available port and will assign it to the conversation.

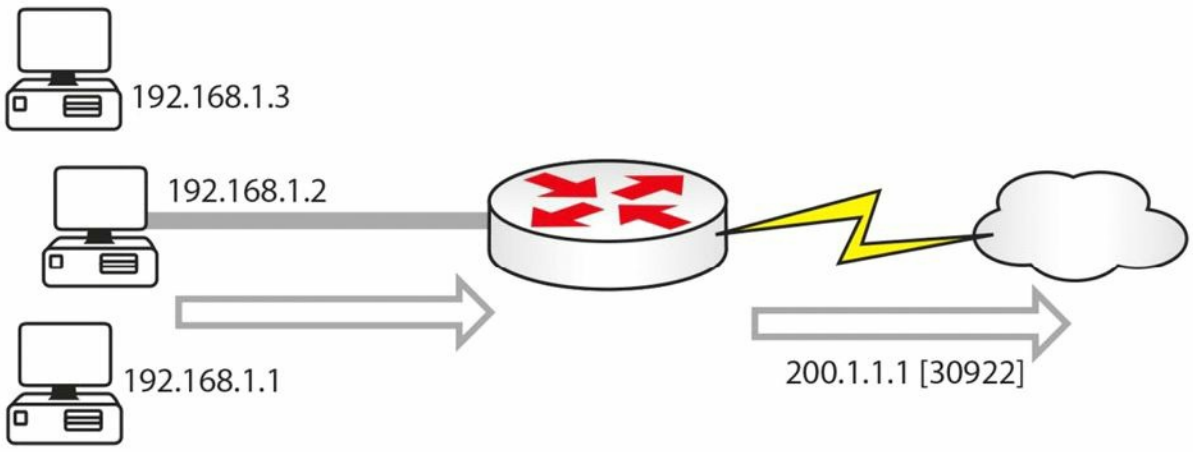


Figure 6.6 – NAT Overload

https://t.me/learningnets

The `show ip nat translations` table this time would show the IP addresses and port numbers:

Inside Addresses	Outside NAT Addresses (with Port Numbers)
192.168.1.1	200.1.1.1:30922
192.168.2.1	200.1.1.2:30975

To configure PAT, you would carry out the exact same configuration as for dynamic NAT, but you would add the keyword [`overload`] to the end of the pool:

```
Router(config)#interface f0/0
Router(config-if)#ip nat inside
Router(config)#interface s0/1
Router(config-if)#ip nat outside
Router(config)#ip nat pool poolname 200.1.1.1 200.1.1.1 netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool poolname overload
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

This should be pretty easy to remember!

> Farai says – "Using PAT with more than one IP is a waste of address space because the router will use the first IP and increment port numbers for each subsequent connection. This is why PAT is typically configured to overload to the interface."

Troubleshooting NAT

Nine times out of ten, the router administrator has forgotten to add the `ip nat outside` or `ip nat inside` command to the router interfaces. In fact, this is almost always the problem! The next most frequent mistakes include the wrong ACL and a misspelled pool name (it is case sensitive).

You can debug NAT translations on the router by using the `debug ip nat [detailed]` command, and you can view the NAT pool with the `show ip nat translations` command.

Day 6 Questions

1. NAT converts the _____ headers for incoming and outgoing traffic and keeps track of each session.
2. The _____ address is the IP address of an outside, or external, host as it appears to inside hosts.
3. How do you designate inside and outside NAT interfaces?
4. Which `show` command displays a list of your NAT table?
5. When would you want to use static NAT?
6. Write the configuration command for NAT 192.168.1.1 to 200.1.1.1.
7. Which command do you add to a NAT pool to enable PAT?

8. NAT most often fails to work because the _____ command is missing.
9. Which `debug` command shows live NAT translations occurring?

https://t.me/learningnets

Day 6 Answers

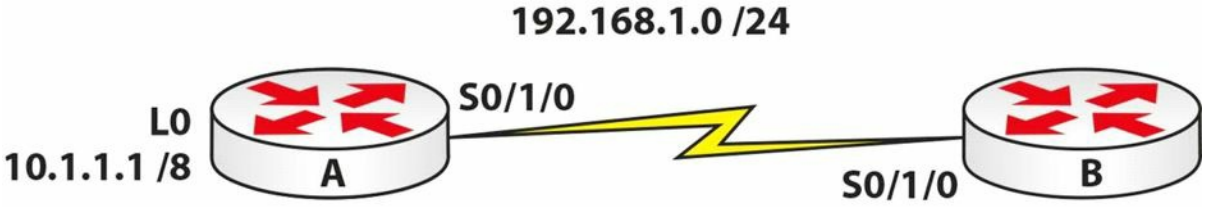
1. Packet.
2. Outside local.
3. With the `ip nat inside` and `ip nat outside` commands.
4. The `show ip nat translations` command.
5. When you have a web server (for example) on the inside of your network.
6. `ip nat inside source static 192.168.1.1 200.1.1.1`.
7. The `overload` command.
8. The `ip nat inside` or `ip nat outside` command.
9. The `debug ip nat [detailed]` command.

https://t.me/learningnets

Day 6 Labs

Static NAT Lab

Topology



Purpose

Learn how to configure static NAT.

Walkthrough

1. Add IP address 192.168.1.1 255.255.255.0 to Router A and change the hostname to Router A. Add IP address 192.168.1.2 255.255.255.0 to Router B. Add a clock rate to the correct side and ping from A to B or from B to A. Check the previous labs if you need a reminder.
2. You need to add an IP address to Router A to simulate a host on the LAN. You can achieve this with a Loopback interface:

```
RouterA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)#interface Loopback0
RouterA(config-if)#ip add 10.1.1.1 255.0.0.0
RouterA(config-if)#
```

3. For testing, you need to tell Router B to send any traffic to any network back out towards Router A. You will do this with a static route:

```
RouterB#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RouterB(config)#ip route 0.0.0.0 0.0.0.0 Serial0/1/0
RouterB(config)#
```

4. Test to see whether the static route is working by pinging from the Loopback interface on Router A to Router B:

```
RouterA#ping
Protocol [ip]:
Target IP address: 192.168.1.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
```

https://t.me/learningnets

```
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/31/32 ms
RouterA#
```

5. Configure a static NAT entry on Router A. Using NAT, translate the 10.1.1.1 address to 172.16.1.1 when it leaves the router. You also need to tell the router which is the inside and outside NAT interface:

```
RouterA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)#int Loopback0
RouterA(config-if)#ip nat inside
RouterA(config-if)#int Serial0/1/0
RouterA(config-if)#ip nat outside
RouterA(config-if)#
RouterA(config-if)#ip nat inside source static 10.1.1.1 172.16.1.1
RouterA(config)#
```

6. Turn on NAT debugging so you can see the translations taking place. Then issue another extended ping (from L0) and check the NAT table. Your output may differ from mine due to changes in IOS.

```
RouterA#debug ip nat
IP NAT debugging is on
RouterA#
RouterA#ping
Protocol [ip]:
Target IP address: 192.168.1.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
```

https://t.me/learningnets

```
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
NAT: s=10.1.1.1->172.16.1.1, d=192.168.1.2 [11]
!
NAT*: s=192.168.1.2, d=172.16.1.1->10.1.1.1 [11]
NAT: s=10.1.1.1->172.16.1.1, d=192.168.1.2 [12]
!
NAT*: s=192.168.1.2, d=172.16.1.1->10.1.1.1 [12]
NAT: s=10.1.1.1->172.16.1.1, d=192.168.1.2 [13]
!
NAT*: s=192.168.1.2, d=172.16.1.1->10.1.1.1 [13]
NAT: s=10.1.1.1->172.16.1.1, d=192.168.1.2 [14]
!
NAT*: s=192.168.1.2, d=172.16.1.1->10.1.1.1 [14]
NAT: s=10.1.1.1->172.16.1.1, d=192.168.1.2 [15]
!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/46/110 ms
RouterA#
NAT*: s=192.168.1.2, d=172.16.1.1->10.1.1.1 [15]
RouterA#show ip nat translations
Pro  Inside global Inside local  Outside local    Outside global
icmp 172.16.1.1:10 10.1.1.1:10   192.168.1.2:10   192.168.1.2:10
icmp 172.16.1.1:6  10.1.1.1:6    192.168.1.2:6    192.168.1.2:6
icmp 172.16.1.1:7  10.1.1.1:7    192.168.1.2:7    192.168.1.2:7
icmp 172.16.1.1:8  10.1.1.1:8    192.168.1.2:8    192.168.1.2:8
icmp 172.16.1.1:9  10.1.1.1:9    192.168.1.2:9    192.168.1.2:9
---  172.16.1.1    10.1.1.1           ---              ---
RouterA#
```

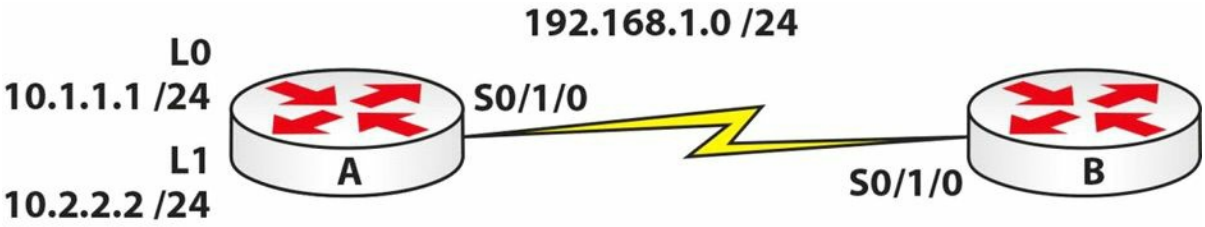
7. Bear in mind that the router will clear the NAT translation soon afterwards in order to clear the NAT address(es) for use by other IP addresses:

```
NAT: expiring 172.16.1.1 (10.1.1.1) icmp 6 (6)
NAT: expiring 172.16.1.1 (10.1.1.1) icmp 7 (7)
```

NAT Pool Lab

Topology

https://t.me/learningnets



Purpose

Learn how to configure a NAT pool (dynamic NAT).

Walkthrough

1. Add IP address 192.168.1.1 255.255.255.0 to Router A and change the hostname to Router A. Add IP address 192.168.1.2 255.255.255.0 to Router B. Add a clock rate to the correct side and ping from A to B or from B to A. Check the previous lab if you need a reminder.
2. You need to add two IP addresses to Router A to simulate a host on the LAN. You can achieve this with two Loopback interfaces. They will be in different subnets but both start with a 10 address:

```
RouterA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)#interface Loopback0
RouterA(config-if)#ip add 10.1.1.1 255.255.255.0
RouterA(config-if)#int l1 ← short for Loopback1
RouterA(config-if)#ip address 10.2.2.2 255.255.255.0
RouterA(config-if)#
```

3. For testing, you need to tell Router B to send any traffic to any network back out towards Router A. You will do this with a static route:

```
RouterB#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RouterB(config)#ip route 0.0.0.0 0.0.0.0 Serial0/1/0
RouterB(config)#
```

4. Test to see whether the static route is working by pinging from the Loopback interface on Router A to Router B:

```
RouterA#ping
Protocol [ip]:
Target IP address: 192.168.1.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
```

https://t.me/learningnets

```
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/31/32 ms
RouterA#
```

5. Configure a NAT pool on Router A. For this lab, use 172.16.1.1 to 172.16.1.10. Any address starting with 10 will be a NAT. Remember that you MUST specify the inside and outside NAT interfaces or NAT won't work:

```
RouterA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)#int l0
RouterA(config-if)#ip nat inside
RouterA(config)#int l1
RouterA(config-if)#ip nat inside
RouterA(config-if)#int Serial0/1/0
RouterA(config-if)#ip nat outside
RouterA(config-if)#exit
RouterA(config)#ip nat pool 60days 172.16.1.1 172.16.1.10 netmask 255.255.255.0
RouterA(config)#ip nat inside source list 1 pool 60days
RouterA(config)#access-list 1 permit 10.1.1.0 0.0.0.255
RouterA(config)#access-list 1 permit 10.2.1.0 0.0.0.255
RouterA(config)#
```

The `ip nat pool` command creates the pool of addresses. You need to give the pool a name of your own choosing. The `netmask` command tells the router which network mask to apply to the pool.

The `source list` command tells the router which ACL to look at. The ACL tells the router which networks will match the NAT pool.

6. Turn on NAT debugging so you can see the translations taking place. Then issue extended pings (from L0 and L1) and check the NAT table. Your output may differ from mine due to changes in IOS. You should see two addresses from the NAT pool being used.

```
RouterA#debug ip nat
RouterA#ping
Protocol [ip]:
Target IP address: 192.168.1.2
Repeat count [5]:
```

https://t.me/learningnets

```
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
NAT: s=10.1.1.1->172.16.1.1, d=192.168.1.2 [26]
!
NAT*: s=192.168.1.2, d=172.16.1.1->10.1.1.1 [16]
NAT: s=10.1.1.1->172.16.1.1, d=192.168.1.2 [27]
!
NAT*: s=192.168.1.2, d=172.16.1.1->10.1.1.1 [17]
NAT: s=10.1.1.1->172.16.1.1, d=192.168.1.2 [28]
!
NAT*: s=192.168.1.2, d=172.16.1.1->10.1.1.1 [18]
NAT: s=10.1.1.1->172.16.1.1, d=192.168.1.2 [29]
!
NAT*: s=192.168.1.2, d=172.16.1.1->10.1.1.1 [19]
NAT: s=10.1.1.1->172.16.1.1, d=192.168.1.2 [30]
!
Success rate is 100 percent (5/5), round-trip min/avg/max = 17/28/32 ms
RouterA#
NAT*: s=192.168.1.2, d=172.16.1.1->10.1.1.1 [20]
RouterA#ping
Protocol [ip]:
Target IP address: 192.168.1.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.2.2.2
Type of service [0]:
Set DF bit in IP header? [no]:
```

https://t.me/learningnets

```
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
Packet sent with a source address of 10.2.2.2
NAT: s=10.2.2.2->172.16.1.2, d=192.168.1.2 [31]
!
NAT*: s=192.168.1.2, d=172.16.1.2->10.2.2.2 [21]
NAT: s=10.2.2.2->172.16.1.2, d=192.168.1.2 [32]
!
NAT*: s=192.168.1.2, d=172.16.1.2->10.2.2.2 [22]
NAT: s=10.2.2.2->172.16.1.2, d=192.168.1.2 [33]
!
NAT*: s=192.168.1.2, d=172.16.1.2->10.2.2.2 [23]
NAT: s=10.2.2.2->172.16.1.2, d=192.168.1.2 [34]
!
NAT*: s=192.168.1.2, d=172.16.1.2->10.2.2.2 [24]
NAT: s=10.2.2.2->172.16.1.2, d=192.168.1.2 [35]
!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/31/32 ms
RouterA#
NAT*: s=192.168.1.2, d=172.16.1.2->10.2.2.2 [25]
RouterA#show ip nat trans
Pro  Inside global Inside local  Outside local     Outside global
icmp 172.16.1.1:16 10.1.1.1:16   192.168.1.2:16    192.168.1.2:16
icmp 172.16.1.1:17 10.1.1.1:17   192.168.1.2:17    192.168.1.2:17
icmp 172.16.1.1:18 10.1.1.1:18   192.168.1.2:18    192.168.1.2:18
icmp 172.16.1.1:19 10.1.1.1:19   192.168.1.2:19    192.168.1.2:19
icmp 172.16.1.1:20 10.1.1.1:20   192.168.1.2:20    192.168.1.2:20
icmp 172.16.1.2:21 10.2.2.2:21   192.168.1.2:21    192.168.1.2:21
icmp 172.16.1.2:22 10.2.2.2:22   192.168.1.2:22    192.168.1.2:22
icmp 172.16.1.2:23 10.2.2.2:23   192.168.1.2:23    192.168.1.2:23
icmp 172.16.1.2:24 10.2.2.2:24   192.168.1.2:24    192.168.1.2:24
icmp 172.16.1.2:25 10.2.2.2:25   192.168.1.2:25    192.168.1.2:25
RouterA#
```

NAT Overload Lab

Repeat the previous lab. This time, when referring to the pool, add the `overload` command to

https://t.me/learningnets

the end of the configuration line. This instructs the router to use PAT. Leave off `Loopback1`. Please note that as Farai says, in the real world, your pool will usually have only one address or you will overload your outside interface.

```
RouterA(config)#ip nat inside source list 1 pool 60days overload
```

I've done some of the previous labs using Cisco Packet Tracer for convenience, so you will often see different output to mine. Here is a sample output from a PAT lab. You will see that the router is adding a port number to each translation. Unfortunately, you see a similar number at the end of the NAT pool labs, which is an annoyance of PAT.

```
RouterA#show ip nat tran
Inside global  Inside local       Outside local     Outside global
10.0.0.1:8759 172.16.1.129:8759 192.168.1.2:8759 192.168.1.2:8759
```

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 7 – IPv6

Day 7 Tasks

- Read the theory lesson below
- Read the ICND1 cram guide

IPv6 has been in development for several years and has actually been implemented on networks all over the world (in conjunciton with IPv4). Many network engineers have expressed their fear about having to learn a new addressing method, and I've even heard many say that they hope to retire before it becomes a requirement.

This fear, however, is unfounded. IPv6 is a user-friendly format, and once you become used to it, you will see that it is an improvement on IPv4 and you may actually come to prefer it. IPv6 is heavily tested in the CCNA exam; for this reason, you need to feel comfortable understanding how it works, as well as how to configure addresses, understand the standard, and apply IPv6 addresses to address network requirements.

Today you will learn about the following:

- History of IPv6
- IPv6 addressing format
- Implementing IPv6
- IPv6 subnetting

This module maps to the following CCNA syllabus requirements:

- Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment
- Describe IPv6 addresses
  - Global Unicast
  - Multicast
  - Link-Local
  - Unique-Local
  - EUI 64
  - Autoconfiguration

History of IPv6

Fit for Purpose?

When Sir Tim Berners-Lee devised the World Wide Web in 1989, there was no way he could have predicted the huge impact it was to have on the world. Personal computers were prohibitively expensive and there was no easy way to communicate over long distances unless

you could afford expensive WAN connections. Even then, there was no agreed communication model for all to follow.

Something needed to change and change came in the form of a new addressing standard for IP. Learning from mistakes made and responding to changes in business requirements, the Internet Engineering Task Force (IETF) published the first of many IPv6 standards as far back as 1998.

There will be no switch-over date; instead, networks will gradually transition to running both IPv4 and IPv6, and then eventually IPv4 will be phased out of existence. At the moment, approximately 1% of all Internet traffic is running on IPv6 (source: Yves Poppe, IPv6 – A 2012 Report Card).

Why Migrate?

I've already said that when IPv4 was devised, the Internet wasn't used by the general public, and why would they? There were no websites, no e-commerce, no mobile networks, and no social media. Even if you could afford a PC, there wasn't much you could do with it. Now, of course, almost everybody is online. We carry out most of our day-to-day tasks using the Internet, and businesses rely on it to exist. Soon we will be using mobile devices to manage our cars and home security, to turn the coffee maker on, to set the heating level, and to set the TV to record our favourite show.

Some of this is already taking place, not only in Europe and the Americas but also in fast-developing countries such as India and China where billions of people live. IPv4 simply isn't up to the job and even if it was, there aren 't enough addresses to cater for demand.

Here are a few benefits to changing to IPv6:

- The simplified IPv6 Packet header
- Larger address space
- IPv6 addressing hierarchy
- IPv6 extensibility
- IPv6 broadcast elimination
- Stateless autoconfiguration
- Integrated mobility
- Integrated enhanced security

I'd like to delve into packet layer analysis of IPv6, as well as the many types of headers available, but there isn't space here to do so, and since it isn't tested in the exam there is no need to include it. Instead, I will focus on what you need to know for the exam and your role as a Cisco engineer.

Hex Numbering

It may be well worthwhile to have a short memory jogger on hex numbering.

https://t.me/learningnets

You know that decimal numbers consist of 10 digits ranging from 0 to 9. Binary consists of two digits ranging from 0 to 1. Hex numbering ranges from 0 to F and has 16 digits. These addresses are also referred to as base 10, base 2, and base 16, respectively.

You can see that each numbering system starts with a zero, so:

Decimal – 0,1,2,3,4,5,6,7,8,9

Binary – 0,1

Hex – 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F

When you write these addresses, you may not realise it but you are using columns from right to left; the rightmost is the one column and the next column is the base number times the preceding column, so:

Numbering Base	N to 3rd power	N to 2nd power	N to 1st power	N
10 – Decimal	1000	100	10	1
2 – Binary	8	4	2	1
16 – Hex	4096	256	16	1

You can see that each successive column from the right increases in value. For decimal numbering it is 10 multiplied by 1. For binary it is 1 and then 1 multiplied by the numbering system of 2. If you compare the three numbering systems up to the last hex digit, you can begin to see why hex is the preferred format for IPv6 addressing.

Decimal	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

https://t.me/learningnets

In order to provide enough addresses for our needs many years into the future, IPv6 has been designed to provide many trillions of available addresses. In order to do this, the numbering range has been expanded from 32 binary bits to 128 bits. Every 4 bits can be represented as one hex digit (as can be seen from the chart above). Logic then dictates that two hex digits will give us 8 bits, which is a single byte, or octet.

An IPv6 address is 128 bits in length and this is broken down into eight sets of 16 bits each separated by a colon when written in full format. Every 4 hex bits can range from 0000 to FFFF, with F being the highest digit available in hex numbering:

0000	0000	0000	0000	0000	0000	0000	0000
to	to	to	to	to	to	to	to
FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF

IPv6 Addressing

As we already know, IPv6 uses 128-bit addresses. Because the address format is different from the IPv4 address format that we are all accustomed to, it is often confusing at first glance. However, once understood, the logic and structure is all very simple. The 128-bit IPv6 addresses use hexadecimal values (i.e., numbers 0 through 9 and letters A through F). While in IPv4 the subnet mask can be represented in either CIDR notation (e.g., /16 or /32) or in dotted-decimal notation (e.g., 255.255.0.0 or 255.255.255.255), IPv6 subnet masks are represented only in CIDR notation due to the length of the IPv6 address. Global 128-bit IPv6 addresses are divided into the following three sections:

- The provider-assigned prefix
- The site prefix
- The interface or host ID

The provider-assigned prefix, which is also referred to as the global address space, is a 48-bit prefix that is divided into the following three distinct parts:

- The 16-bit reserved IPv6 global prefix
- The 16-bit provider-owned prefix
- The 16-bit provider-assigned prefix

The IPv6 global prefix is used to represent the IPv6 global address space. All IPv6 global Internet addresses fall within the 2000::/16 to 3FFF::/16 range. The 16-bit provider-owned IPv6 prefix is assigned to and owned by the provider. The assignment of these prefixes follows the same rules as prefix assignment in IPv4. The provider-owned prefix falls within the 0000::/32 to FFFF::/32 range.

The next 16-bits represent an IPv6 prefix assigned to an organisation by the actual provider from within the provider-assigned prefix address space. This prefix falls within the 0000::/48 to FFFF::/48 range. Collectively, these first 48-bits are referred to as the provider-assigned prefix,

which is illustrated in Figure 7.1 below:

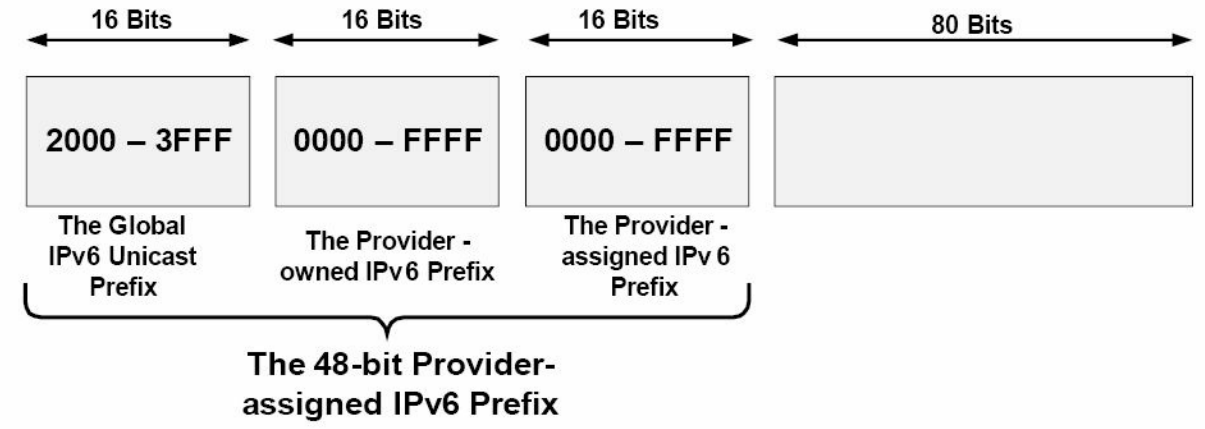


Figure 7.1 – The 48-bit Provider-Assigned IPv6 Prefix

The site prefix is the next 16 bits following the 48-bit provider-assigned prefix. The subnet mask length for a site prefix is /64, which includes the 48-bit provider-assigned prefix. This prefix length allows for 264 addresses within each site prefix. Figure 7.2 below illustrates the 16-bit site prefix:

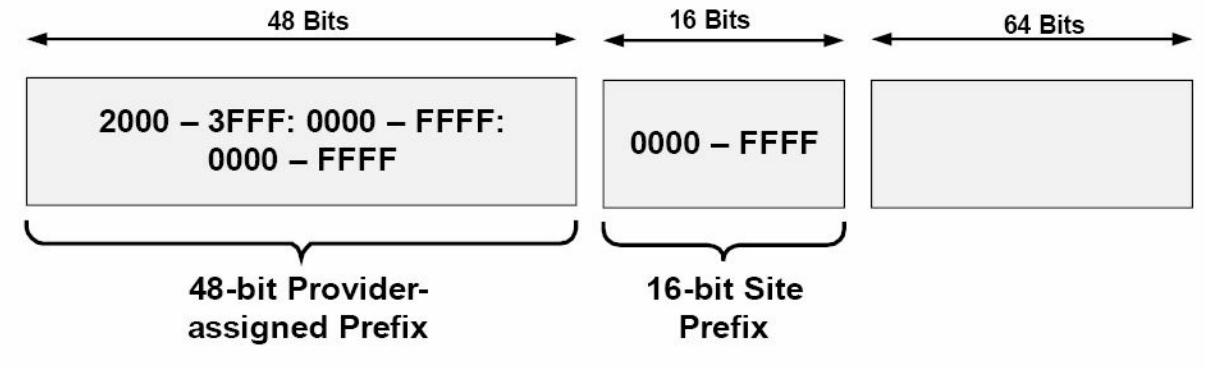


Figure 7.2 – The 16-bit IPv6 Site Prefix

Following the site prefix, the next 64 bits are used for interface or host addressing. The interface or host ID portion of an IPv6 address represents the network device or host on the IPv6 subnet. The different ways in which the interface or host address is determined will be described in detail later in this module. Figure 7.3 below illustrates how IPv6 prefixes are assigned:

https://t.me/learningnets

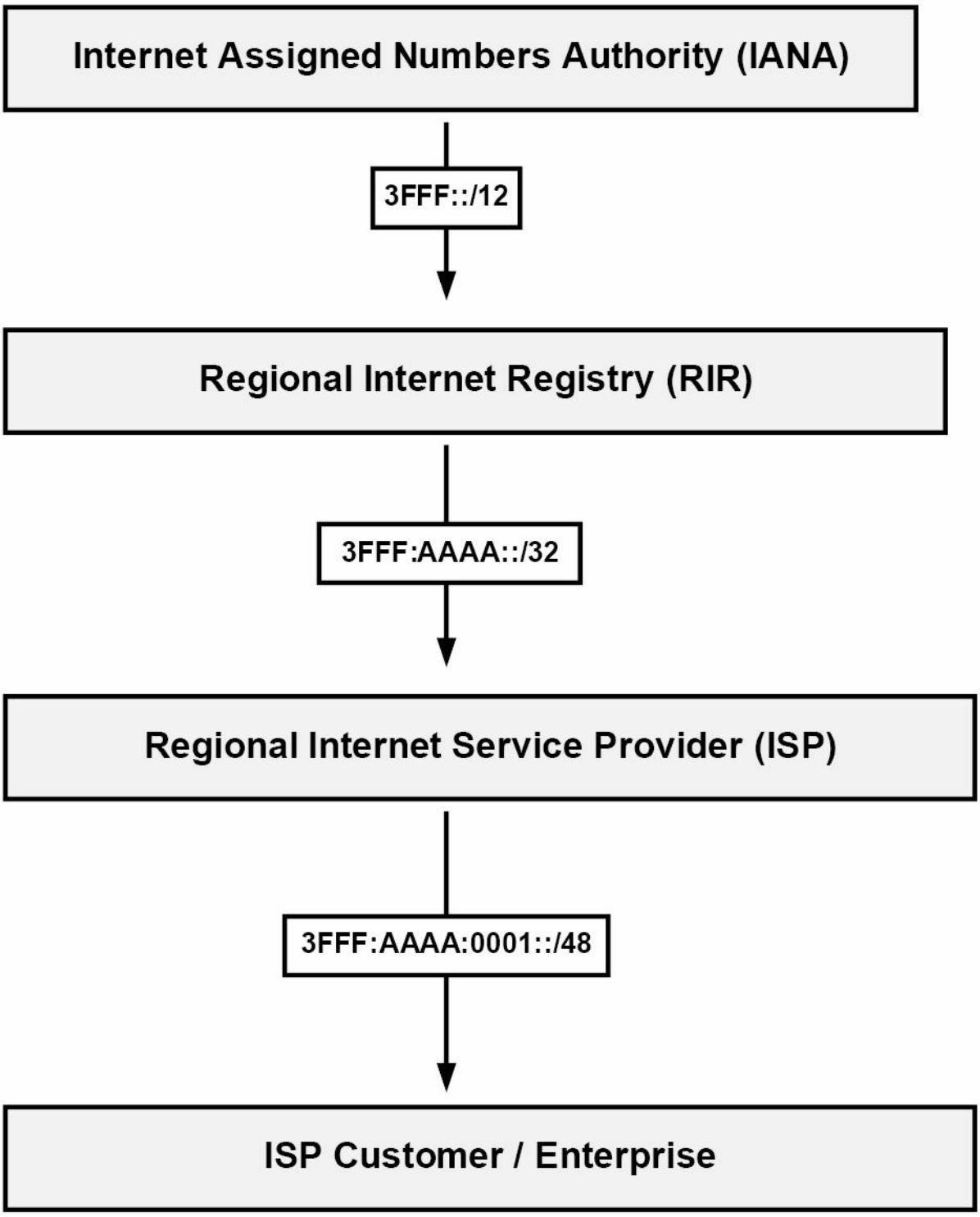


Figure 7.3 – Assigning IPv6 Prefixes

Referencing Figure 7.3, once customers have been assigned the /48 prefix by the ISP, they are then free to assign and use whatever site prefixes and host or interface addresses they want within that 48-bit provider-assigned prefix. The sheer amount of address space available makes it impossible for any single enterprise customer to require more than a single provider-assigned prefix, while still allowing all devices within the enterprise network to be allocated a unique IPv6 global address. NAT, therefore, will never be required for IPv6.

IPv6 Address Representation

The three ways in which IPv6 addresses can be represented are as follows:

- The preferred or complete address representation or form

https://ine.com/learning/labs

- Compressed representation
- IPv6 addresses with an embedded IPv4 address

While the preferred form or representation is the most commonly used method for representing the 128-bit IPv6 address in text format, it is also important to be familiar with the other two methods of IPv6 address representation. These methods are described in the following sections.

The Preferred Form

The preferred representation for an IPv6 address is the longest format, also referred to as the complete form of an IPv6 address. This format represents all 32 hexadecimal characters that are used to form an IPv6 address. This is performed by writing the address as a series of eight 16-bit hexadecimal fields, separated by a colon (e.g., 3FFF:1234:ABCD:5678:020C:CEFF:FEA7:F3A0).

Each 16-bit field is represented by four hexadecimal characters and each character represents 4 bits. Each 16-bit hexadecimal field can have a value of between 0x0000 and 0xFFFF, although, as will be described later in this module, different values have been reserved for use in the first 16 bits, so all possible values are not used. When writing IPv6 addresses, hexadecimal characters are not case sensitive. In other words, 2001:ABCD:0000 and 2001:abcd:0000 are the exact same thing. The complete form for IPv6 address representation is illustrated in Figure 7.4 below:

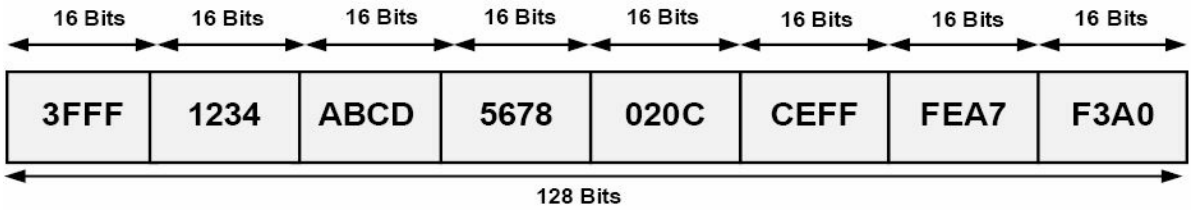


Figure 7.4 – The Preferred Form for IPv6 Address Representation

The following IPv6 addresses are examples of valid IPv6 addresses in the preferred form:

- 0000:0000:0000:0000:0000:0000:0000:0001
- 2001:0000:0000:1234:0000:5678:af23:bcd5
- 3FFF:0000:0000:1010:1A2B:5000:0B00:DE0F
- fec0:2004:ab10:00cd:1234:0000:0000:6789
- 0000:0000:0000:0000:0000:0000:0000:0000

Compressed Representation

Compressed representation allows for IPv6 addresses to be compressed in one of two ways. The first method allows a double colon (::) to be used to compress consecutive zero values in a valid IPv6 address for successive 16-bit fields comprised of zeros or for leading zeros in the IPv6 address. When using this method, it is important to remember that the double colon can be used only once in an IPv6 address.

When the compressed format is used, each node and router is responsible for counting the

https://t.me/learningnets

number of bits on either side of the double colon to determine the exact number of zeros it represents. Table 7.1 below shows IPv6 addresses in the preferred form and the compressed representation of those addresses:

Table 7.1 – Complete IPv6 Addresses in the Preferred Compressed Form

Complete IPv6 Address Representation	Compressed IPv6 Address Representation
0000:0000:0000:0000:0000:0000:0000:0001	::0001
2001:0000:0000:1234:0000:5678:af23:bcd5	2001::1234:0000:5678:af23:bcd5
3FFF:0000:0000:1010:1A2B:5000:0B00:DE0F	3FFF::1010:1A2B:5000:0B00:DE0F
FEC0:2004:AB10:00CD:1234:0000:0000:6789	FEC0:2004:AB10:00CD:1234::6789
0000:0000:0000:0000:0000:FFFF:172.16.255.1	::FFFF:172.16.255.1
0000:0000:0000:0000:0000:0000:172.16.255.1	::172.16.255.1
0000:0000:0000:0000:0000:0000:0000:0000	::

As previously stated, the double colon cannot be used more than once in a single IPv6 address. If, for example, you wanted to represent the complete IPv6 address for 2001:0000:0000:1234:0000:0000:af23:bcd5 in compressed form, you could use the double colon only once, even though there are two consecutive strings of zeros within the address. Therefore, attempting to compress the address to 2001::1234::af23:bcd5 would be considered illegal; however, the same IPv6 address could be compressed to either 2001::1234:0000:0000:af23:bcd5 or 2001:0000:0000:1234::af23:bcd5, depending upon preference.

The second method of IPv6 compressed address representation is applicable to each 16-bit field and allows leading zeros to be omitted from the IPv6 address. When using this method, if every bit in the 16-bit field is set to 0, then one zero must be used to represent this field. In this case, not all of the zero values can be omitted. Table 7.2 below shows IPv6 addresses in the preferred form and how they can be compressed using the second method of IPv6 compressed form representation.

Table 7.2 – Complete IPv6 Addresses in the Alternative Compressed Form

Complete IPv6 Address Representation	Compressed IPv6 Address Representation
0000:0123:0abc:0000:04b0:0678:f000:0001	0:123:abc:0:4b0:678:f000:1
2001:0000:0000:1234:0000:5678:af23:bcd5	2001:0:0:1234:0:5678:af23:bcd5
3FFF:0000:0000:1010:1A2B:5000:0B00:DE0F	3FFF:0:0:1010:1A2B:5000:B00:DE0F
fec0:2004:ab10:00cd:1234:0000:0000:6789	fec0:2004:ab10:cd:1234:0:0:6789
0000:0000:0000:0000:0000:FFFF:172.16.255.1	0:0:0:0:0:FFFF:172.16.255.1
0000:0000:0000:0000:0000:0000:172.16.255.1	0:0:0:0:0:0:172.16.255.1
0000:0000:0000:0000:0000:0000:0000:0000	0:0:0:0:0:0:0:0

https://t.me/Learningnets

While there are two methods of representing the complete IPv6 address in compressed form, it

is important to remember that both methods are not mutually exclusive. In other words, these methods can be used at the same time to represent the same IPv6 address. This is commonly used when the complete IPv6 address contains both consecutive strings of zeros and leading zeros in other fields within the address. Table 7.3 below shows IPv6 addresses in the complete form that include both consecutive strings of zeros and leading zeros, and how these addresses are represented in the compressed form:

Table 7.3 –Complete IPv6 Addresses Using Both Compressed Form Methods

Complete IPv6 Address Representation	Compressed IPv6 Address Representation
0000:0000:0000:0000:1a2b:000c:f123:4567	::1a2b:c:f123:4567
FEC0:0004:AB10:00CD:1234:0000:0000:6789	FEC0:4:AB10:CD:1234::6789
3FFF:0c00:0000:1010:1A2B:0000:0000:DE0F	3FFF:c00:0:1010:1A2B::DE0F
2001:0000:0000:1234:0000:5678:af23:00d5	2001::1234:0:5678:af23:d5

IPv6 Addresses with an Embedded IPv4 Address

The third representation of an IPv6 address is to use an embedded IPv4 address within the IPv6 address. While valid, it is important to keep in mind that this method is being deprecated and is considered obsolete because it is applicable only in the transition of IPv4 to IPv6.

The Different IPv6 Address Types

IPv4 supports four different classes of addresses, which are Anycast, Broadcast, Multicast, and Unicast. While the term Anycast has not been used in previous modules in this guide, it is important to remember that Anycast addresses are not special types of addresses. Instead, an Anycast address is simply an IP address that is assigned to multiple interfaces. Common examples of technologies that use Anycast addressing include IP Multicast implementations and 6to4 relay implementation.

NOTE: 6to4 is a transition mechanism for migrating from IPv4 to IPv6. For the CCNA exam, you only need to know that it exists.

With Anycast addressing, devices use the common address that is closest to them based on the routing protocol metric. The next closest address is then used in the event that the primary address is no longer reachable. This concept is illustrated in Figure 7.5 below:

https://t.me/learningnets

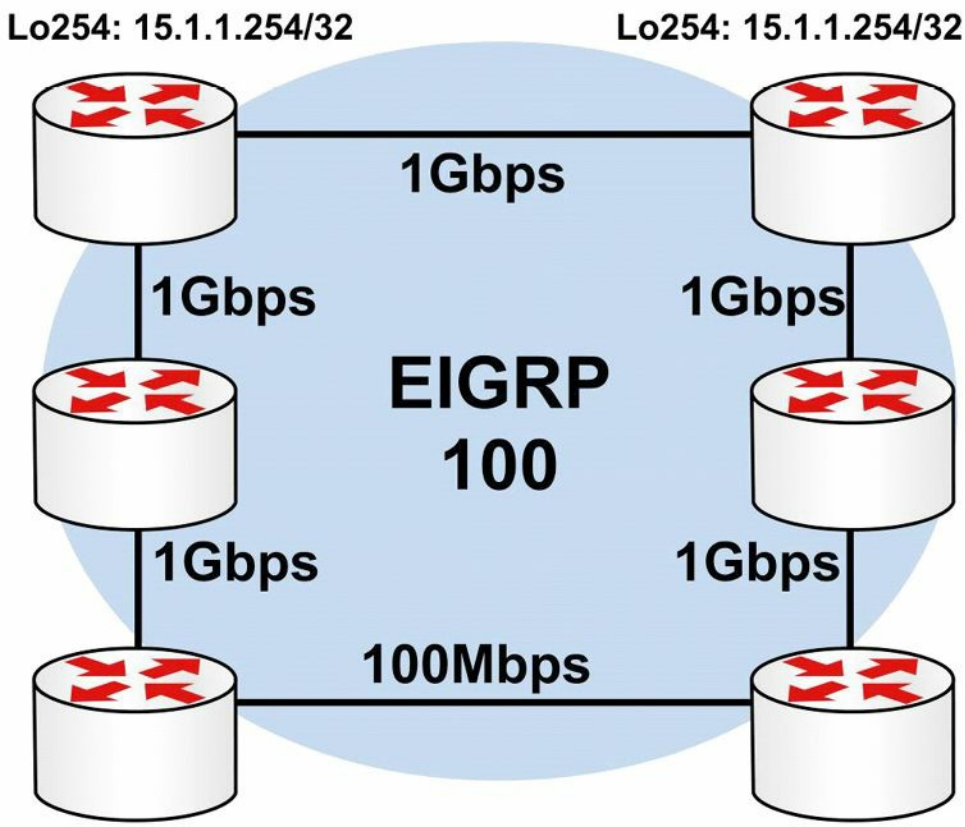


Figure 7.5 – Understanding Anycast Addressing

Referencing Figure 7.5, both R1 and R2 have a Loopback 254 interface that is configured using a common address: 15.1.1.254/32. This prefix is then advertised dynamically via EIGRP. By default, both R1 and R2 will prefer the 15.1.1.254/32 prefix via their respective Loopback interfaces, as that is a directly connected subnet. Therefore, the common address used will never result in a conflict on either router.

Assuming normal EIGRP metric calculation, R3 and R5 will prefer the Anycast address advertised by R1 due to the lower IGP metric. Similarly, R4 and R6 will prefer the Anycast address advertised by R2 due to the lower IGP metric. In the event that either R1 or R2 fails, the remaining routers in the network will use the Anycast address advertised by the remaining router. When using Anycast addressing, organisations can use a Unicast address either in the RFC 1918 address space or within their public block.

NOTE: You are not expected to implement any Anycast addressing or solutions in the current CCNA exam. However, it is important to be familiar with the concept. It will make more sense after you have reviewed the routing chapters.

At this level, IPv4 Broadcast, Multicast, and Unicast addresses require no further explanation and will not be described in any additional detail in this module or in the remainder of this guide. While IPv4 supports these four different types of addresses, IPv6 does away with the Broadcast addresses and instead supports only the following types of addresses:

- Link-Local addresses
- Site-Local addresses
- Aggregate Global Unicast addresses

https://t.me/learningnets

- Multicast addresses
- Anycast addresses
- Loopback addresses
- Unspecified addresses

Link-Local Addresses

IPv6 Link-Local addresses can be used only on the local link (i.e., a shared segment between devices), and are automatically assigned to each interface when IPv6 is enabled on that interface. These addresses are assigned from the Link-Local prefix FE80::/10. Keep in mind that FE80::/10 is the equivalent of FE80:0:0:0:0:0:0:0/10, which can also be represented as FE80:0000:0000:0000:0000:0000:0000:0000/10. To complete the address, bits 11 through 64 are set to 0 and the interface Extended Unique Identifier 64 (EUI-64) is appended to the Link-Local address as the low-order 64 bits. The EUI-64 is comprised of the 24-bit manufacturer ID assigned by the IEEE and the 40-bit value assigned by that manufacturer to its products. EUI-64 addressing is described in greater detail later in this module. The format for a Link-Local address is illustrated in Figure 7.6 below:

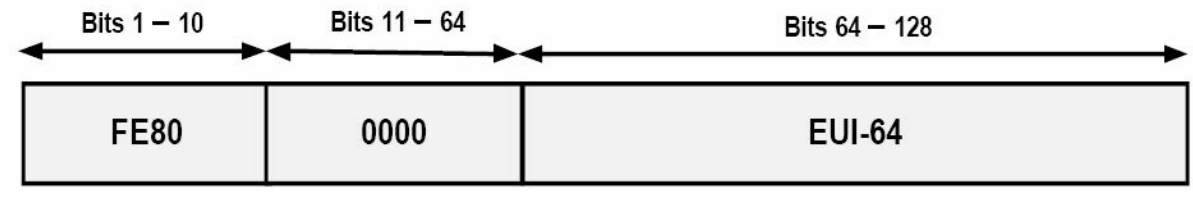


Figure 7.6 – IPv6 Link-Local Addressing

Link-local addresses are unique in that they do not change once assigned to an interface. This means that if an interface is assigned a public IPv6 address (e.g., 2001:1000::1/64) and the public IPv6 prefix was changed (i.e., 2001:2000::1/64), the Link-Local address would not change. This allows the host or router to remain reachable by its neighbour, while IPv6 global Internet addresses change. IPv6 routers should not forward packets that have Link-Local source or destination addresses to other IPv6 routers.

Site-Local Addresses

Site-Local addresses are Unicast addresses that are used only within a site. Unlike Link-Local addresses, Site-Local addresses must be configured manually on network devices. These addresses are the IPv6 equivalent of the private IPv4 address space defined in RFC 1918 and can be used by organisations that do not have globally routable IPv6 address space. These addresses are not routable on the IPv6 Internet.

While it is possible to perform NAT for IPv6, it is not recommended; hence, the reason for the much larger IPv6 addresses. Site-Local addresses are comprised of the FEC0::/10 prefix, a 54-bit subnet ID, and an interface identifier in the EUI-64 format used by Link-Local addresses. While the 54 bits in a Link-Local address are set to a value of 0, the same 54 bits in Site-Local addresses are used to create different IPv6 prefixes (up to 254). The format for the Site-Local address is illustrated in Figure 7.7 below:

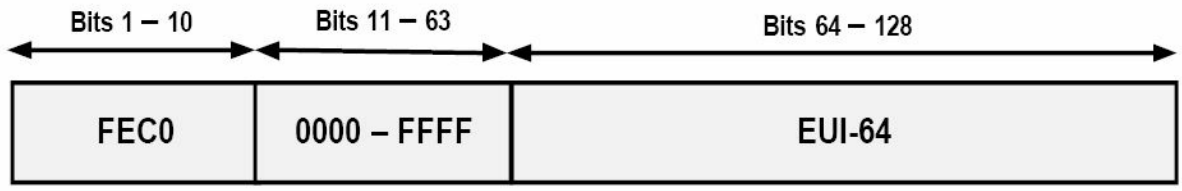


Figure 7.7 – IPv6 Site-Local Addressing

While IPv6 Site-Local addresses are described in this section and are still supported in Cisco IOS software, it is important to know that these addresses are deprecated by RFC 3879 (Deprecating Site Local Addresses). Moreover, RFC 4193 (Unique Local IPv6 Unicast Addresses) describes Unique-Local addresses (ULAs), which serve the same function as Site-Local addresses but they are not routable on the IPv6 global Internet, only within a site.

Unique-Local addresses are assigned from the FC00::/7 IPv6 address block, which is then further divided into two /8 address groups referred to as the assigned and random groups. These two groups are the FC00::/8 and the FD00::/8 IPv6 address blocks. The FC00::/8 block is managed by an allocation authority for /48s in use, while the FD00::/8 block is formed by appending a randomly generated 40-bit string to derive a valid /48 block.

Aggregate Global Unicast Addresses

Aggregate Global Unicast addresses are the IPv6 addresses used for generic IPv6 traffic, as well as for the IPv6 Internet. These are similar to the public addresses used in IPv4. From a network addressing point of view, each IPv6 Global Unicast address is comprised of three main sections: the prefix received from the provider (48 bits in length), the site prefix (16 bits in length), and the host portion (64 bits in length). This makes up the 128-bit address used in IPv6.

As we learned earlier in this module, the provider-assigned prefix is assigned to an organisation by an IPv6 provider. By default, these prefixes use /48 prefix lengths. In addition, these prefixes are assigned from the IPv6 address spaces (i.e., the /32 prefix lengths) that are owned by the provider. Each provider will own its own IPv6 address space, and the IPv6 prefix assigned by one provider cannot be used on the network of another provider.

Within a site, administrators can then subnet the provider-assigned 48-bit prefix into 64-bit site prefixes by using bits 49 through 64 for subnetting, allowing for 65,535 different subnets for use within their network. The host portion of an IPv6 address represents the network device or host on the IPv6 subnet. This is represented by the low-order 64 bits of the IPv6 address.

Aggregate Global Unicast addresses for IPv6 are assigned by the Internet Assigned Numbers Authority (IANA) and fall within the IPv6 prefix 2000::/3. This allows for a range of Aggregate Global Unicast addresses from 2000 to 3FFF, as illustrated in Table 7.4 below:

Table 7.4 – IPv6 Aggregate Global Unicast Addresses

Description	Address
First Address in Range	2000:0000:0000:0000:0000:0000:0000:0000
Last Address in Range	3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Binary Notation	The three high-order bits are set to 001

https://t.me/learningnets

From the 2000::/3 IPv6 block, only three subnets have been allocated for use at the time this module was written. These allocations are illustrated in Table 7.5 below:

Table 7.5 – Assigned IPv6 Aggregate Global Unicast Addresses

IPv6 Global Prefix	Binary Representation	Description
2001::/16	0010 0000 0000 0001	Global IPv6 Internet (Unicast)
2002::/16	0010 0000 0000 0010	6to4 Transition Prefix
3FFE::/16	0010 1111 1111 1110	6bone Prefix

NOTE: The 6to4 transition addresses and the 6bone prefix are described later in this guide.

Within the range of IPv6 Global Aggregate Unicast addresses, a special experimental range is reserved called ORCHID (an acronym for Overlay Routable Cryptographic Hash Identifiers defined in RFC 4843). ORCHID addresses are non-routed IPv6 addresses used for cryptographic hash identifiers. These addresses use the IPv6 prefix 2001:10::/28. Going into detail on ORCHID addresses is beyond the scope of the current CCNA exam requirements and will not be included in this module or in the remainder of this guide.

Multicast Addresses

The Multicast addresses used in IPv6 are derived from the FF00::/8 IPv6 prefix. In IPv6, Multicast operates in a different manner than that of Multicast in IPv4. IP Multicast is used extensively in IPv6 and replaces IPv4 protocols, such as the Address Resolution Protocol (ARP). In addition, Multicast is used in IPv6 for prefix advertisements and renumbering, as well as for Duplicate Address Detection (DAD). These concepts are all described later in this module.

Multicast packets in IPv6 do not use the TTL value to restrict such packets to the local network segment. Instead, the scoping is defined within the Multicast address itself via the use of the Scope field. IPv6 nodes on a network segment listen to Multicast and may even send Multicast packets to exchange information. This allows all nodes on an IPv6 segment to know about all the other neighbours on that same segment. The format for Multicast addresses used in IPv6 networks is illustrated in Figure 7.8 below:

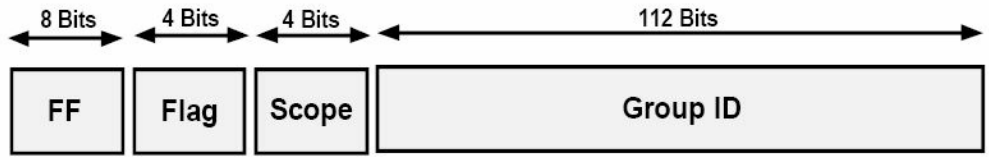


Figure 7.8 – IPv6 Multicast Addressing

As illustrated in Figure 7.8, the format of the IPv6 Multicast address is slightly different from the formats of the other IPv6 addresses you have learned about up until this point. The first 8 bits of the IPv6 Multicast address represent the Multicast prefix FF::/8. The Flag field in the IPv6 Multicast address is used to indicate the type of Multicast address, either permanent or

temporary.

Permanent IPv6 Multicast addresses are assigned by IANA, while temporary IPv6 Multicast addresses can be used in pre-deployment Multicast testing. The Flag field may contain one of the two possible values illustrated in Table 7.6 below:

Table 7.6 – IPv6 Permanent and Temporary Multicast Addresses

Type of Multicast Address	Binary Representation	Hexadecimal Value
Permanent	0000	0
Temporary	0001	1

The next 4 bits in the Multicast address represent the scope. In IPv6 Multicasting, this field is a mandatory field that restricts Multicast packets from being sent to other areas in the network. This field essentially provides the same function as the TTL field that is used in IPv4. However, with IPv6, there are several types of scopes, which are listed in Table 7.7 below:

Table 7.7 – IPv6 Multicast Address Scopes

Scope Type	Binary Representation	Hexadecimal Value
Interface-Local	0001	1
Link-Local	0010	2
Subnet-Local	0011	3
Admin-Local	0100	4
Site-Local	0101	5
Organization	1000	8
Global	1110	E

Within the IPv6 Multicast prefix, certain addresses are reserved. These reserved addresses are referred to as Multicast Assigned addresses, which are presented in Table 7.8 below:

Table 7.8 – IPv6 Reserved Multicast Addresses

Address	Scope	Description
FF01::1	Hosts	All hosts on the Interface-Local scope
FF01::2	Hosts	All routers on the Interface-Local scope
FF02::1	Link-Local	All hosts on the Link-Local scope
FF02::2	Link-Local	All routers on the Link-Local scope
FF05::2	Site	All routers on the Site scope

In addition to these addresses, a Solicited-Node Multicast address is enabled automatically for each Unicast and Anycast address configured on a router interface or network host. This address has a Link-Local scope, which means that it will never traverse farther than the local network segment. Solicited-Node Multicast addresses are used for the following two reasons:

https://t.me/learningnets

the replacement of IPv4 ARP and DAD.

Because IPv6 does not use ARP, Solicited-Node Multicast addresses are used by network hosts and routers to learn the Data Link addresses of neighbouring devices. This allows for the conversion and sending of IPv6 packets to IPv6 hosts and routers as frames. DAD is part of the IPv6 Neighbor Discovery Protocol (NDP), which will be described in detail later in this module. DAD simply allows a device to validate whether an IPv6 address is already in use on the local segment before it configures the address as its own using autoconfiguration. In essence, it provides a similar function to Gratuitous ARP used in IPv4. Solicited-Node Multicast addresses are defined by the IPv6 prefix FF02::1:FF00:0000/104. These addresses are comprised of the FF02::1:FF00:0000/104 prefix in conjunction with the low-order 24 bits of the Unicast or Anycast address. Figure 7.9 below illustrates the format of these IPv6 addresses:

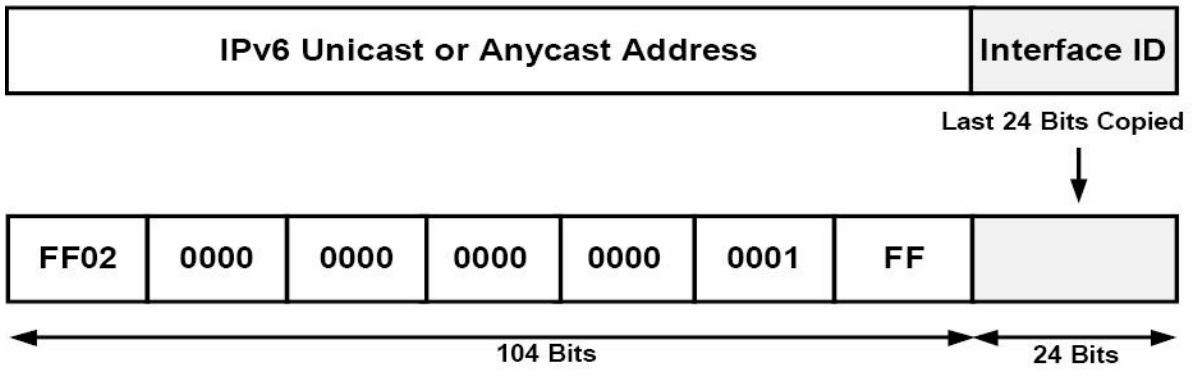


Figure 7.9 – IPv6 Solicited-Node Multicast Addresses

In a manner similar to IPv4 Multicast mapping for Ethernet, IPv6 also uses a unique means to map Layer 3 IPv6 Multicast addresses to Layer 2 Multicast addresses. Multicast mapping in IPv6 is enabled by appending the low-order 32 bits of a Multicast address to the 16-bit prefix 33:33, which is the defined Multicast Ethernet prefix for IPv6 networks. This is illustrated in Figure 7.10 below for all the routers on the Interface-Local scope prefix FF02::2:

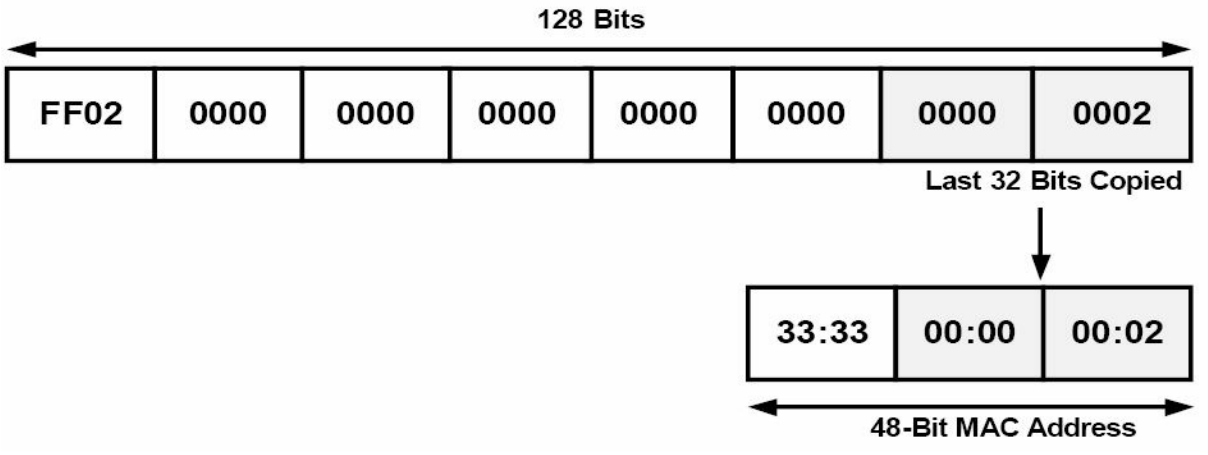


Figure 7.10 – IPv6 Multicast Addresses

Anycast Addresses

Anycast, which was introduced earlier in this section, can be described simply as one-to-nearest communication, because the nearest common address, based on routing protocol metrics, will always be preferred by the local device. In IPv6 there is no specially allocated range for Anycast,

https://t.me/learningnets

as Anycast addresses use Global Unicast, Site-Local, or even Link-Local addresses. However, there is an Anycast address reserved for special use. This special address is referred to as the Subnet-Router Anycast address and is formed with the subnet's 64-bit Unicast prefix, with the remaining 64 bits set to zero (e.g., 2001:1a2b:1111:d7e5:0000:0000:000:0000). Anycast addresses must not be used as the source address of an IPv6 packet. These addresses are typically used by protocols such as Mobile IPv6, which is outside the scope of the CCNA.

Loopback Addresses

Loopback addresses in IPv6 are used in the same manner as in IPv4. Each device has one IPv6 Loopback address, which is comparable to the 127.0.0.1 Loopback address used in IPv4, and this address is used by the device itself. IPv6 Loopback addresses use the prefix ::1, which can be represented as 0000:0000:0000:0000:0000:0000:0000:0001 in the preferred address format. This means that in Loopback addresses, all bits are set to 0, except for the last bit, which is always set to 1. These addresses are always assigned automatically when IPv6 is enabled on a device and they can never be changed.

Unspecified Addresses

In IPv6 addressing, unspecified addresses are simply Unicast addresses that are not assigned to any interface. These addresses indicate the absence of an IPv6 address and are used for special purposes that include IPv6 DHCP and DAD. Unspecified addresses are represented by all 0 values in the IPv6 address and can be written using the :: prefix. In the preferred format, these addresses are represented as 0000:0000:0000:0000:0000:0000:0000:0000.

IPv6 Protocols and Mechanisms

While version 6 of the Internet Protocol is similar to version 4, there are significant differences in the operation of the former compared to the latter. The following IPv6 protocols and mechanisms are described in this section:

- ICMP for IPv6
- The IPv6 Neighbor Discovery Protocol (NDP)
- IPv6 stateful autoconfiguration
- IPv6 stateless autoconfiguration

ICMP for IPv6

ICMP is used to report errors and other information to the source hosts regarding the delivery of IP packets to the intended destination. ICMPv6, which is defined in RFC 2463 as protocol number 58, supports messages for ICMPv4 and includes additional messages for ICMPv6. ICMPv6 is used in the Next Header field of the basic IPv6 packet header. Unlike in IPv4, IPv6 views ICMPv6 as an upper-layer protocol, such as TCP, for example, which means that ICMPv6 is placed after all possible extension headers in the IPv6 packet. The fields that are contained within the ICMPv6 packet are illustrated in Figure 7.11 below:

https://t.me/learningnets

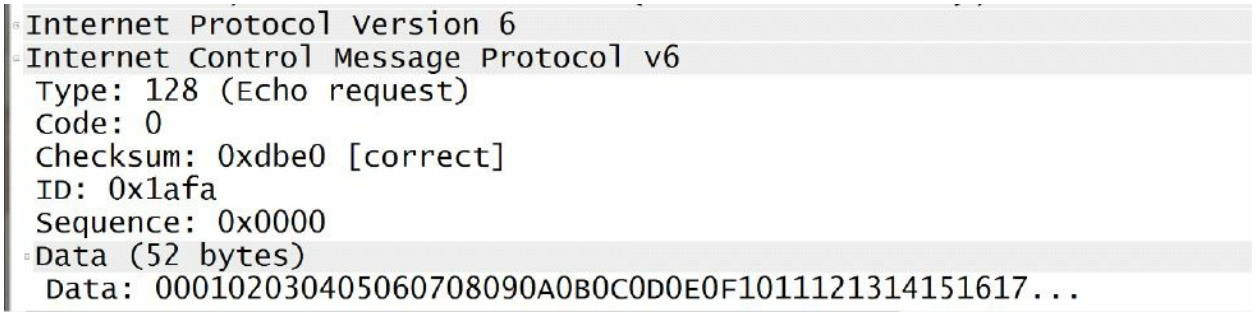


Figure 7.11 – The ICMPv6 Packet Header

Within the ICMPv6 packet header, the 8-bit Type field is used to indicate or identify the type of ICMPv6 message. This field is used to provide both error and informational messages. Table 7.9 below lists and describes some common values that can be found within this field:

Table 7.9 – ICMPv6 Message Types

ICMPv6 Type	Description
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
128	Echo Request
129	Echo Reply

NOTE: These same message types are also used in ICMPv4.

Following the Type field, the 8-bit Code field provides details pertaining to the type of message sent. Table 7.10 below illustrates common values for this field, which are also shared by ICMPv4:

Table 7.10 – ICMPv6 Codes

ICMPv6 Code	Description
0	Echo Reply
3	Destination Unreachable
8	Echo
11	Time Exceeded

Following the Code field, the 16-bit Checksum field contains a computed value used to detect data corruption in ICMPv6. Finally, the Message or Data field is an optional, variable-length field that contains the data specific to the message type indicated by the Type and Code fields. When used, this field provides information to the destination host. ICMPv6 is a core component of IPv6. Within IPv6, ICMPv6 is used for the following:

- Duplicate Address Detection (DAD)
- The replacement of ARP

https://t.me/learningnets

- ☐ IPv6 stateless autoconfiguration
- ☐ IPv6 prefix renumbering
- ☐ Path MTU Discovery (PMTUD)

NOTE: Of the options above, DAD and stateless autoconfiguration will be described later in this section. PMTUD is beyond the scope of the current CCNA exam requirements and will not be described in any additional detail in this module or in the remainder of this guide.

The IPv6 Neighbor Discovery Protocol (NDP)

The IPv6 NDP enables the plug-and-play features of IPv6. It is defined in RFC 2461 and is an integral part of IPv6. NDP operates in the Link Layer and is responsible for the discovery of other nodes on the link, determining the Link Layer addresses of other nodes, finding available routers, and maintaining reachability information about the paths to other active neighbour nodes. NDP performs functions for IPv6 similar to the way ARP (which it replaces) and ICMP Router Discovery and Router Redirect Protocols do for IPv4. However, it is important to remember that NDP provides greater functionality than the mechanisms used in IPv4. Used in conjunction with ICMPv6, NDP allows for the following:

- ☐ Dynamic neighbour and router discovery
- ☐ The replacement of ARP
- ☐ IPv6 stateless autoconfiguration
- ☐ Router redirection
- ☐ Host parameter discovery
- ☐ IPv6 address resolution
- ☐ Next-hop router determination
- ☐ Neighbor Unreachability Detection (NUD)
- ☐ Duplicate Address Detection (DAD)

NOTE: You are not required to delve into specifics on each of the advantages listed above.

Neighbor Discovery Protocol defines five types of ICMPv6 packets, which are listed and described in Table 7.11 below:

Table 7.11 – ICMPv6 NDP Message Types

ICMPv6 Type	Message Type Description and IPv6 Usage
133	Used for Router Solicitation (RS) messages
134	Used for Router Advertisement (RA) messages
135	Used for Neighbor Solicitation (NS) messages
136	Used for Neighbor Advertisement (NA) messages
137	Used for Router Redirect messages

https://t.me/learningnets

Router Solicitation messages are sent by hosts when interfaces are enabled for IPv6. These messages are used to request that routers on the local segment generate RA messages immediately, rather than at the next scheduled RA interval. Figure 7.12 below illustrates a wire capture of an RS message:

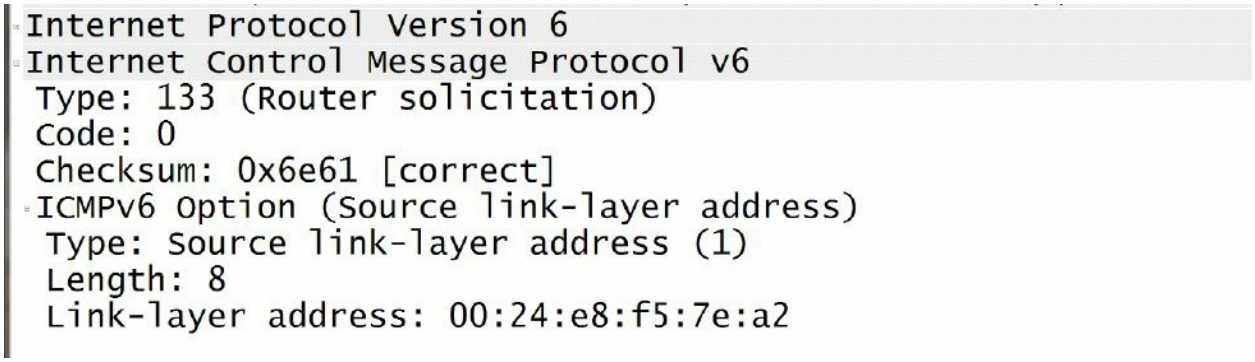


Figure 7.12 – IPv6 Router Solicitation Message

Upon receiving the RS message, routers advertise their presence using RA messages, which typically include prefix information for the local link as well as any additional configuration, such as suggested hop limits. The information contained within the RA is illustrated in Figure 7.13 below:

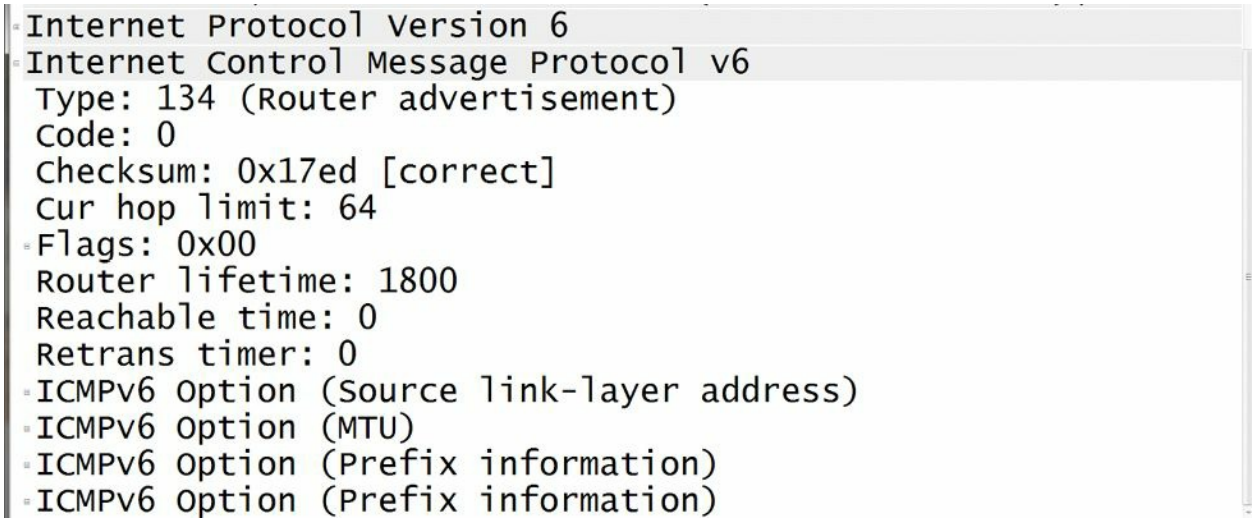


Figure 7.13 – IPv6 Router Advertisement Message

To reiterate, RS and RA messages are for router-to-host or host-to-router exchanges, as illustrated below:

https://t.me/learningnets

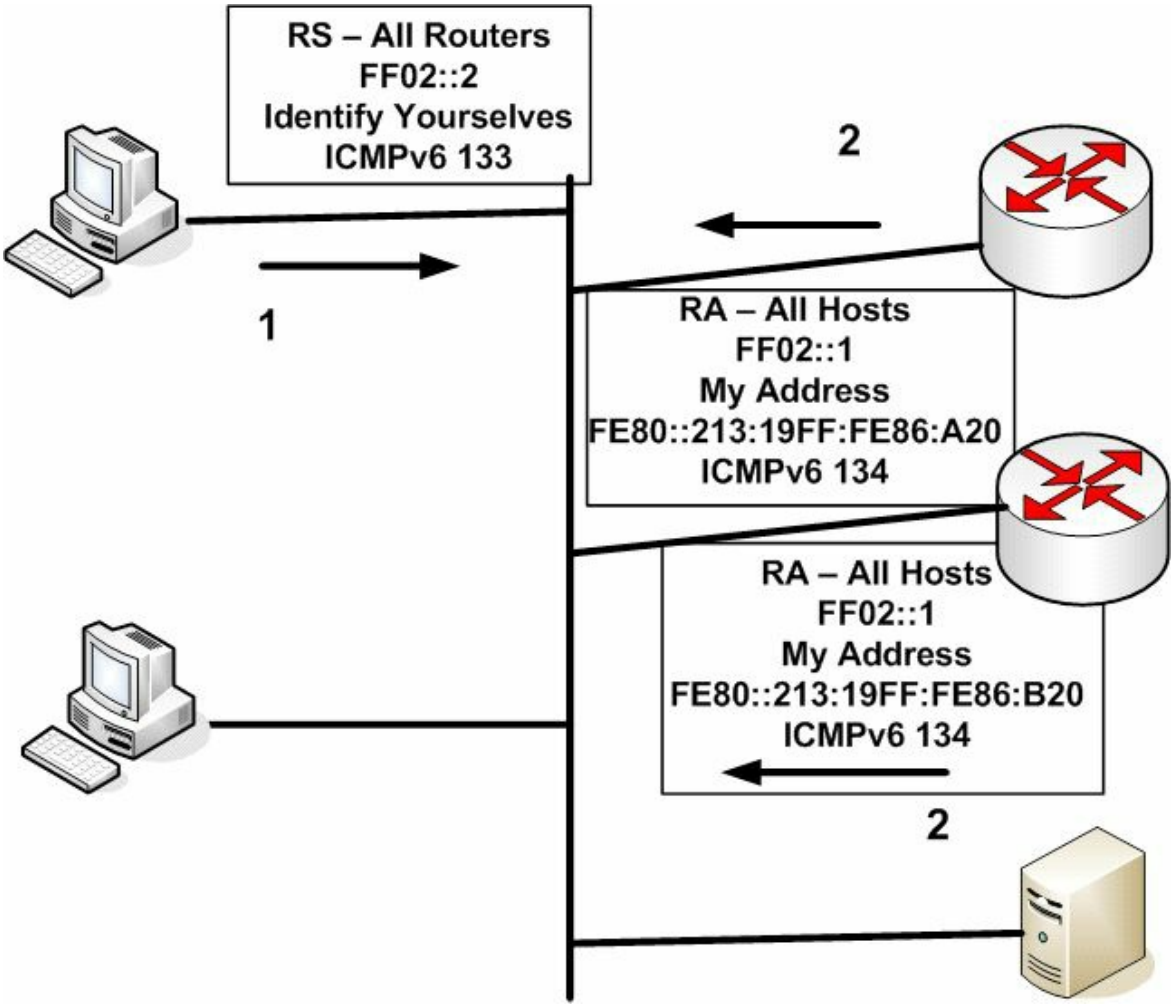


Figure 7.14 – IPv6 RS and RA Messages

IPv6 NS messages are Multicast by IPv6 routers on the local network segment and are used to determine the Data Link address of a neighbour or to verify that a neighbour is still reachable (thus replacing the ARP function). These messages are also used for Duplicate Address Detection. While delving into detail on NS messages is beyond the scope of the CCNA exam requirements, Figure 7.15 below illustrates a wire capture of an IPv6 Neighbor Solicitation message:

```
Internet Control Message Protocol v6
 Type: 135 (Neighbor solicitation)
 Code: 0
 Checksum: 0x3f71 [correct]
 Target: fe80::213:19ff:fe86:a20
 ICMPv6 Option (Source link-layer address)
  Type: Source link-layer address (1)
  Length: 8
  Link-layer address: 00:24:e8:f5:7e:a2
```

Figure 7.15 – IPv6 Neighbor Solicitation Message

Neighbor Advertisement messages are typically sent by routers on the local network segment in response to received NS messages. However, if, for example, an IPv6 prefix changes, then routers may also send out unsolicited NS messages advising other devices on the local network segment of the change. As is the case with NA messages, going into detail on the format or fields contained within the NA message is beyond the scope of the CCNA exam requirements. Figures 7.16 and 7.17 below illustrate a wire capture of the Neighbor Advertisement message,

https://t.me/learningnets

which is also sent via IPv6 Multicast:

```
Internet Control Message Protocol v6
 Type: 136 (Neighbor advertisement)
 Code: 0
 Checksum: 0x909f [correct]
 Flags: 0xa0000000
  1... .... .... .... .... .... .... .... = Router
  .0.. .... .... .... .... .... .... .... = Not adverted
  ..1. .... .... .... .... .... .... .... = Override
 Target: fe80::20c:ceff:fea7:f3a0
 ICMPv6 Option (Target link-layer address)
  Type: Target link-layer address (2)
  Length: 8
  Link-layer address: 00:0c:ce:a7:f3:a0
```

Figure 7.16 – IPv6 Neighbor Advertisement Message

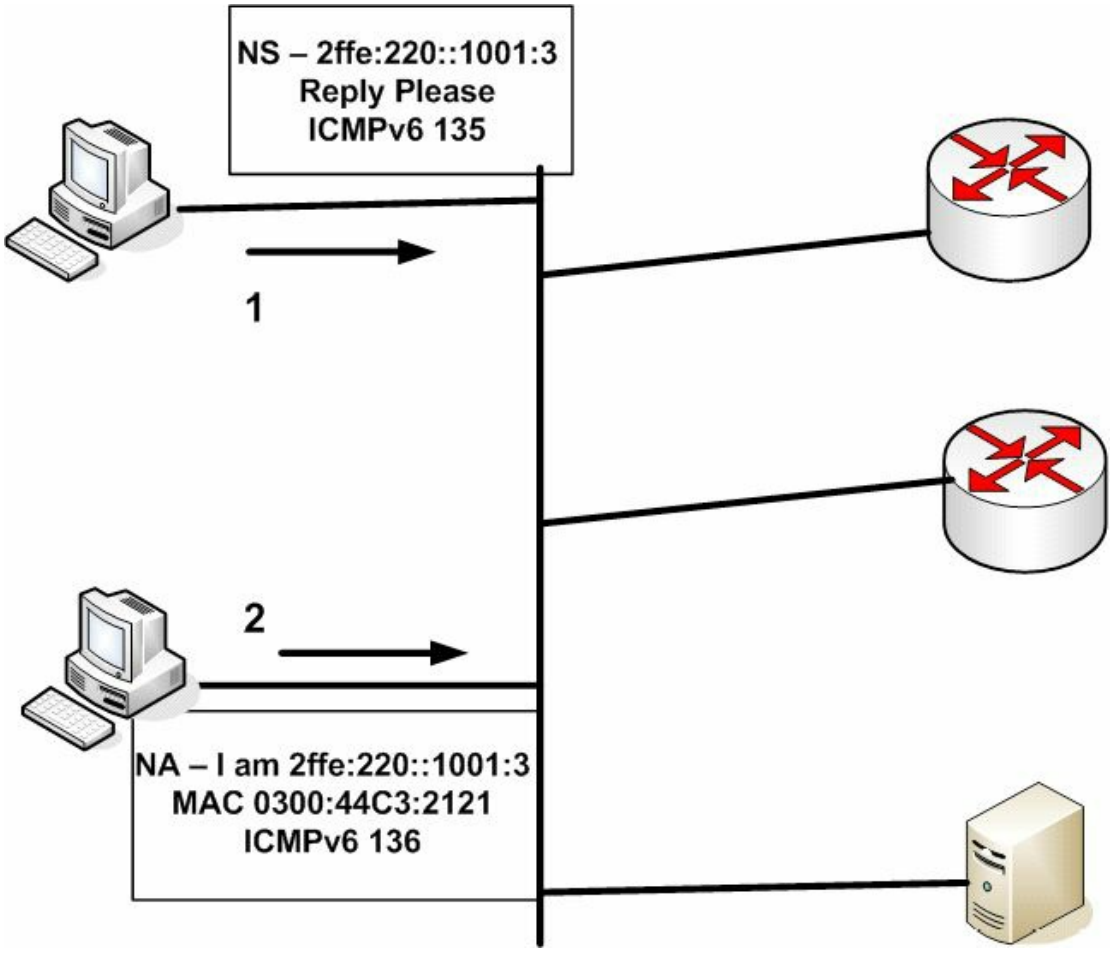


Figure 7.17 – IPv6 Neighbor Advertisement Messages

Finally, router redirection uses ICMPv6 Redirect messages, which are defined as message type 137. Router redirection is used to inform network hosts that a router with a better path to the intended destination exists on the network. It works in the same manner as it does for ICMPv4, which redirects traffic in current IPv4 networks.

IPv6 Stateful Autoconfiguration

As previously stated in this module, stateful autoconfiguration allows network hosts to receive their addressing information from a network server (e.g., via DHCP). This method of autoconfiguration is supported by both IPv4 and IPv6. In IPv6 networks, DHCPv6 is used to provide stateful (and stateless) autoconfiguration services for IPv6 hosts. In IPv6

https://t.me/learningnets

implementations, when an IPv6 host receives RA messages from routers on the local network segment, the host examines these packets to determine whether DHCPv6 can be used. The RA messages provide this information by setting either the M (Managed) or the O (Other) bits to 1.

With DHCP the client is configured to obtain information from the DHCP server. With DHCPv6, the client doesn't know where the information comes from, which could be from SLAAC, stateful DHCPv6, or a combination of both.

The M bit in Router Advertisement messages is the Managed Address Configuration Flag bit. When this bit is set (i.e., it contains a value of 1), it instructs the IPv6 host to obtain a stateful address, which is provided by DHCPv6 servers. The O bit in Router Advertisement messages is the Other Stateful Configuration Flag bit. When this bit is set (i.e., it contains a value of 1), it instructs the IPv6 host to use DHCPv6 to obtain more configuration settings, such as DNS and WINS servers, for example.

If a host has not been configured with an IPv6 address, it can use one of three methods to obtain one, as well as other network settings such as the DNS server address:

- SLACC – Stateless Autoconfiguration M and O bits set to 0 means that there is no DHCPv6 information. The host receives all necessary information from an RA.
- Stateful DHCPv6 – M flag set to 1 tells the host to use DHCPv6 for all address and network information.
- Stateless DHCPv6 – M flag set to 0 and O flag set to 1 means that the host will use SLACC for the address (from an RA) but will also obtain other information from DNS servers.

While one of the advantages of IPv6 is stateless autoconfiguration capability, stateful autoconfiguration still provides several advantages, which include the following:

- Greater controls than those provided by stateless autoconfiguration
- Can be used on networks when stateless autoconfiguration is available
- Provides addressing to network hosts in the absence of routers
- Can be used for network renumbering by assigning new prefixes to hosts
- Can be used to issue entire subnets to customer premise equipment

IPv6 Stateless Autoconfiguration

IPv6 permits interfaces to self-configure an IP address in order for host-to-host communication to take place. Stateful autoconfiguration involves a server allocating address information, and for IPv6 DHCPv6 is used. Stateful refers to the fact that details of an exchange are stored by the server (or router), whereas stateless means they are not. DHCPv6 can either be stateful or stateless.

In IPv6, stateless autoconfiguration allows hosts to configure their Unicast IPv6 addresses by themselves based on prefix advertisements from routers on the local network segment. Other network information can be obtained from the DHCPv6 server (such as the DNS server address). The three mechanisms that allow for stateless autoconfiguration in IPv6 are as follows:

https://t.me/learningnets

- Prefix advertisement
- Duplicate Address Detection (DAD)
- Prefix renumbering

IPv6 prefix advertisement uses ICMPv6 Router Advertisement messages, which are sent to the all-hosts-on-the-local-link IPv6 Multicast address FF02::1. By design, only routers are allowed to advertise prefixes on the local link. When stateless autoconfiguration is employed, it is imperative to remember that the prefix length used must be 64 bits (e.g., 2001:1a2b::/64).

Following the configuration of the prefix, RA messages used for IPv6 stateless autoconfiguration include the following information:

- The IPv6 prefix
- The lifetime
- Default router information
- Flags and/or Options fields

As previously stated, the IPv6 prefix must be 64 bits. In addition, multiple IPv6 prefixes may be advertised on the local segment. When hosts on the network segment receive the IPv6 prefix, they append their MAC address to the prefix in EUI-64 format, which was described earlier in this module, and automatically configure their IPv6 Unicast address. This provides a unique 128-bit IPv6 address to each host on the network segment.

The lifetime value for each advertised prefix is also provided to the nodes and may contain a value from 0 to infinite. When nodes receive the prefix, they validate the lifetime value and cease using the prefix when the lifetime value reaches 0. Alternatively, if a value of infinite is received for a particular prefix, the network hosts will never cease using that prefix. Each advertised prefix contains two lifetime values: the valid lifetime value and the preferred lifetime value.

The valid lifetime value is used to determine how long the host address will remain valid. When this value expires (i.e., reaches a value of 0), the host address becomes invalid. The preferred lifetime value is used to determine how long an address configured via stateless autoconfiguration will remain valid. This value must be less than or equal to the value specified in the valid lifetime and is typically used for prefix renumbering.

The default router provides information about the existence and lifetime of its IPv6 address. By default, the address used for default routers is the Link-Local address (FE80::/10). This allows the Global Unicast address to be changed without interrupting network services, as would be the case in IPv4 if a network were renumbered.

Finally, the Flags and Options fields can be used to instruct network hosts to use stateless autoconfiguration or stateful autoconfiguration. These fields are included in the wire capture of the Router Advertisement shown in Figure 7.13.

Duplicate Address Detection is an NDP mechanism used in stateless autoconfiguration when a

https://t.me/learningnets

host on the network segment is booting up. DAD mandates that before a network host permanently configures its own IPv6 address during boot up, it should validate that another network host is not already using the IPv6 address it wants to use.

Duplicate Address Detection performs this validation by using Neighbor Solicitation (ICMPv6 Type 135) and Solicited-Node Multicast addresses. The host sends a Neighbor Solicitation on the local network segment using an unspecified IPv6 address (i.e., the :: address) as its source address and the Solicited-Node Multicast address of the IPv6 Unicast address it wants to use as the destination address. If no other host is using this same address, the host will not automatically configure itself with this address; however, if no other device is using the same address, the host automatically configures itself and begins to use this IPv6 address.

Finally, prefix renumbering allows for the transparent renumbering of network prefixes in IPv6 when changing from one prefix to another. Unlike in IPv4, where the same global IP address can be advertised by multiple providers, the strict aggregation of the IPv6 address space prevents providers from advertising prefixes that do not belong to their organisation.

In cases where a transition is made from one IPv6 Internet provider to another, the IPv6 prefix renumbering mechanism provides a smooth and transparent transition from one prefix to another. Prefix renumbering uses the same ICMPv6 messages and Multicast address used in prefix advertisement. Prefix renumbering is made possible by using the time parameters contained within the Router Advertisement messages.

In Cisco IOS software, routers can be configured to advertise current prefixes with the valid and preferred lifetime values decreased to a value closer to zero, which allows those prefixes to become invalid faster. The routers are then configured to advertise the new prefixes on the local network segments. This allows the old and new prefixes to exist on the same network segment.

During this transition period, hosts on the local network segment use two Unicast addresses: one from the old prefix and one from the new prefix. Any current connections using the old prefix are still handled; however, any new connections from these hosts are made using the new prefix. When the old prefix expires, only the new prefix is used.

Configuring Stateless DHCPv6

There are a few simple steps to follow in order to configure stateless DHCPv6 on a router:

- Create the pool name and other parameters
- Enable it on an interface
- Modify Router Advertisement settings

An Identity Association (IA) is a collection of addresses assigned to the client. There must be at least one IA assigned per interface using DHCPv6. We won't go into configuration examples for the CCNA exam.

Enabling IPv6 Routing in Cisco IOS Software

Now that you have a solid understanding of IPv6 fundamentals, the remainder of this module

will focus on the configuration of IPv6 in Cisco IOS software. By default, IPv6 routing functionality is disabled in Cisco IOS software. Therefore, IPv6 routing functionality must be enabled manually using the `ipv6 unicast-routing` global configuration command.

After enabling IPv6 routing globally, the `ipv6 address [ipv6-address/prefix-length | prefix-name sub-bits/prefix-length | anycast | autoconfig <default> | dhcp | eui-64 | link-local]` interface configuration command can be used to configure interface IPv6 addressing. The `[ipv6-address/prefix-length]` keyword is used to specify the IPv6 prefix and prefix length assigned to the interface. The following configuration illustrates how to configure a router interface with the first address on the 3FFF:1234:ABCD:5678::/64 subnet:

```
R1(config)#ipv6 unicast-routing
R1(config)#interface FastEthernet0/0
R1(config-if)#ipv6 address 3FFF:1234:ABCD:5678::/64
R1(config-if)#exit
```

Following this configuration, the `show ipv6 interface [name]` command can be used to validate the configured IPv6 address subnet, as illustrated below:

```
R1#show ipv6 interface FastEthernet0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20C:CEFF:FEA7:F3A0
  Global unicast address(es):
    3FFF:1234:ABCD:5678::1, subnet is 3FFF:1234:ABCD:5678::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FFA7:F3A0
...
[Truncated Output]
```

As was stated earlier in this module, IPv6 allows multiple prefixes to be configured on the same interface. If multiple prefixes have been configured on the same interface, the `show ipv6 interface [name] prefix` command can be used to view all assigned prefixes as well as their valid and preferred lifetime values. The following output displays the information that is printed by this command for a router interface with multiple IPv6 subnets configured:

```
R1#show ipv6 interface FastEthernet0/0 prefix
IPv6 Prefix Advertisements FastEthernet0/0
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default
       N - Not advertised, C - Calendar
     default [LA] Valid lifetime 2592000, preferred lifetime 604800
AD   3FFF:1234:ABCD:3456::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
AD   3FFF:1234:ABCD:5678::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

https://t.me/learningnets

```
AD   3FFF:1234:ABCD:7890::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
AD   3FFF:1234:ABCD:9012::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

NOTE: As was stated earlier, the valid and preferred lifetime values can be adjusted from default values, allowing for a smooth transition when implementing prefix renumbering. This configuration, however, is beyond the scope of the CCNA exam requirements and will not be illustrated in this lesson.

Continuing with the use of the `ipv6 prefix` interface configuration command, the `[prefix-name sub-bits/prefix-length]` keyword is used to configure a general prefix, which specifies the leading bits of the subnet to be configured on the interface. This configuration is beyond the scope of the current CCNA exam requirements and will not be illustrated in this module.

The `[anycast]` keyword is used to configure an IPv6 Anycast address. As was stated earlier, Anycast addressing simply allows the same common address to be assigned to multiple router interfaces. Hosts use the Anycast address that is closest to them based on routing protocol metrics. Anycast configuration is beyond the scope of the CCNA exam requirements and will not be illustrated in this module.

The `[autoconfig <default>]` keyword enables stateless autoconfiguration (SLAAC). If this keyword is used, the router will dynamically learn prefixes on the link and then add EUI-64 addresses for all the learned prefixes. The `<default>` keyword is an optional keyword that allows a default route to be installed. The following configuration example illustrates how to enable stateless autoconfiguration on a router interface and additionally allow the default route to be installed.

```
R2(config)#ipv6 unicast-routing
R2(config)#interface FastEthernet0/0
R2(config-if)#ipv6 address autoconfig default
R2(config-if)#exit
```

Following this configuration, router R2 will listen to Router Advertisement messages on the local segment on which the FastEthernet0/0 interface resides. The router will configure dynamically an EUI-64 address for each learned prefix and then install the default route pointing to the Link-Local address of the advertising router. The dynamic address configuration is validated using the `show ipv6 interface [name]` command, as illustrated below:

```
R2#show ipv6 interface FastEthernet0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::213:19FF:FE86:A20
  Global unicast address(es):
    3FFF:1234:ABCD:3456:213:19FF:FE86:A20, subnet is 3FFF:1234:ABCD:3456::/64 [PRE]
      valid lifetime 2591967 preferred lifetime 604767
    3FFF:1234:ABCD:5678:213:19FF:FE86:A20, subnet is 3FFF:1234:ABCD:5678::/64 [PRE]
      valid lifetime 2591967 preferred lifetime 604767
    3FFF:1234:ABCD:7890:213:19FF:FE86:A20, subnet is 3FFF:1234:ABCD:7890::/64 [PRE]
      valid lifetime 2591967 preferred lifetime 604767
    3FFF:1234:ABCD:9012:213:19FF:FE86:A20, subnet is 3FFF:1234:ABCD:9012::/64 [PRE]
```

https://t.me/learningnets

```
      valid lifetime 2591967 preferred lifetime 604767
    FEC0:1111:1111:E000:213:19FF:FE86:A20, subnet is FEC0:1111:1111:E000::/64 [PRE]
      valid lifetime 2591967 preferred lifetime 604767
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF86:A20
  MTU is 1500 bytes
...
[Truncated Output]
```

In the output above, notice that while no explicit IPv6 addresses were configured on the interface, an EUI-64 address was configured dynamically for the subnet the router discovered by listening to Router Advertisement messages. The timers for each of these prefixes are derived from the router advertising the RA messages. In addition to verifying the stateless autoconfiguration, the `show ipv6 route` command can be used to validate the default route to the Link-Local address of the preferred advertising router, as illustrated below:

```
R2#show ipv6 route ::/0
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS inter area, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via FE80::20C:CEFF:FEA7:F3A0, FastEthernet0/0
```

Continuing with the `ipv6 address` command, the `[dhcp]` keyword is used to configure the router interface to use stateful autoconfiguration (i.e., DHCPv6) to acquire the interface addressing configuration. With this configuration, an additional keyword, `[rapid-commit]`, can also be appended to the end of this command to allow the two-message exchange method for address assignment and other configuration information.

Reverting back to the topic of discussion, with the `ipv6 address` command, the `[eui-64]` keyword is used to configure an IPv6 address for an interface and enables IPv6 processing on the interface using an EUI-64 interface ID in the low-order 64 bits of the address. By default, Link-Local, Site-Local, and IPv6 stateless autoconfiguration all use the EUI-64 format to make their IPv6 addresses. EUI-64 addressing expands the 48-bit MAC address into a 64-bit address. This is performed in two steps, both of which are described in the following section. This process is referred to as stateless autoconfiguration, or SLAAC.

In the first step of creating the EUI-64 address, the value FFEE is inserted into the middle of the MAC address, thereby expanding the MAC address from 48 bits, which is 12 hexadecimal characters, to 64 bits, which is 16 hexadecimal characters. The conversion of the 48-bit MAC

https://t.me/learningnets

address into the 64-bit EUI address is illustrated in Figure 7.18 below:

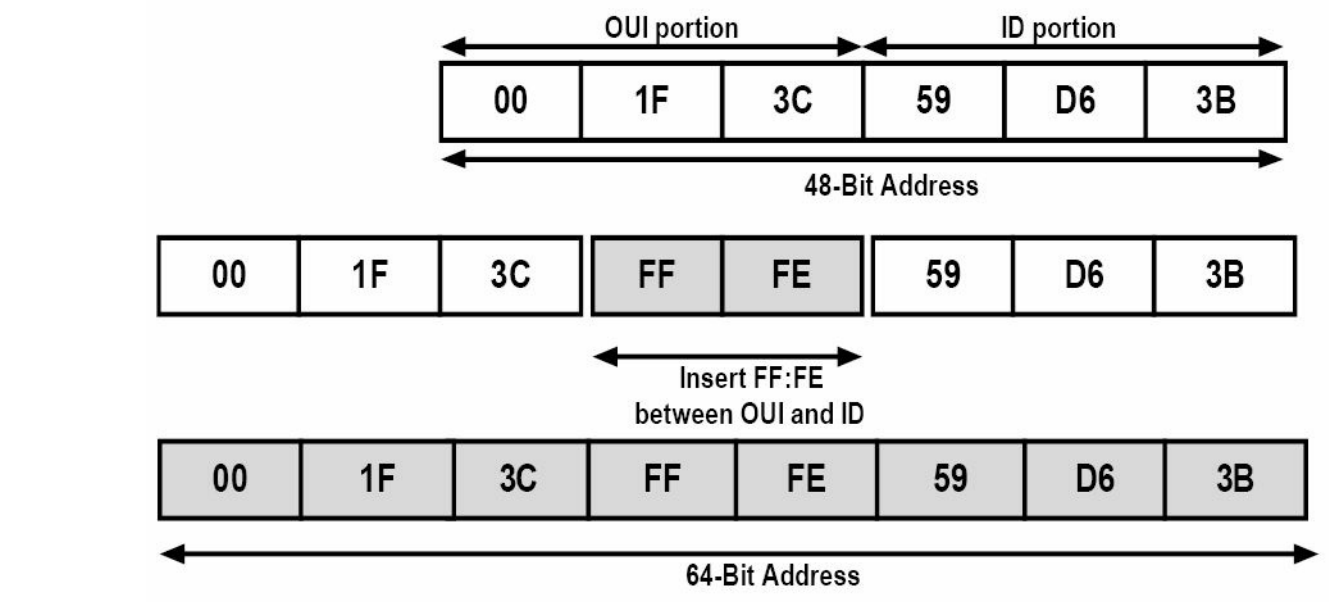


Figure 7.18 – Creating the EUI-64 Address

The second step of EUI-64 addressing entails the setting of the seventh bit of the 64-bit address. This seventh bit is used to identify whether the MAC address is unique. If this bit is set to 1, this indicates that the MAC address is a globally managed MAC address – which means that the MAC address has been assigned by a vendor. If this bit is set to 0, this indicates that the MAC address is locally assigned – which means that the MAC address has been added by the administrator, for example. To clarify this statement further, as an example, MAC address 02:1F:3C:59:D6:3B would be considered a globally-assigned MAC address, while MAC address 00:1F:3C:59:D6:3B would be considered a local address. This is illustrated in Figure 7.19 below:

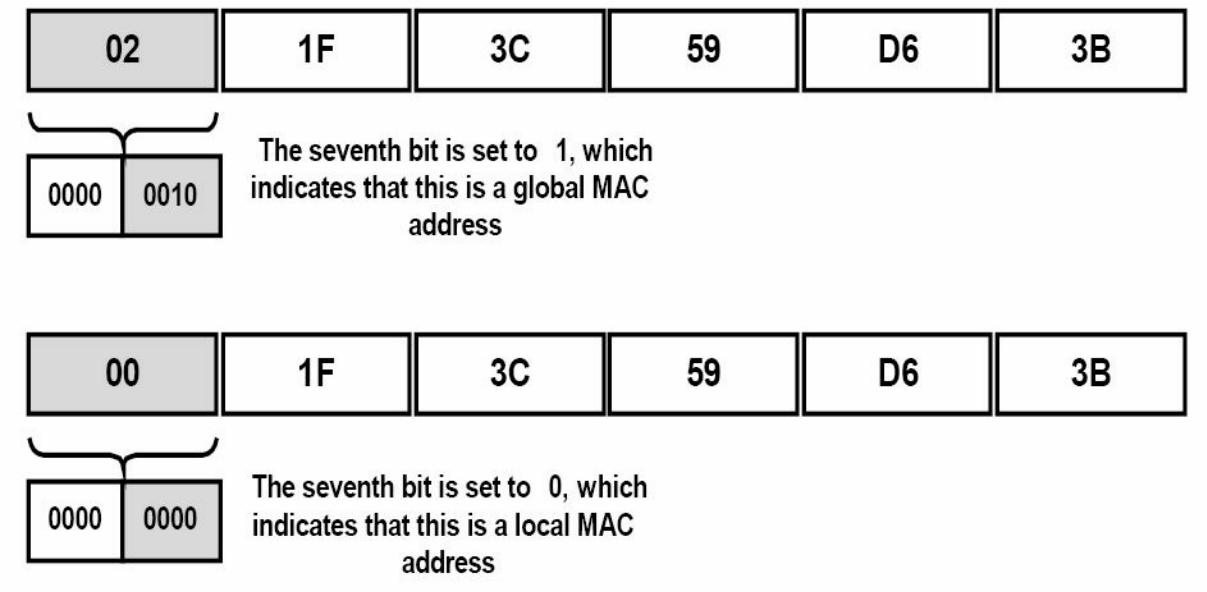


Figure 7.19 – Determining Local and Global MAC Addresses

The following configuration example illustrates how to assign an IPv6 prefix to an interface and configure the router to create the interface ID automatically using EUI-64 addressing:

```
R2(config)#interface FastEthernet0/0
R2(config-if)#ipv6 address 3fff:1a2b:3c4d:5e6f::/64 eui-64
```

https://t.me/learningnets

```
R2(config-if)#exit
```

Following this configuration, the `show ipv6 interface` command can be used to validate the IPv6 interface ID assigned to the FastEthernet0/0 interface, as illustrated below:

```
R2#show ipv6 interface FastEthernet0/0
FastEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::213:19FF:FE86:A20
  Global unicast address(es):
    3FFF:1A2B:3C4D:5E6F:213:19FF:FE86:A20, subnet is 3FFF:1A2B:3C4D:5E6F::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF86:A20
  MTU is 1500 bytes
...
[Truncated Output]
```

To validate the creation of the EUI-64 address, you can verify the complete IPv6 address by also viewing the MAC address for the specified interface using the `show interface` command:

```
R2#show interface FastEthernet0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0013.1986.0a20 (bia 0013.1986.0a20)
   Internet address is 10.0.1.1/30
```

From the output above, you can see that the EUI-64 address is indeed valid and is based on the MAC address of the interface. In addition, the address is global, as the seventh bit has been enabled (i.e., contains a non-zero value).

Finally, the `[link-local]` keyword is used to assign a Link-Local address to the interface. By default, it is important to remember that an IPv6 prefix does not have to be enabled on the interface in order for a Link-Local address to be created dynamically. Instead, if the `ipv6 enable` interface configuration command is issued under an interface, a Link-Local address is created automatically for that interface using EUI-64 addressing.

To configure a Link-Local address manually, you must assign an address within the FE80::/10 Link-Local address block. The following configuration example illustrates how to configure a Link-Local address on an interface:

```
R3(config)#interface FastEthernet0/0
R3(config-if)# ipv6 address fe80:1234:abcd:1::3 link-local
R3(config-if)#exit
```

Following this configuration, the `show ipv6 interface [name]` command can be used to validate the manual configuration of the Link-Local address, as shown in the output below:

```
R3#show ipv6 interface FastEthernet0/0
FastEthernet0/0 is up, line protocol is up
```

https://t.me/learningnets

```
  IPv6 is enabled, link-local address is FE80:1234:ABCD:1::3
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF00:1111
  MTU is 1500 bytes
...
[Truncated Output]
```

NOTE: When configuring Link-Local addresses manually, if Cisco IOS software detects another host using one of its IPv6 addresses, an error message will be printed on the console and the command will be rejected. Be very careful when configuring Link-Local addressing manually.

Subnetting with IPv6

As you have already learned, IPv6 addresses are allocated to companies with a prefix. The host part of the address is always 64 bits and the standard prefix is usually 48 bits or /48. This leaves 16 bits free for network administrators to use for subnetting.

Because the same rules apply to both IPv4 and IPv6, as far as network addressing is concerned, you can have only one network per network segment. You can't break the address and use some host bits on one part of the network and some on another.

If you look at the addressing in the chart below, the situation should make more sense:

Global Routing Prefix	Subnet ID	Interface ID
48 bits or /48	16 bits (65,536 possible subnets)	64 bits

You need never concern yourself about running out of host bits per subnet because each subnet has over 18 quintillion hosts. It's unlikley that any organisation would ever run out of subnets, but even if this were the case, another global routing prefix could easily be provided by the ISP.

Let's say, for example, that you are allocated the global routing prefix 0:123:abc/48. This address is occupying three sections of a full IPv6 address and each section or quartet is 16 bits, so you have 48 bits used so far. The host portion will require 64 bits, leaving you 16 bits for allocation as subnets.

You would simply start counting up in hex from zero (zero is legal) and keep going. For your hosts you would do the same, unless you wanted to reserve the first few addresses for servers on the segment, for example.

Let me use a simpler prefix for our example – 2001:123:abc/48. The first subnet would be all zeros and, of course, the first host on each subnet would be all zeros, which is legal (since you don't reserve the all 0s and all 1s addresses in IPv6). You would represent the all zeros host by

https://t.me/learningnets

using the abbreviated format of ::. Here are the first few subnets and host addresses:

Global Prefix	Subnet	First Address
2001:123:abc	0000	::
2001:123:abc	0001	::
2001:123:abc	0002	::
2001:123:abc	0003	::
2001:123:abc	0004	::
2001:123:abc	0005	::
2001:123:abc	0006	::
2001:123:abc	0007	::
2001:123:abc	0008	::
2001:123:abc	0009	::
2001:123:abc	000A	::
2001:123:abc	000B	::
2001:123:abc	000C	::
2001:123:abc	000D	::
2001:123:abc	000E	::
2001:123:abc	000F	::
2001:123:abc	0010	::
2001:123:abc	0011	::
2001:123:abc	0012	::
2001:123:abc	0013	::
2001:123:abc	0014	::
2001:123:abc	0015	::
2001:123:abc	0016	::
2001:123:abc	0017	::

https://t.me/learningnets

You have already noticed a difference from IPv4 addressing rules, I'm sure, in that you can use

the all zeros subnet and the first subnet address is always all zeros. Looking at a simple network topology, you could allocate the subnets in the fashion below:

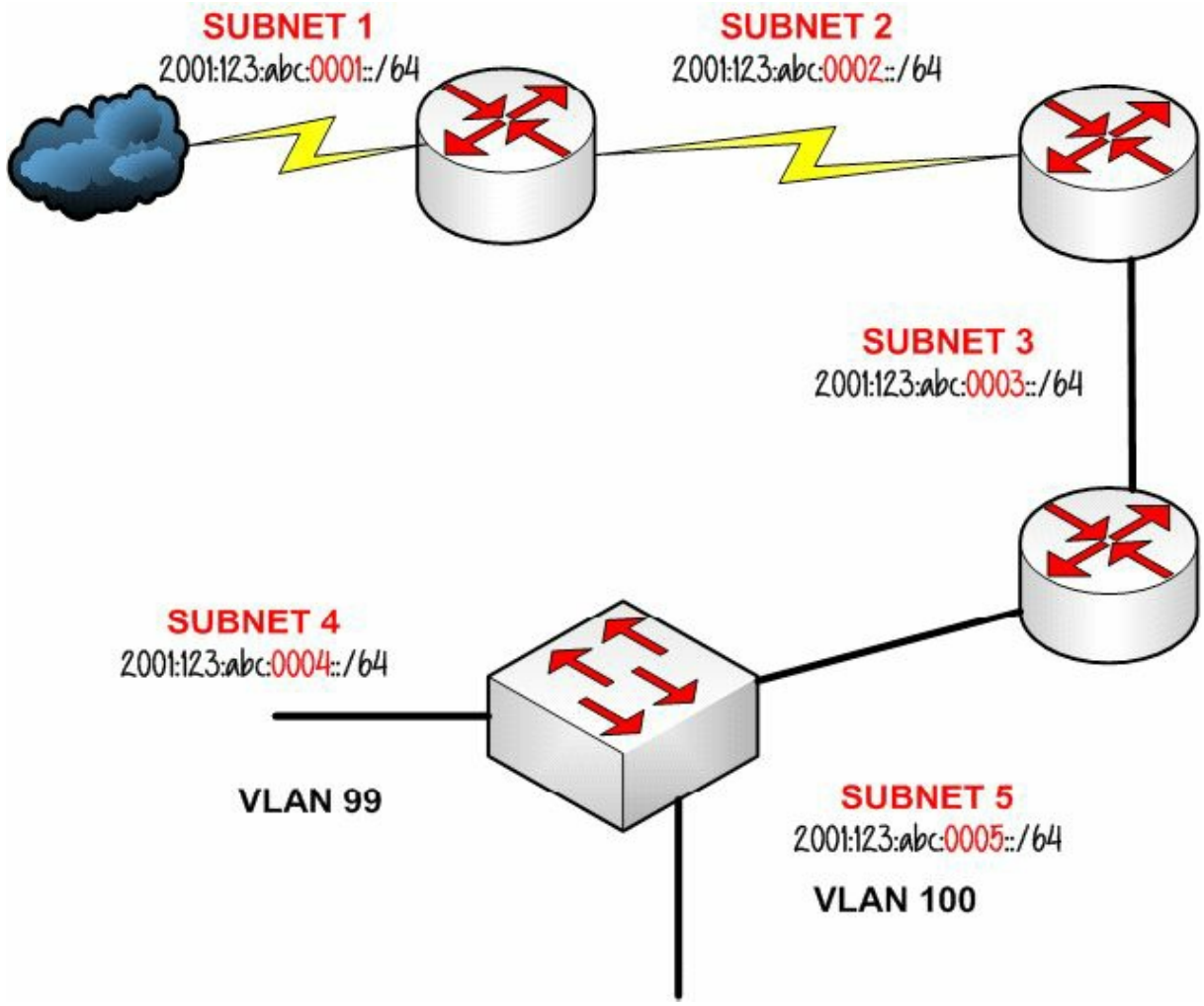


Figure 7.20 – Allocating IPv6 Subnets

Can it really be that easy? If you recall from the IPv4 subnetting section, it can become somewhat of a nightmare to figure that out, as well as having to work out how many hosts and subnets and remembering to exclude certain addresses. IPv6 subnetting is far easier. You may not be allocated a 48-bit prefix, it could be /56 for a home network or smaller, but the principle would be the same. You can also subnet off the bit boundary, but this would be most unusual and unfair of Cisco to expect you to go into that amount of detail in the short amount of time you have in the exam. Hopefully, the exam won't be a mean attempt to catch you out, but you never know. Just in case, here is an example of a /56 prefix length address:

2001:123:abc:8bbc:1221:cc32:8bcc:4231/56

The prefix is 56 bits, which translates to 14 hex digits (14 x 4 = 56), so you know that the prefix will take you to the middle of a quartet. This is where you could make a mistake in the exam. You must zero hex bits 3 and 4 in the quartet before the prefix breaks:

2001:123:abc:8b00:0000:0000:0000:0000/56

I've underlined the quartet where the bit boundary is broken. In haste and due to time pressures in the exam, you could well miss this important step. Remember that you would also abbreviate this address (the first host on the first subnet) to:

https://t.me/learningnets

2001:123:abc:8b00::/56

If they do try to catch you out in the exam, it would probably be an attempt to have you remove the trailing zeros from the quartet before the bit boundary is broken:

2001:123:abc:8b::/56

The above abbreviation is illegal.

You can steal bits from the host portion to use for subnets, but there should never be a reason to and it would break the ability to use many of the features IPv6 was invented to utilise, including stateless autoconfiguration.

IPv6 Compared to IPv4

A network engineer should have a very clear picture of the advantages IPv6 brings over IPv4. Looking at the enhancements of IPv6, we can summarise the following:

- Ipv6 has an expanded address space, from 32 bits to 128 bits.
- IPv6 uses hexadecimal notation instead of dotted-decimal notation (as in IPv4).
- IPv6 addresses are globally unique due to the extended address space, eliminating the need for NAT.
- IPv6 has a fixed header length (40 bytes), allowing vendors to improve switching efficiency.
- IPv6 supports enhanced options (that offer new features) by placing extension headers between the IPv6 header and the Transport Layer header.
- IPv6 offers address autoconfiguration, providing for dynamic assignment of IP addresses even without a DHCP server.
- IPv6 offers support for labeling traffic flows.
- IPv6 has security capabilities built in, including authentication and privacy via IPSec.
- IPv6 offers MTU path discovery before sending packets to a destination, eliminating the need for fragmentation.
- IPv6 supports site multi-homing.
- IPv6 uses the ND (Neighbor Discovery) protocol instead of ARP.
- IPv6 uses AAAA DNS records instead of A records (as in IPv4).
- IPv6 uses Site-Local addressing instead of RFC 1918 (as in IPv4).
- IPv4 and IPv6 use different routing protocols.
- IPv6 provides for Anycast addressing.

https://t.me/learningnets

Day 7 Questions

1. IPv6 addresses must always be used with a subnet mask. True or false?
2. Name the three types of IPv6 addresses.
3. Which command enables IPv6 on your router?
4. The 0002 portion of an IPv6 address can be shortened to just 2. True or false?
5. How large is the IPv6 address space?
6. With IPv6, every host in the world can have a unique address. True or false?
7. IPv6 does not have natively integrated security features. True or false?
8. IPv6 implementations allow hosts to have multiple addresses assigned. True or false?
9. How can the broadcast functionality be simulated in an IPv6 environment?
10. How many times can the double colon (::) notation appear in an IPv6 address?

https://t.me/learningnets

Day 7 Answers

1. False.
2. Unicast, Multicast, and Anycast.
3. The `ipv6 unicast-routing` command.
4. True.
5. 128 bits.
6. True.
7. False.
8. True.
9. By using Anycast.
10. One time.

https://t.me/learningnets

Day 7 Lab

IPv6 Concepts Lab

Test the IPv6 concepts and commands detailed in this module on a pair of Cisco routers that are directly connected:

- ☐ Enable IPv6 Global Unicast routing on both routers
- ☐ Manually configure an IPv6 address on each of the connected interfaces. For example:
  - 2001:100::1/64 on R1
  - 2001:100::2/64 on R2
- ☐ Verify the configuration using the `show ipv6 interface` and `show ipv6 interface prefix` commands
- ☐ Test direct ping connectivity
- ☐ Repeat the test using IPv6 stateless autoconfiguration (`ipv6 address autoconfig default`)
- ☐ Repeat the test using EUI-64 addresses (IPv6 address 2001::/64 EUI-64)
- ☐ Hard code an interface Link-Local address: IPv6 address fe80:1234:abcd:1::3 Link-Local
- ☐ Verify the IPv6 routing table

Visit www.in60days.com and watch me do this lab for free.

Hex Conversion and Subnetting Practice

Please spend the rest of this day's lesson practicing these critical topics:

- ☐ Conversion from decimal to hex (random numbers)
- ☐ Conversion from hex to decimal (random numbers)
- ☐ IPv6 subnetting (random networks and scenarios)

https://t.me/learningnets

Day 8 – Integrating IPv4 and IPv6 Network Environments

Day 8 Tasks

- Read the theory lesson below
- Read the ICND1 cram guide

As you have learned in the previous module, numerous advantages can be gained by migrating from IPv4 to IPv6. To recap, these advantages include the following:

- The simplified IPv6 packet header
- Larger address space
- IPv6 addressing hierarchy
- IPv6 extensibility
- IPv6 Broadcast elimination
- Stateless autoconfiguration
- Integrated mobility
- Integrated enhanced security

This module maps to the following CCNA syllabus requirement:

- Describe the technological requirements for running IPv6 in conjunction with IPv4, such as dual-stack implementation

NOTE: Because the above advantages were described in detail in the previous module, they will not be described again here.

In Day 7's lesson on IPv6, we focused exclusively on a pure IPv6 environment and learned about how IPv6 operates, as well as how the different routing protocols that support IPv6 routing are configured and validated in Cisco IOS software. While it is important to have a solid understanding of IPv6 on its own, the reality of the situation is that IPv4 is still the most predominately used version of the Internet Protocol. For this reason, it is important to understand how to integrate the two different protocol stacks when considering migrating to a pure IPv6 environment.

While migrating to an IPv6 environment would offer the previously mentioned advantages, the reality of the present situation is that not all addressable devices support IPv6, and therefore IPv4 and IPv6 must coexist within the same network for devices running different protocol stacks in order to use the same network infrastructure. IPv4 and IPv6 integration and coexistence strategies are divided into three broad classes, as follows:

- Dual-stack implementation
- Tunnelling
- Protocol translation

Dual-stack implementation is required when internetwork devices and hosts use both protocol stacks (i.e., IPv4 and IPv6) at the same time. Dual-stack implementation allows the hosts to use either IPv4 or IPv6 to establish end-to-end IP sessions with other hosts.

NOTE: Dual-stack implementation does not mean that the IPv4-only and IPv6-only hosts have the ability to communicate with each other. To do so, additional protocols and mechanisms are needed. Dual-stack simply means that the hosts (and infrastructure) are able to support both the IPv4 protocol stack and the IPv6 protocol stack.

In situations where dual-stack implementation cannot be used, it is possible to tunnel the IPv6 packets over IPv4 networks. In these implementations, tunnels are used to encapsulate IPv6 packets in IPv4 packets, allowing them to be sent across portions of the network that don't have or do not yet natively support IPv6. This allows the IPv6 "islands" to communicate over the underlying IPv4 infrastructure.

NOTE: With tunnelling, nodes or internetwork devices must support dual-stack in order to tunnel the IPv6 packets over the IPv4 infrastructure.

Finally, in some cases, it is possible that IPv4-only environments will need to communicate with IPv6-only environments, and vice versa. In these situations, neither dual-stack nor tunnelling implementations can be used so protocol translation between IPv4 and IPv6 must be enabled. While supported, this is the least desirable method of integrating IPv4 and IPv6 networks. However, because it is supported, it is important to understand how to do this.

The remainder of this module will describe, in detail, the dual-stack implementation and tunnelling methods of integrating IPv4 and IPv6 networks. Included are configuration examples specific to Cisco IOS software.

IPv4 and IPv6 Dual-Stack Implementations

With dual-stack implementations, while some hosts have the capability to use both the IPv4 and the IPv6 protocol stacks, they still require some help in deciding when to use the IPv6 protocol stack instead of the IPv4 protocol stack. Fortunately, this is possible using one of two methods, which are described as follows:

- The first method requires manual configuration by the user. If users know the IPv6 address of the destination IPv6 host, they can use that to establish an IPv6 session manually to that host from their dual-stack host. Although this method works well, it can become quite cumbersome to remember IPv4 and IPv6 addresses for multiple hosts.
- The second method entails using a naming service, such as DNS. With this method, the Fully Qualified Domain Names (FQDNs), such as www.howtonetwork.com, are configured using both IPv4 and IPv6 addresses. The FQDN is represented by an A record for the IPv4 protocol stack and an AAAA record for the IPv6 protocol stack, which allows the DNS server to be queried using either IPv4 or IPv6.

Implementing Dual-Stack Support in Cisco IOS Software

While delving into the different ways in which different types of hosts by different vendors can support dual-stack implementations is beyond the scope of the CCNA exam requirements, as a future network engineer, it is imperative to understand how to implement dual-stack solutions

https://t.me/learningnets

in Cisco IOS software. In Cisco IOS routers, dual-stack operation is enabled by simply configuring both an IPv4 address and an IPv6 address on the router interface.

Multiple IPv4 addresses can be specified by appending the `[secondary]` keyword to the end of the `ip address [address] [mask]` interface configuration command. For IPv6, however, the `[secondary]` keyword is not required, as multiple prefixes can be configured per interface using the `ipv6 address` interface configuration command, which was described in detail in Day 7's lesson. The following configuration example illustrates how to configure multiple IPv4 and IPv6 addresses and prefixes on a single router interface:

```
R3(config)#ipv6 unicast-routing
R3(config)#interface FastEthernet0/0
R3(config-if)#ip address 10.0.0.3 255.255.255.0
R3(config-if)#ip address 10.0.1.3 255.255.255.0 secondary
R3(config-if)#ip address 10.0.2.3 255.255.255.0 secondary
R3(config-if)#ipv6 address 3fff:1234:abcd:1::3/64
R3(config-if)#ipv6 address 3fff:1234:abcd:2::3/64
R3(config-if)#ipv6 address 3fff:1234:abcd:3::3/64
R3(config-if)#ipv6 enable
R3(config-if)#exit
```

NOTE: While IPv4 routing is enabled by default in Cisco IOS software, IPv6 routing is disabled by default and must be explicitly enabled.

Following the configuration of the IPv4 and IPv6 addresses, you can simply view the router configuration to validate your configuration, as illustrated in the following output:

```
R3#show running-config interface FastEthernet0/0
Building configuration...
Current configuration : 395 bytes
!
interface FastEthernet0/0
ip address 10.0.1.3 255.255.255.0 secondary
ip address 10.0.2.3 255.255.255.0 secondary
ip address 10.0.0.3 255.255.255.0
ipv6 address 3FFF:1234:ABCD:1::3/64
ipv6 address 3FFF:1234:ABCD:2::3/64
ipv6 address 3FFF:1234:ABCD:3::3/64
ipv6 enable
end
```

To view specific IPv4 and IPv6 interface parameters, simply use the Cisco IOS software `show ip interface [name]` or the `show ipv6 interface [name]` commands. Following is the output of the `show ip interface` command for the FastEthernet0/0 interface:

```
R3#show ip interface FastEthernet0/0 | section address
  Internet address is 10.0.0.3/24
```

https://t.me/learningnets

```
  Broadcast address is 255.255.255.255
  Helper address is not set
  Secondary address 10.0.1.3/24
  Secondary address 10.0.2.3/24
  Network address translation is disabled
```

The following output illustrates the information printed by the `show ipv6 interface` command for the same FastEthernet0/0 interface used in the previous example:

```
R3#show ipv6 interface FastEthernet0/0 | section address
  IPv6 is enabled, link-local address is FE80::213:19FF:FE86:A20
  Global unicast address(es):
    3FFF:1234:ABCD:1::3, subnet is 3FFF:1234:ABCD:1::/64
    3FFF:1234:ABCD:2::3, subnet is 3FFF:1234:ABCD:2::/64
    3FFF:1234:ABCD:3::3, subnet is 3FFF:1234:ABCD:3::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::5
    FF02::6
    FF02::9
    FF02::1:FF00:3
  Hosts use stateless autoconfig for addresses.
```

Configuring Static IPv4 and IPv6 Host Addresses in Cisco IOS Software

Cisco IOS software supports the configuration of both static IPv4 and IPv6 host addresses using the `ip host [name] [v4-address]` and `ipv6 host [name] [v6-address]` global configuration commands, respectively. The following example illustrates how to configure static IPv4 and IPv6 host names and addresses in Cisco IOS software:

```
R1(config)#ip host TEST-HOST 10.0.0.3
R1(config)#ipv6 host TEST-HOST 3FFF:1234:ABCD:1::3
```

The static IPv4 and IPv6 host configuration can be validated using the `show hosts` command, the output of which is printed below:

```
R1#show hosts
...
[Truncated Output]
...
Host         Port  Flags      Age Type   Address(es)
TEST-HOST    None  (perm, OK)  0   IP     10.0.0.3
TEST-HOST    None  (perm, OK)  0   IPv6   3FFF:1234:ABCD:1::3
```

https://t.me/learningnets

When the same host is configured with both a static IPv4 and IPv6 address, Cisco IOS software

will use the IPv6 address. If DNS is used, the dual-stack host will first search AAAA (IPv6) records and then fall back to the A records (IPv4) when configured with both IPv6 and IPv4 DNS servers. This default behaviour can be validated by performing a simple ping to the previously configured static host "TEST-HOST" as follows:

```
R1#ping test-host repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 3FFF:1234:ABCD:1::3, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 0/1/4 ms
```

Configuring IPv4 and IPv6 DNS Servers in Cisco IOS Software

The configuration of both IPv4 and IPv6 DNS servers in Cisco IOS software still uses the `ip name-server [address]` global configuration command. This same command has now been modified to allow the DNS server IP address to be specified as either an IPv4 or an IPv6 address. The following example illustrates how to configure a router to use both an IPv4 and an IPv6 DNS server:

```
R1(config)#ip name-server ?
  A.B.C.D     Domain server IP address (maximum of 6)
  X:X:X:X::X  Domain server IP address (maximum of 6)
R1(config)#ip name-server 3FFF:1234:ABCD:1::2
R1(config)#ip name-server 192.168.1.2
```

NOTE: As was previously mentioned, when IPv6 and IPv4 DNS servers are configured on the same router, the router will look for the AAAA records first (i.e., IPv6). However, if AAAA records are not found, the host looks for an A record to communicate with the hostname.

Tunnelling IPv6 Datagrams across IPv4 Networks

Tunnelling, the second method of integrating IPv6 and IPv4 networks, entails encapsulating the IPv6 packets or datagrams and sending them over IPv4 networks. In order to support the different tunnelling mechanisms that will be described in this section, Cisco IOS edge routers must have a dual-stack implementation that allows the IPv6 packets to be encapsulated in IPv4 packets, and then de-encapsulated at the terminating router. It should be noted that intermediate routers do not need to run IPv6. In other words, these routers would simply be IPv4-only routers. Figure 8.1 below illustrates a typical tunnelling implementation:

https://t.me/learningnets

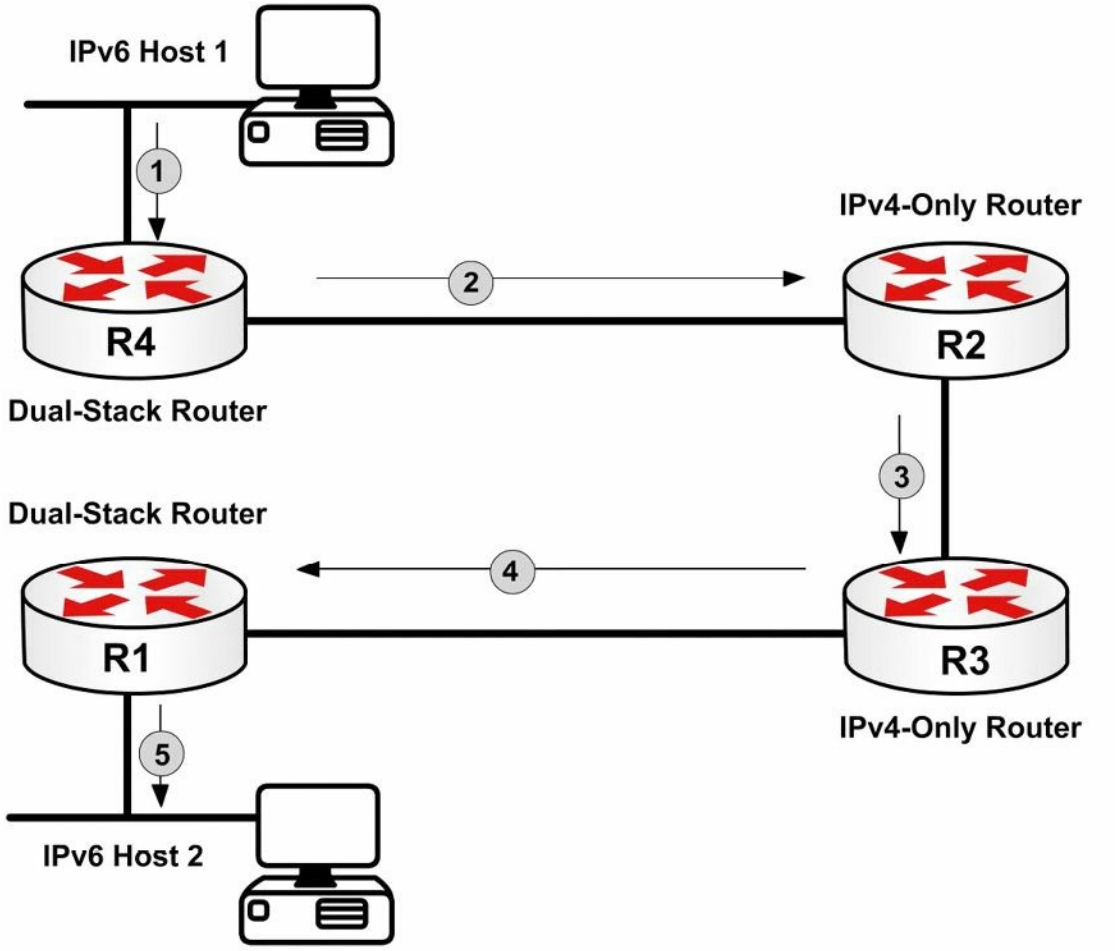


Figure 8.1 – Tunnelling IPv6 Packets over IPv4 Networks

Referencing Figure 8.1, assuming that IPv6 Host 1 is sending datagrams to IPv6 Host 2, the following sequence of events occurs as those packets transit the network:

1. IPv6 Host 1 sends the IPv6 packets destined to IPv6 Host 2 to its default gateway, which is router R4. These are native IPv6 packets, with IPv6 source and destination addresses included in the header.
2. Router R4 is a dual-stack router. The LAN interface has been enabled for IPv6, while the WAN interface has been enabled for IPv4. R4 has a tunnel configured between its WAN interface and the WAN interface of R1, which is also a dual-stack router. Upon receiving the IPv6 packets, R4 encapsulates them in IPv4 packets and forwards them to R2. The destination address for these packets is sent to R1 and the router sets the value of the IPv4 header to 41 to indicate encapsulation of IPv6 packets in IPv4 packets.
3. R2 receives the IPv4 packets and simply routes or forwards those towards their final destination using the destination address specified in the IPv4 header.
4. R3 receives the IPv4 packets from R2 and simply forwards those towards their final destination using the destination address specified in the IPv4 packet header.
1. R1, the terminating router and exit point for the tunnel, receives the native IPv4 packets and de-encapsulates them, leaving only the IPv6 datagrams. The router then forwards the IPv6 packets to Host 2.

The encapsulation and de-encapsulation process is transparent to the two hosts, as well as to

https://t.me/learningnets

the intermediate routers between the tunnel endpoints. Several methods can be used to tunnel IPv6 packets in IPv4 packets (see below). We won't go into any configuration details in this guide because it's beyond the CCNA exam requirements.

Other tunnelling methods include the below. Cisco may expect you know they exist but you should not be asked any questions about how they operate.

- Static (manually configured) IPv6 tunnelling
- 6to4 tunnelling
- Automatic IPv4-compatible tunnelling
- ISATAP tunnelling
- Generic Routing Encapsulation tunnelling

https://t.me/learningnets

Day 8 Questions

1. Name three IPv4 to IPv6 transition mechanism classes.
2. _____ implementation is required when internetwork devices and hosts use both protocol stacks (i.e., IPv4 and IPv6) at the same time.
3. With dual-stack implementation, name two methods that help hosts decide when to use the IPv6 protocol stack instead of the IPv4 protocol stack.
4. While IPv4 routing is enabled by default in Cisco IOS software, IPv6 routing is disabled by default and must be explicitly enabled. True or false?
5. Name a command that will provide IPv6 interface parameters.
6. The static IPv4 and IPv6 host configuration can be validated using the _____ command.
7. Which command is used to configure an IPv6 DNS server?
8. _____ entails encapsulating the IPv6 packets or datagrams and sending them over IPv4 networks.

https://t.me/learningnets

Day 8 Answers

1. Dual-stack implementation, tunnelling, and protocol translation.
2. Dual-stack.
3. Manual configuration and naming service.
4. True.
5. The `show ipv6 interface` command.
6. `show hosts`.
7. The `ip name-server` command.
8. Tunnelling.

https://t.me/learningnets

Day 8 Labs

IPv4 – IPv6 Basic Integration Lab

Test the IPv6 concepts and commands detailed in this module on a pair of Cisco routers that are directly connected:

- ☐ Enable IPv6 Unicast routing on the devices and configure both IPv4 and IPv6 addresses on directly connected interfaces
- ☐ Verify the configuration using the `show interface` and `show ipv6 interface` commands
- ☐ Configure IPv4 and IPv6 hosts for remote interface addresses
- ☐ Verify the hosts configuration (`show` commands) on the devices
- ☐ Ping by using the host names between the devices
- ☐ Configure IPv4 and IPv6 DNS servers on both devices

IPv4 – IPv6 Tunnelling Lab

Repeat the scenario from the IPv6 over IPv4 tunnelling section (including all the mechanisms) on a home network environment. Follow the sequence of events presented in that section.

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 9 – Access Control Lists

Day 9 Tasks

- Read today's lesson notes (below)
- Complete today's lab
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website

Along with subnetting and VLSM, access control lists (ACLs) are one of the bugbear subjects for new Cisco students. Among the problems are learning the IOS configuration commands, understanding ACL rules (including the implicit "deny all" rule), and learning the port numbers and protocol types.

Like any subject, you should take the learning process one step at a time, apply every command you see here to a router, and do lots and lots of labs.

Today you will learn about the following:

- ACL basics
- Standard, extended, and named ACLs
- ACL rules
- Wildcard masks
- ACL configuration
- Troubleshooting ACLs

This module maps to the following CCNA syllabus requirements:

- Describe the types, features, and applications of ACLs
  - Standard
  - Sequence numbers
  - Editing
  - Extended
  - Named
  - Numbered
  - Log option
  - Configure and verify ACLs in a network environment

ACL Basics

The point of ACLs is to filter the traffic which passes through your router. I don't know of any

https://t.me/learningnets

network which should permit any traffic type to enter or leave it.

As well as filtering traffic, ACLs can be used to reference NAT pools, to filter your debugging commands, and with route maps (this is outside of the CCNA syllabus requirements). Depending upon the type of ACL you configure, you can filter traffic based on source network or IP addresses, destination network or IP addresses, protocols, or port numbers. You can apply ACLs to any router interface, including your Telnet ports.

The three main types of ACLs are as follows:

- Standard numbered
- Extended numbered
- Standard or extended named

Standard numbered ACLs are the most basic form of ACL you can apply to the router. While they are the easiest to configure, they have the most limited range of filters available. They can only filter based on the source IP address or network. The way to recognise a standard ACL is by the number which precedes the configuration lines; these numbers will be from 1 to 99.

Extended numbered ACLs allow far more granularity but can be trickier to configure and troubleshoot. They can filter a destination or source IP address or network, a protocol type, and a port number. The numbers you can use to configure extended ACLs are 100 to 199, inclusive.

Named ACLs allow you to associate a list of filters with a name rather than a number. This makes them easier to identify in router configurations. Named ACLs can actually be either extended or standard; you choose which at the initial configuration line of the ACL.

For success in the CCNA exam, and to make it as a new Cisco engineer, you need to understand the following:

- Port numbers
- ACL rules
- Command syntax for ACLs

Port Numbers

You simply must know the common port numbers by heart if you want to pass the CCNA exam and to work on live networks. Looking up common port numbers isn't an option when you have customers watching what you are doing. Here are the most common port numbers you will encounter and will need to know:

TABLE 9.1 – Common CCNA Port Numbers

Port	Service	Port	Service
20	FTP Data	80	HTTP
21	FTP Control	110	POP3
22	SSH	119	NNTP

https://t.me/learningnets

23	Telnet	123	NTP
25	SMTP	161/162	SNMP
53	DNS	443	HTTPS (HTTP with SSL)
69	TFTP		

Access Control List Rules

This is one of the hardest parts to understand. I've never seen a complete list of rules written down in one Cisco manual. Some refer to them generally or explain some of them, but then miss others completely. The difficulty is that the rules always apply but (until now) you found them only by trial and error. Here are the rules you need to know:

ACL Rule 1 – Use only one ACL per interface per direction.

This makes good sense. You wouldn't want to have several ACLs doing different things on the same interface. Simply configure one ACL which does everything you need it to, rather than spreading out filters over two or more lists. I could have added "per protocol" to the above rule because you could have an IPX access control list, but IP is really the only protocol in use in modern networks.

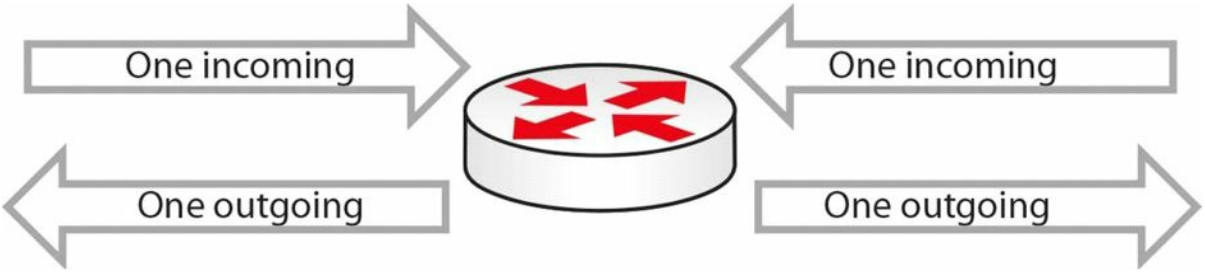


Figure 9.1 – One ACL per Interface per Direction

ACL Rule 2 – The lines are processed top-down.

Some engineers become confused when their ACL doesn't perform as expected. The router will look at the top line of the ACL, and if it sees a match, it will stop there and will not examine the other lines. For this reason, you need to put the most specific entries at the top of the ACL. For example, take the ACL blocking host 172.16.1.1:

Permit 10.0.0.0		No match
Permit 192.168.1.1		No match
Permit 172.16.0.0	✔	Match – Permit
Permit 172.16.1.0		Not processed
Deny 172.16.1.1		Not processed

In the example above, you should have put the Deny 172.16.1.1 line at the top, or at least above the Permit 172.16.0.0 statement.

ACL Rule 3 – There is an implicit "deny all" at the bottom of every ACL.

https://t.me/learningnets

This catches many engineers out. There is an invisible command at the bottom of every ACL. This command is set to deny all traffic which hasn't been matched yet. The only way to stop this command coming into effect is to configure a "permit all" at the bottom manually. For example, take an incoming packet from IP address 172.20.1.1:

Permit 10.0.0.0	No match
Permit 192.168.1.1	No match
Permit 172.16.0.0	No match
Permit 172.16.1.0	No match
[Deny all]	**Match – DROP PACKET**

You actually wanted the packet to be permitted by the router, but instead it denies it. The reason

is the implicit "deny all," which is a security measure.

ACL Rule 4 – The router can't filter self-generated traffic.

This can cause confusion when doing testing before implementing your ACL on a live network. A router won't filter traffic it generated itself. This is demonstrated in Figure 9.2 below:

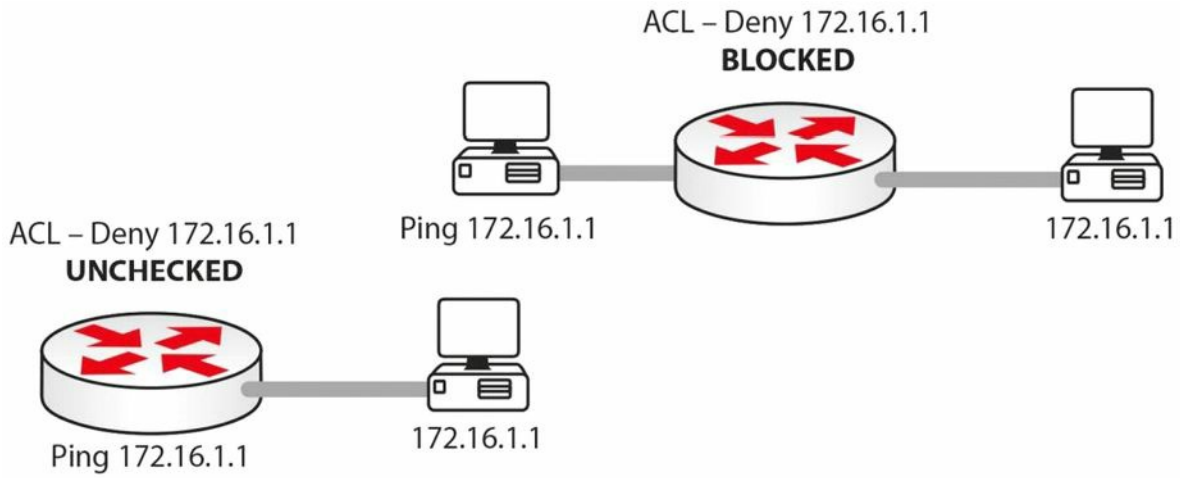


Figure 9.2 – ACL Testing with Self-Generated Traffic

ACL Rule 5 – You can't edit a live ACL.

In fact, until IOS 12.4 you could only edit a named ACL, not standard or extended ACLs. This was a limitation of ACL architecture. Before IOS 12.4, if you wanted to edit a standard or extended ACL, you had to follow these steps (I used list 99 as an example):

1. Stop ACL traffic on the interface with the `no ip access-group 99 in` command.
2. Copy and paste the ACL into Notepad and edit it there.
3. Go into ACL mode and paste in the new ACL.
4. Apply the ACL to the interface again.

Here are the steps on a live router:

https://t.me/learningnets

ACL created and applied to interface:

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 1 permit 172.16.1.1
Router(config)#access-list 1 permit 172.16.2.1
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group 1 in
```

Take off the active interface:

```
Router(config)#int FastEthernet0/0
Router(config-if)#no ip access-group 1 in
Router(config-if)#^Z
```

Show the ACLs. Copy and paste into Notepad and make the changes:

```
Router#show run
```
← or `show ip access lists`

```
access-list 1 permit host 172.16.1.1
access-list 1 permit host 172.16.2.1
```

You actually need to add an exclamation mark in-between each line of configuration (if you are pasting it in) to tell the router to do a carriage return:

```
access-list 1 permit host 172.16.1.1
!
access-list 1 permit host 172.16.2.2
```

The lines being pasted into the router configuration are shown below. Delete the previous ACL and then paste in the new version:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no access-list 1
Router(config)#access-list 1 permit host 172.16.1.1
Router(config)#!
Router(config)#access-list 1 permit host 172.16.2.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
show ip access
Router#show ip access-lists
Standard IP access list 1
    permit host 172.16.1.1
    permit host 172.16.2.2
Router#
Router(config)#int FastEthernet0/0
Router(config-if)#ip access-group 1 in
```
← reapply to the interface

https://t.me/learningnets

The commands above may not work if you are using Packet Tracer. Also, please do try these commands on a router because they are exam topics. Bear in mind that you should disable the ACL on the interface (so it's no longer live) before you edit it in order to avoid strange or unpredictable behaviour. I'll show you how to edit live ACLs on IOS 12.4 and later shortly.

ACL Rule 6 – Disable the ACL on the interface.

Many engineers, when they want to test or deactivate the ACL for a while, will actually delete it altogether. This isn't necessary. If you want to stop the ACL from working, simply remove it from the active interface it is applied to:

```
Router(config)#int FastEthernet0/0
Router(config-if)#no ip access-group 1 in
Router(config-if)#^Z
```

ACL Rule 7 – You can reuse the same ACL.

I've seen this often on live networks. You will usually have the same ACL policy throughout your network. Rather than configuring several ACLs, simply refer to the same ACL and apply it to as many interfaces as you require. Figure 9.3 below illustrates this concept:

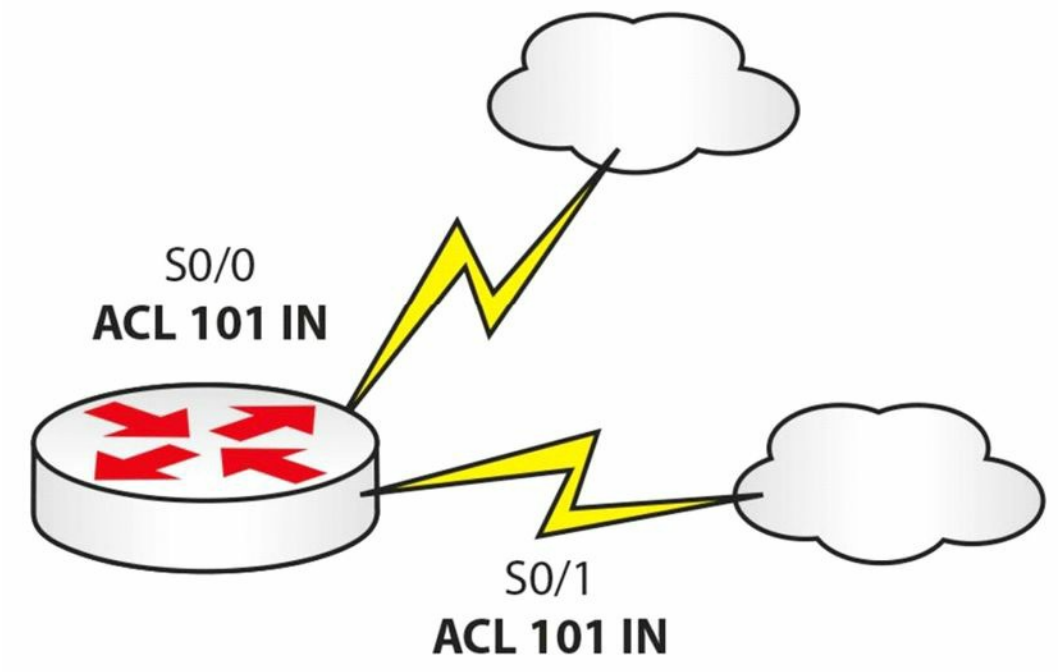


Figure 9.3 – You Can Reuse an ACL

ACL Rule 8 – Keep them short!

The basic rule with ACLs is to keep them short and focused. Many novice Cisco engineers stretch their ACL over many lines when, with some thought, it could be tightened to just a few lines of configuration. I've mentioned previously that you want your most specific lines of configuration on top. This is good practice and saves CPU cycles on the router.

Good ACL configuration skills come with knowledge and practise.

ACL Rule 9 – Put your ACL as close to the source as possible.

Cisco documentation advises us to put an EXTENDED ACL as close to the SOURCE as possible and STANDARD ACL as close to the DESTINATION as possible, because that will prevent

https://t.me/learningnets

unnecessary overhead but will still allow any “legitimate” traffic.

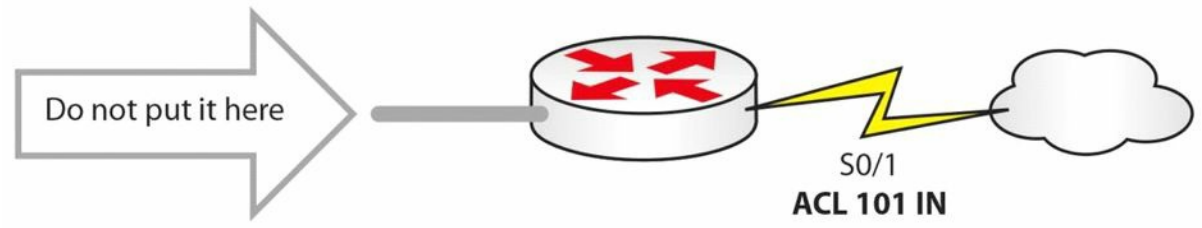


Figure 9.4 – Put Your ACL Close to the Source

> Farai says – “The official Cisco advice is EXTENDED as close to the SOURCE as possible and STANDARD as close to the DESTINATION as possible.”

Wildcard Masks

Wildcard masks are essential to learn because they are used as part of command line configuration in ACLs and some routing protocols. They exist because there has to be a way to tell the router which parts of an IP address or network address you want to match.

The matching is done at the binary level, but you can easily configure wildcard masks using the same notation you use for subnet masks. A binary 1 tells the router to ignore the digit and a 0 means match the digit.

The easy way to perform wildcard masking for the CCNA exam is simply to ensure that you add a number to the subnet mask to give you a total of 255. So, if your subnet mask in one octet was 192, you would add 63 to it to make 255. If it was 255, you would add 0. Take a look at the examples below:

Subnet	255	255	255	192
Wildcard	0	0	0	63
Equals	**255**	**255**	**255**	**255**

Subnet	255	255	224	0
Wildcard	0	0	31	255
Equals	**255**	**255**	**255**	**255**

Subnet	255	128	0	0
Wildcard	0	127	255	255
Equals	**255**	**255**	**255**	**255**

You need to enter a wildcard mask if you want your ACL to match a subnet or an entire network. For example, if you wanted to match 172.20.1.0 255.255.224.0, you would enter the following:

https://t.me/learningnets

```
Router(config)#access-list 1 permit 172.20.1.0 0.0.31.255
```

Matching subnet 192.200.1.0 255.255.255.192 would require the following:

```
Router(config)#access-list 1 permit 192.200.1.0 0.0.0.63
```

Be careful when applying network statements with OSPF, which also requires a wildcard mask.

The same principle applies when you have a network with two host bits, as you will need to enter an ACL to match these. For example, matching subnet 192.168.1.0 255.255.255.252 or /30, you will need to enter the following:

```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.3
```

I have left off some configuration, as I just want to show the relevant part. This will match hosts 1 and 2 on the 192.168.1.0 network. If you wanted to match hosts 5 and 6 on the 192.168.1.4/30 network, you would enter the following:

```
Router(config)#access-list 1 permit 192.168.1.4 0.0.0.3
```

Read through the subnetting and VLSM notes to understand this concept further. It is important!

Configuring Access Control Lists

As with any skill, repetition makes mastery. As I've said before, you must type on a router every example I give, do as many labs as possible, and then make up your own examples. You need to be fast and you need to be accurate, both in the exam and in the real world.

The standard and extended ACLs presented in the next sections are numbered ACLs. These represent the classic way of configuring ACLs. Named ACLs are the other way of configuring ACLs and they are presented in a subsequent section.

Standard ACLs

Standard numbered ACLs are the easiest to configure, so this is the best place to start. Standard ACLs can only filter based on a source network or IP address.

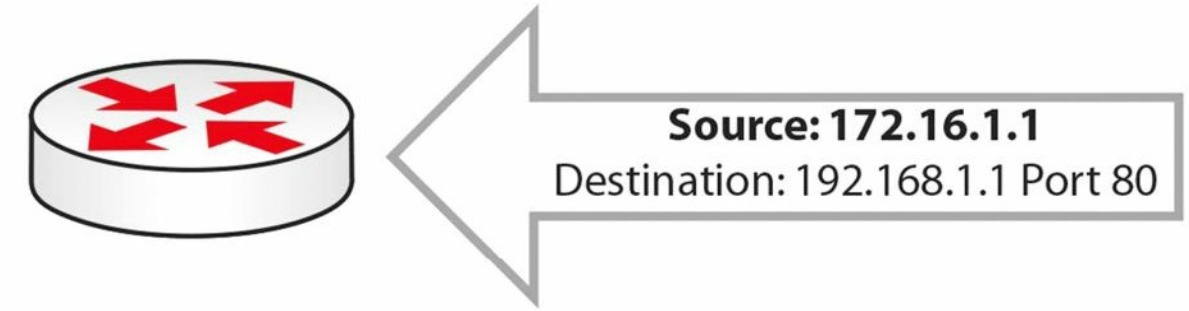


Figure 9.5 – Incoming Packet with Source and Destination

In Figure 9.5 above, the incoming packet has a source and destination address, but your standard ACL will only look at the source address. Your ACL would permit or deny this source address (see Figure 9.6):

```
Router(config)#access-list 1 permit host 172.16.1.1
```

https://t.me/learningnets

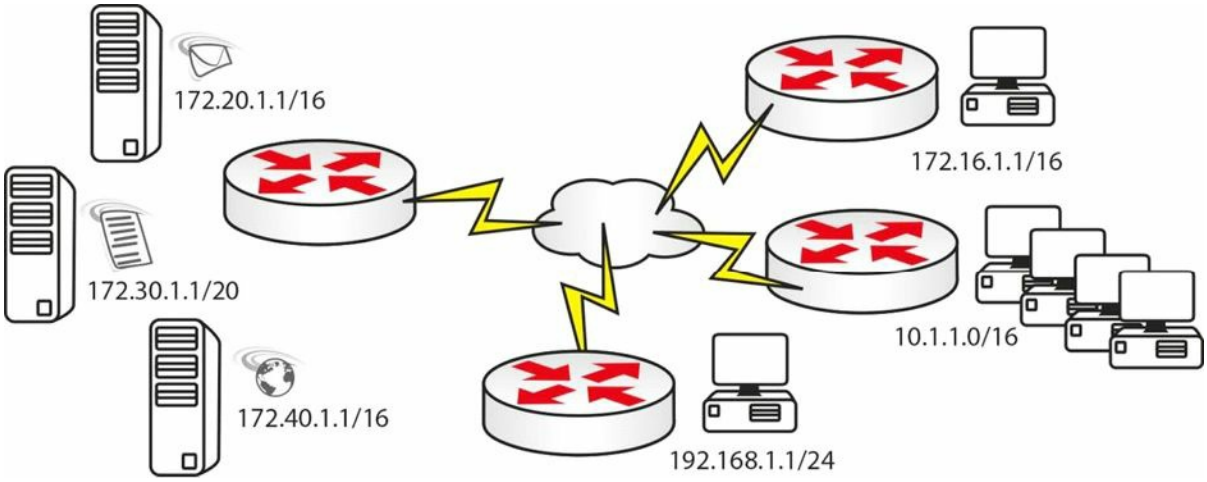


Figure 9.6 – Network with Multiple Hosts/Networks

```
Router(config)#access-list 1 permit host 172.16.1.1
Router(config)#access-list 1 permit host 192.168.1.1
Router(config)#access-list 1 permit 10.1.0.0 0.0.255.255
```

This would be applied to the server side router. Remember that there will be an implicit "deny all" at the end of this list, so all other traffic will be blocked.

Extended ACLs

Far more granularity is built into extended numbered ACLs; however, this makes them trickier to configure. You can filter source or destination networks, ports, protocols, and services.

Generally, you can look at the configuration syntax for extended ACLs, as follows:

```
access list# permit/deny [service/protocol] [source network/IP] [destination network/IP]
[port#]
```

For example:

```
access-list 101 deny tcp 10.1.0.0 0.0.255.255 host 172.30.1.1 eq telnet
access-list 100 permit tcp 10.1.0.0 0.0.255.255 host 172.30.1.1 eq ftp
access-list 100 permit icmp any any
```

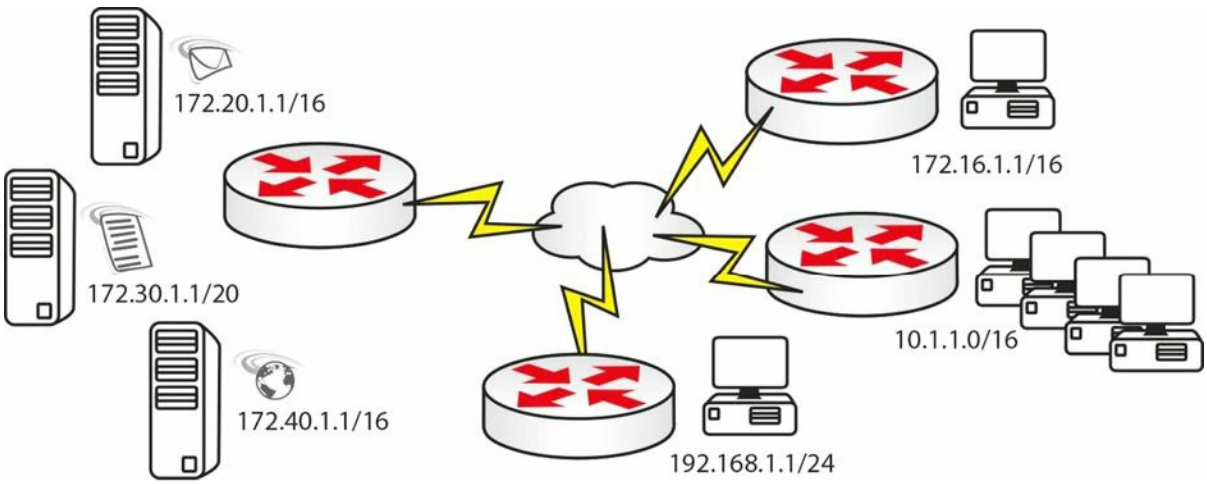


Figure 9.7 – Blocking Server Access Example

An ACL you could configure for the network above, featuring e-mail, web, and file servers, would be as follows (applied on the server side):

https://t.me/learningnets

```
access-list 100 permit tcp host 172.16.1.1 host 172.20.1.1 eq smtp
```

```
access-list 100 permit tcp 10.1.0.0 0.0.255.255 host 172.30.1.1 eq ftp
access-list 100 permit tcp host 192.168.1.1 host 172.40.1.1 eq www
```

Or, it could be the next ACL, if you had different requirements:

```
access-list 101 deny icmp any 172.20.0.0 0.0.255.255
access-list 101 deny tcp 10.1.0.0 0.0.255.255 host 172.30.1.1 eq telnet
```

Or, it could be as follows:

```
access-list 102 permit tcp any host 172.30.1.1 eq ftp established
```

The `[established]` keyword tells the router to permit the traffic only if it was originated by hosts on the inside. The three-way handshake flags (ACK or RST bit) will indicate this.

Named ACLs

Unlike numbered ACLs, named ACLs can be easily identified based on their descriptive name, and this is useful especially in large configurations. They were introduced to add flexibility and ease of management of ACLs. Named ACLs can be considered more of a configuration enhancement, as it does not modify the core ACL structure (it just modifies the way we refer to an ACL).

The syntax is similar to the numbered ACLs, with the major difference of using names instead of numbers to identify ACLs. Just like in the case of numbered ACLs, you can configure standard or extended named ACLs.

Another difference when configuring named ACLs is that you always have to use the `ip access-list` command, unlike with numbered ACLs, where you could also use the simple `access-list` command.

```
Router(config)#access-list ?
  <1-99>             IP standard access list
  <100-199>          IP extended access list
  <1100-1199>        Extended 48-bit MAC address access list
  <1300-1999>        IP standard access list (expanded range)
  <200-299>          Protocol type-code access list
  <2000-2699>        IP extended access list (expanded range)
  <700-799>          48-bit MAC address access list
  dynamic-extended   Extend the dynamic ACL absolute timer
  rate-limit         Simple rate-limit specific access list
Router(config)#ip access-list ?
  extended    Extended access list
  log-update  Control access list log updates
  logging     Control access list logging
  resequence  Resequence access list
  standard    Standard access list
R1(config)#ip access-list standard ?
  <1-99>      Standard IP access-list number
```

https://t.me/learningnets

```
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name
R1(config)#ip access-list extended ?
  <100-199>    Extended IP access-list number
  <2000-2699>  Extended IP access-list number (expanded range)
  WORD         Access-list name
```

Named ACLs have a slightly different syntax than the other types of ACLs do (standard numbered and extended numbered). You can also edit live named ACLs, which is a useful feature. You simply need to tell the router that you want to configure a named ACL, and whether you want it to be standard or extended. You can also edit numbered ACLs with later IOS releases, so please check the documentation for your platform.

When creating a named ACL using the `ip access-list` command, Cisco IOS will place you in the ACL configuration mode where you can enter or remove ACL entries (denied or permitted access conditions). Figure 9.8 below shows an example of a named ACL, followed by the corresponding output:

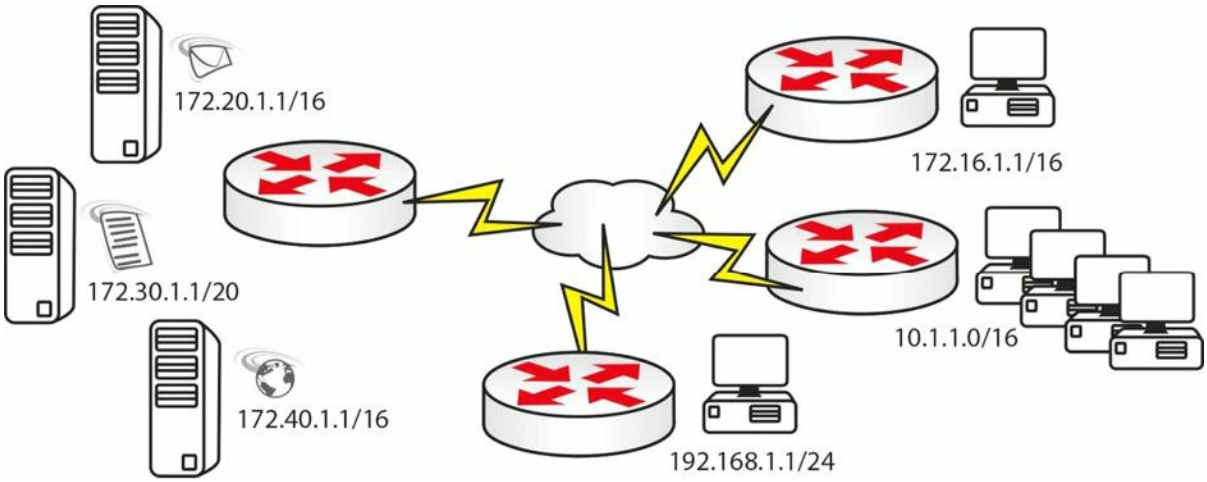


Figure 9.8 – Named ACL

```
Router(config)#ip access-list extended BlockWEB
Router(config-ext-nacl)#?
Ext Access List configuration commands:
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  dynamic         Specify a DYNAMIC list of PERMITs or DENYs
  evaluate        Evaluate an access list
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
Router(config-ext-nacl)#deny tcp any any eq 80
Router(config-ext-nacl)#permit ip any any
```

https://t.me/learningnets

Named ACL verification can be done using the following commands:

- `show ip access-lists`: shows all ACLs created on the device.
- `show ip access-lists <acl_name>`: shows a particular named ACL

```
Router(config)#do show ip access-lists
Standard IP access list test
    30 permit 10.1.1.1
    20 permit 192.168.1.1
    15 permit 172.20.1.1
    10 permit 172.16.1.1
```

To learn how you can add or delete ACL entries in a named ACL, please refer to the "ACL Sequence Numbers" section below.

Applying ACLs

In order to come into effect, you must apply your ACL to an interface or router port. I say this because I've seen many novice Cisco engineers type the ACL and then wonder why it isn't working! Or they configure it but apply the wrong ACL number or name to the interface.

If you are applying an ACL to a line, you have to specify it with the `access-class` command, and to an interface, it is the `ip access-group` command. Why Cisco have you do this, I will never know!

Here are three examples of ACLs being applied to a port or interface.

Interface:

```
Router(config)#int FastEthernet0/0
Router(config-if)#ip access-group 101 in
```

Line:

```
Router(config)#line vty 0 15
Router(config-line)#access-class 101 in
```

Interface:

```
Router(config)#int FastEthernet0/0
Router(config-if)#ip access-group BlockWEB in
```

ACL Sequence Numbers

With 12.4 onwards, you can see that Cisco IOS adds sequence numbers to each ACL entry. So now I can create an access control list and then remove a line from it.

```
Router(config)#ip access-list standard test
Router(config-std-nacl)#permit 172.16.1.1
Router(config-std-nacl)#permit 192.168.1.1
Router(config-std-nacl)#permit 10.1.1.1
Router(config-std-nacl)#
Router(config-std-nacl)#exit
```

https://t.me/learningnets

```
Router(config)#exit
Router#
*Jun  6 07:38:14.155: %SYS-5-CONFIG_I: Configured from console by console access
Router#show ip access-lists
Standard IP access list test
    30 permit 10.1.1.1
    20 permit 192.168.1.1
    10 permit 172.16.1.1
```

Note that the sequence numbers are not displayed in the router running configuration. In order to see them you have to issue a `show [ip] access-list` command.

Add an ACL Line

To add a new ACL line, you can simply enter the new sequence number and then the ACL statement. The example below shows how you can add line 15 to your existing ACL:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access
Router(config)#ip access-list standard test
Router(config-std-nacl)#15 permit 172.20.1.1
Router(config-std-nacl)#
Router(config-std-nacl)#do show ip access
Router(config-std-nacl)#do show ip access-lists
Standard IP access list test
    30 permit 10.1.1.1
    20 permit 192.168.1.1
    15 permit 172.20.1.1
    10 permit 172.16.1.1
Router(config-std-nacl)#
```

Remove an ACL Line

To remove an ACL line, you can simply enter the `no <seq_number>` command, like in the example below where line 20 is deleted:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access
Router(config)#ip access-list standard test
Router(config-std-nacl)#no 20
Router(config-std-nacl)#
Router(config-std-nacl)#do show ip access
Router(config-std-nacl)#do show ip access-lists
Standard IP access list test
```

https://t.me/learningnets

```
    30 permit 10.1.1.1
    15 permit 172.20.1.1
    10 permit 172.16.1.1
Router(config-std-nacl)#
```

Resequence an ACL

To resequence an ACL, you can use the `ip access-list resequence <acl_name> <starting_seq_number> <step_to_increment>` command. The behaviour of this command can be examined in the example below:

```
Router(config)#ip access-list resequence test 100 20
Router(config)#do show ip access-lists
Standard IP access list test
    100 permit 10.1.1.1
    120 permit 172.20.1.1
    140 permit 172.16.1.1
Router(config-std-nacl)#
```

The resequence command created new sequence numbers, starting from 100, and incremented them by 20 for each new ACL line.

ACL Logging

By default, ACL entries that are matched by packets traversing a router interface create incremental counters that can be analysed using the `show ip access-lists` command, as can be seen in the example below:

```
Router#show ip access-lists
Extended IP access list test
    10 deny tcp any any eq 80 (10 matches)
    20 permit ip any any (56 matches)
```

If you need more detailed information about the traffic that is being matched by the ACL entries, you can configure the `log` or `log-input` parameters to the relevant ACL entries.

```
Router(config)#ip access-list extended test
Router(config)#no 10
Router(config)#10 deny tcp any any eq 80 log
Router#show ip access-lists
Extended IP access list test
    10 deny tcp any any eq 80 log
    20 permit ip any any (83 matches)
```

In the configuration sample above, ACL logging for test ACL entry 10 is configured. When a packet hits that ACL entry, the ACL counters will continue to increase but the router will also generate a log message that contains details about the specific ACL hit:

```
%SEC-6-IPACCESSLOGP: list test denied tcp 10.10.10.2(24667) -> 10.10.10.1(80), 1 packet
```

https://t.me/learningnets

If you need even more details about the transaction, you can replace the `log` paramter with the `log-input` parameter, as you can see in the example below:

```
Router(config)#ip access-list extended test
Router(config)#no 10
Router(config)#10 deny tcp any any eq 80 log-input
Router#show ip access-lists
Extended IP access list test
    10 deny tcp any any eq 80 log-input
    20 permit ip any any (125 matches)
```

When the specific ACL entry is hit, a more detailed log message is generated by the router, which includes the incoming interface and the source MAC address:

```
%SEC-6-IPACCESSLOGP: list test denied tcp 10.10.10.2(14013) (FastEthernet0/0
00aa.aabb.ccdd) -> 10.10.10.1(80), 1 packet
```

ACL logging can be very useful for troubleshooting to see what exactly is dropped/permitted, but one thing must be noted for real-world situations (this is beyond the scope of the CCNA exam): ACL entries that contain `[log]` or `[log-input]` keyword are process-switched by the router (as opposed to being CEF-switched, which is the default in modern routers – this will be covered later in the book). This requires more router CPU cycles, which can become a problem if there is a lot of traffic that is hitting the logged ACL entry.

Using ACLs to Limit Telnet and SSH Access

Besides filtering the traffic on an interface level, ACLs can be associated with many other device features, including filtering traffic on VTY lines. In a previous module, you learned how you can configure Telnet or SSH acsess to a device (e.g., router or switch) using the `line vty` command.

Sometimes you may not want to accept all Telnet/SSH connections to or from the device. In order to manipulate this you must define an ACL that defines the type of traffic that will be allowed or denied on the VTY line. The ACL can be numbered or named. You associate the ACL to the VTY line using the `access-class <acl> [in|out]` command.

The following example defines an ACL permitting Telnet traffic from host 10.10.10.1, which will then be applied inbound to the VTY lines:

```
Router(config)#ip access-list extended VTY_ACCESS
Router(config-ext-nacl)#permit tcp host 10.10.10.1 any eq telnet
Router(config-ext-nacl)#deny tcp any any
Router(config-ext-nacl)#exit
Router(config)#
Router(config)#line vty 0 4
Router(config-line)# access-class VTY_ACCESS in
Router(config-line)#
```

You can verify the configuration using the following commands:

```
Router#show run | begin line vty
```

https://t.me/learningnets

```
line vty 0 4
access-class VTY_ACCESS in
.....
```

Troubleshooting and Verifying ACLs

I think that with an understanding of the configuration commands and rules you should be fine with access control lists. If your ACL isn't working, first check that there is basic IP connectivity by pinging. Then check whether you have applied your ACL, that there are no typos, and whether you need to allow any IP traffic to pass (remember the implicit "deny all"). Some of the most important verification steps in the ACL troubleshooting process include:

- Verifying the ACL statistics
- Verifying the permitted networks
- Verifying the ACL interface and direction

Verifying the ACL Statistics

After you have successfully configured an ACL and applied it to an interface, it is very important to have a method by which you can verify the correct behaviour of the ACL, especially how many times an ACL entry has been used (hit). Based on the number of hits, you can adjust your filtering policy or you can enhance your ACLs to improve the overall security. Based on your needs, you can verify the ACL statistics on a global level or per interface (starting with IOS 12.4).

Global ACL Statistics

Global ACL statistics can be verifyied using the `show ip access-list` or `show access-list` commands, which can refer to a numbered or a named ACL:

```
Router#show ip access-lists
Extended IP access list test
    10 deny tcp any any eq 80 (10 matches)
    20 permit ip any any (56 matches)
```

This method may not provide very specific information in situations in which you apply the same ACL on different interfaces, as it offers overall statistics.

Per Interface ACL Statistics

In situations where you want to examine per interface ACL hits, either inbound or outbound, you can use the `show ip access-list interface <interface_number> [in|out]` command, as illustrated below:

```
Router#show ip access-list interface FastEthernet0/1 in
Extended IP access list 100 in
   10 permit ip host 10.10.10.1 any (5 matches)
   30 permit ip host 10.10.10.2 any (31 matches)
```

If no direction is specified, any input or output ACL applied to the specific interface is displayed. This feature is also called "ACL Manageability" and is available starting with IOS 12.4.

https://t.me/learningnets

Verifying the Permitted Networks

Sometimes, especially in large environments where you have to configure many ACLs, you can make typo errors when configuring the ACL entries and this can lead to wrong traffic flows being blocked on different interfaces. In order to verify the correct ACL entries (permit and deny statements) you can use either the `show run | section access-list` or the `show ip access-list` commands, as described in previous sections.

Verifing the ACL Interface and Direction

One common error when applying an ACL to an interface is applying it in the wrong direction, meaning inbound instead of outbound and outbound instead of inbound. This can cause a lot of issues, both from a functionality and security perspective. One of the first steps you should take in an ACL troubleshooting process is verifying that the ACL is applied to the correct interface and in the correct direction.

Multiple commands exist to verify this, including the `show run` and the `show ip access-list interface <interface> [in|out]` commands.

https://t.me/learningnets

Day 9 Questions

1. You can have a named, extended, and standard ACL on one incoming interface. True or false?
2. You want to test why your ping is blocked on your Serial interface. You ping out from the router but it is permitted. What went wrong? (Hint: See ACL Rule 4.)
3. Write a wildcard mask to match subnet mask 255.255.224.0.
4. What do you type to apply an IP access control list to the Telnet lines on a router?
5. How can you verify ACL statistics per interface (name the command)?
6. How do you apply an ACL to an interface?

https://t.me/learningnets

Day 9 Answers

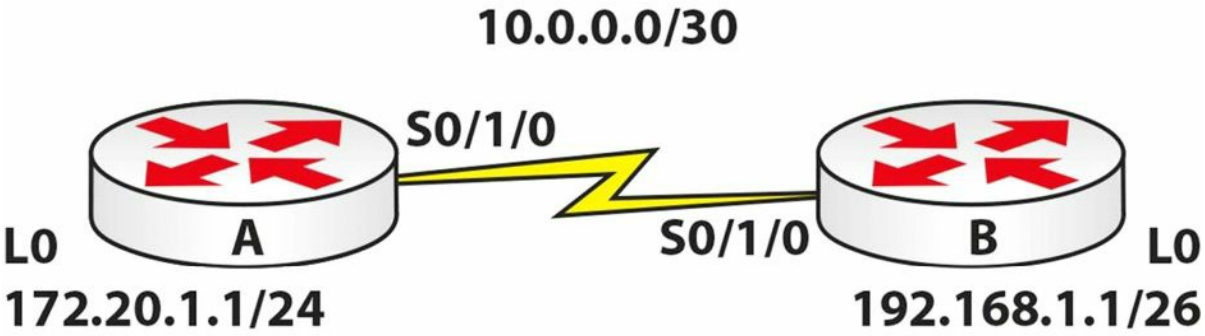
1. False. You can only configure a single ACL on an interface per direction.
2. A router won't filter traffic it generated itself.
3. 0.0.31.255.
4. `access-class`.
5. Issue the `show ip access-list interface` command.
6. Issue the `ip access-group <ACL_name> [in|out]` command.

https://t.me/learningnets

Day 9 Labs

Standard ACL Lab

Topology



Purpose

Learn how to configure a standard ACL.

Walkthrough

1. Configure the network above. Add a static route on each router so any traffic for any network leaves the Serial interface. You are doing this because, though not a routing lab, you still need the traffic to route. Add .1 to the Router A Serial interface and .2 to the Router B Serial interface.

```
RouterA(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0
RouterB(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0
```

2. Configure a standard ACL on Router A permitting the 192.168.1.0/10 network. By default, all other networks will be blocked.

```
RouterA(config)#access-list 1 permit 192.168.1.0 0.0.0.63
RouterA(config)#int Serial0/1/0
RouterA(config-if)#ip access-group 1 in
RouterA(config-if)#exit
RouterA(config)#exit
RouterA#
```

3. Test the ACL by pinging from Router B, which by default will use the 10.0.0.1 address.

```
RouterB#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

4. Test another ping, but source it from 192.168.1.1 and this should work.

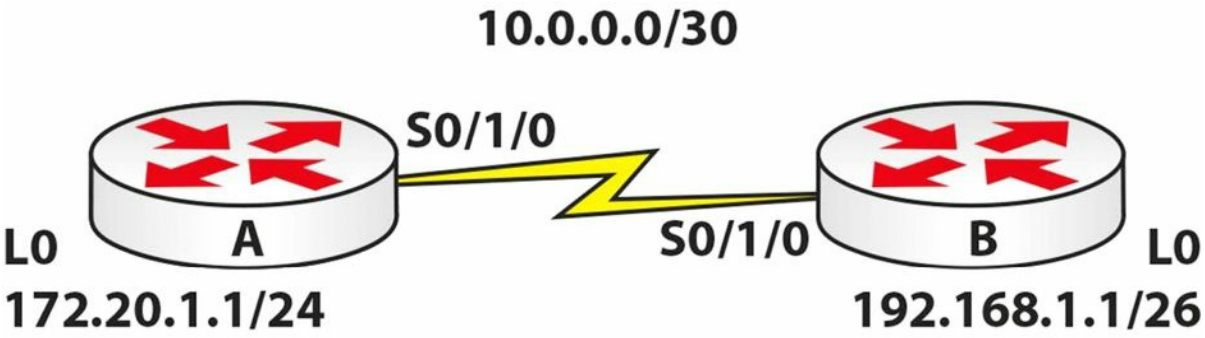
```
RouterB#ping
Protocol [ip]:
Target IP address: 10.0.0.1
Repeat count [5]:
```

https://t.me/learningnets

```
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/31/32 ms
```

Extended ACL Lab

Topology



Purpose

Learn how to configure an extended ACL.

Walkthrough

1. Configure the network above. Add a static route on Router B so any traffic for any network leaves the Serial interface. You are doing this because, though not a routing lab, you still need the traffic to route.

```
RouterB(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0
```

2. Add an extended ACL to Router A. Permit Telnet traffic to your Loopback interface only. Remember to permit Telnet also.

```
RouterA(config)#access-list 100 permit tcp any host 172.20.1.1 eq 23
RouterA(config)#int s0/1/0
RouterA(config-if)#ip access-group 100 in
RouterA(config-if)#line vty 0 15
RouterA(config-line)#password cisco
```

https://t.me/learningnets

```
RouterA(config-line)#login
RouterA(config-line)#^Z
RouterA#
```

The ACL line above is number 100, which tells the router it is extended. What you want to allow uses TCP. It is allowing TCP from any network destined for host 172.20.1.1 on the Telnet port, which is 23. When you issue a `show run` command, the router actually replaces the port number with the name, as illustrated below:

```
access-list 100 permit tcp any host 172.20.1.1 eq telnet
```

3. Now test a Telnet from Router B. First, Telnet to the Serial interface on Router A, which should be blocked. Then test the Loopback interface.

```
RouterB#telnet 10.0.0.1
Trying 10.0.0.1 ...
% Connection timed out; remote host not responding
RouterB#telnet 172.20.1.1
Trying 172.20.1.1 ...Open
User Access Verification
Password: ←password won't show when you type it
RouterA> ←Hit Control+Shift+6 together and then let go and press the X key to quit.
```

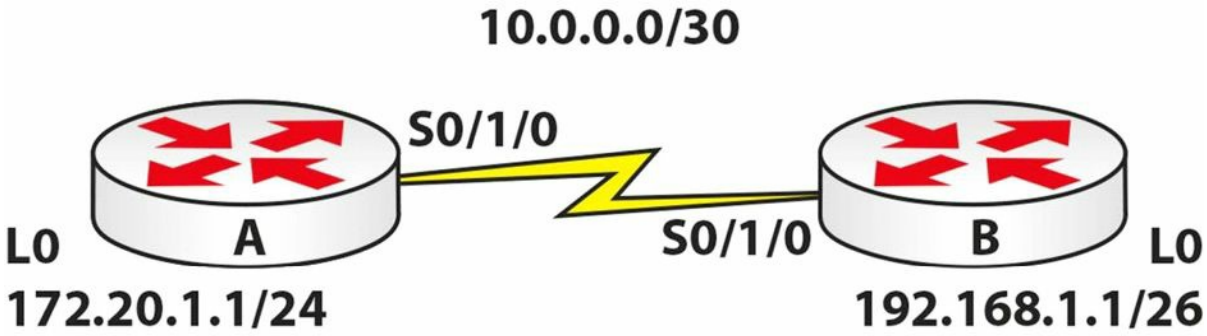
NOTE: We will be covering ACLs in other labs, but you really need to know these cold. For this reason, try other TCP ports, such as 80, 25, etc. In addition, try UDP ports, such as 53. You won't be able to test them easily without a PC attached to Router B.

Going further, mix up the IP addresses, permitting Telnet (in this example) to the Serial interface but not the Loopback interface. Then put an ACL on Router B instead. I can't over-emphasise how important this is. If you need to wipe the ACL, you can simply type the following:

```
RouterA(config)#no access-list 100
```

Named ACL Lab

Topology



Purpose

Learn how to configure a named ACL.

https://t.me/learningnets

Walkthrough

1. Configure the network above. Add a static route on each router so any traffic for any network leaves the Serial interface. You are doing this because, though not a routing lab, you still need the traffic to route.

```
RouterA(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0
RouterB(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0
```

2. Add an extended named ACL on Router B. Permit pings from host 172.20.1.1 but no other hosts or networks.

```
RouterB(config)#ip access-list extended blockping
RouterB(config-ext-nacl)#permit icmp host 172.20.1.1 any RouterB(config-ext-nacl)#exit
RouterB(config)#int s0/1/0
RouterB(config-if)#ip access-group blockping in
RouterB(config-if)#
```

3. Now test the ACL with pings from the Serial interface on Router A and the Loopback interface (which should work).

```
RouterA#ping 192.168.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

UUUUU

Success rate is 0 percent (0/5)

RouterA#ping

Protocol [ip]:

Target IP address: 192.168.1.1

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 172.20.1.1

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

Packet sent with a source address of 172.20.1.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 31/34/47 ms
```

NOTE: You need to understand which service is which, as well as which port numbers various services use. Otherwise, you will really struggle to configure an ACL. This ACL is pretty straightforward and can be achieved with one line. If you had

https://t.me/learningnets

routing protocols running, then they would need to be permitted.

To permit RIP, specify the following:

```
access-list 101 permit udp any any eq rip
```

To permit OSPF, specify the following:

```
access-list 101 permit ospf any any
```

To permit EIGRP, specify the following:

```
access-list 101 permit eigrp any any
```

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 10 – Routing Concepts

Day 10 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's lab
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website

The ICND1 exam requires you to have an understanding of basic routing and packet flow across a network. We will also take a look at the technology behind routing protocols.

Today you will learn about the following:

- Basic routing
- Classful and classless protocols
- Routing protocol classes

This module maps to the following CCNA syllabus requirements:

- Describe basic routing concepts
  - CEF
  - Packet forwarding
  - Router lookup process
- Differentiate methods of routing and routing protocols
  - Link State vs. Distance Vector
  - Next hop
  - IP routing table
  - Passive interfaces (how they work)

Basic Routing

The role of routing protocols is to learn about other networks dynamically, exchange routing information with other devices, and connect internal and/or external networks.

It is important to note that routing protocols DO NOT send packets across the network. Their role is to determine the best path for routing. Routed protocols actually send the data, and the most common example of a routed protocol is IP.

Different routing protocols use different means of determining the best or most optimal path to a network or network node. Some types of routing protocols work best in static environments or environments with few or no changes, but it might take a long time to

https://t.me/learningnets

converge when changes to those environments are made. Other routing protocols, however, respond very quickly to changes in the network and can converge rapidly.

Network convergence occurs when all routers in the network have the same view and agree on optimal routes. When convergence takes a long time to occur, intermittent packet loss and loss of connectivity may be experienced between remote networks. In addition to these problems, slow convergence can result in network routing loops and outright network outages. Convergence is determined by the routing protocol algorithm used.

Because routing protocols have different characteristics, they differ in their scalability and performance. Some routing protocols are suitable only for small networks, while others may be used in small, medium, and large networks.

Packet Forwarding

Packet forwarding involves two processes:

- Determining the best path
- Sending the packet (switching)

When the router receives a packet for a directly connected network, the router checks the routing table and then the packet is forwarded to that network, as shown in Figure 10.1 below:

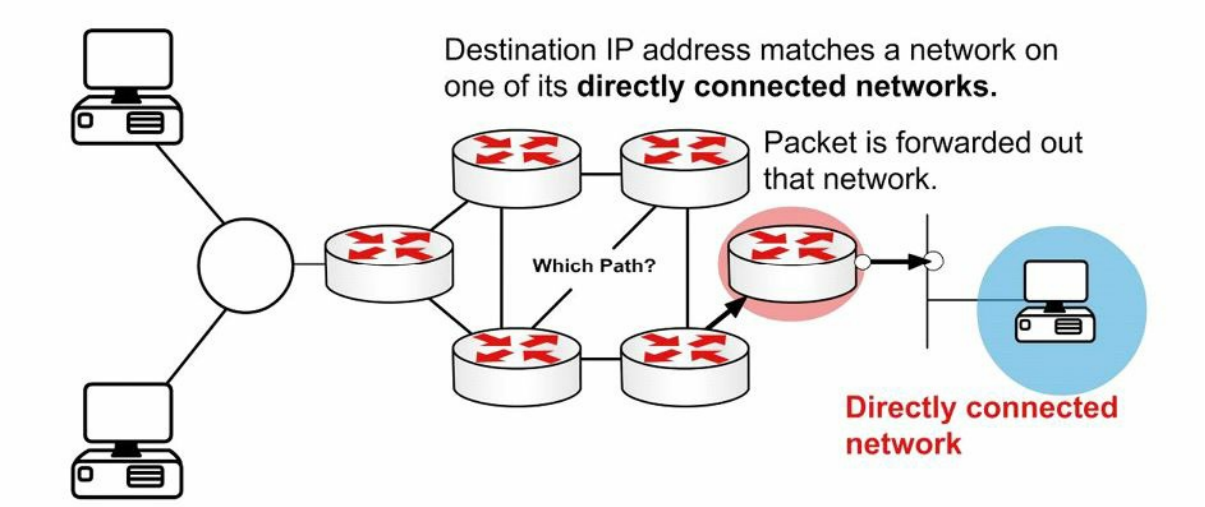


Figure 10.1 – Directly Connected Networks

If the packet is destined for a remote network, the routing table is checked and if there is a route or default route, the packet is forwarded to the next-hop router, as shown in Figure 10.2 below:

https://t.me/learningnets

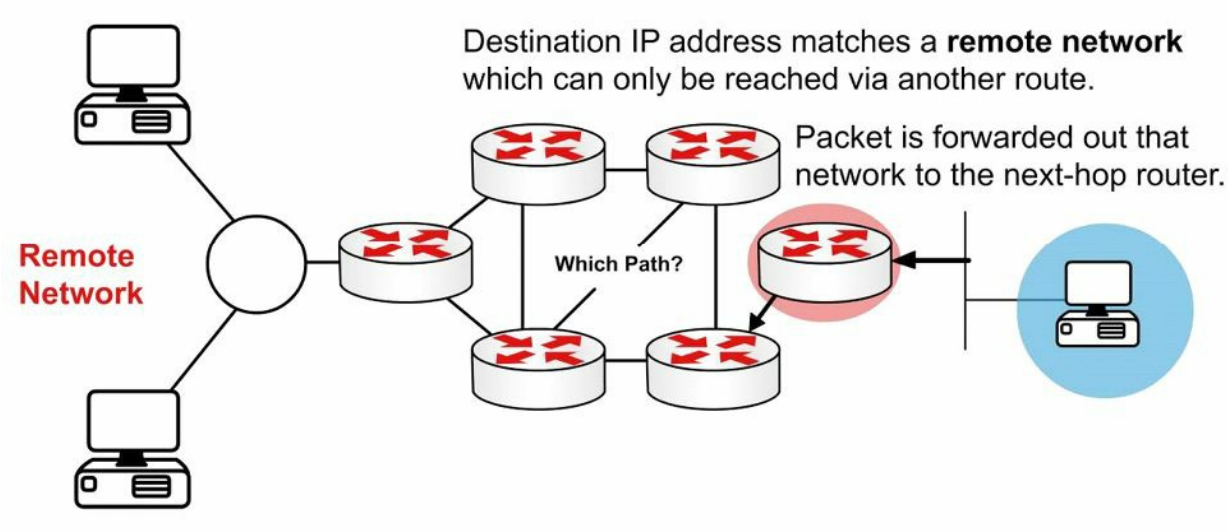


Figure 10.2 – Remote Networks

If the packet is destined for a network not in the routing table and no default route exists then it is dropped, as shown in Figure 10.3 below:

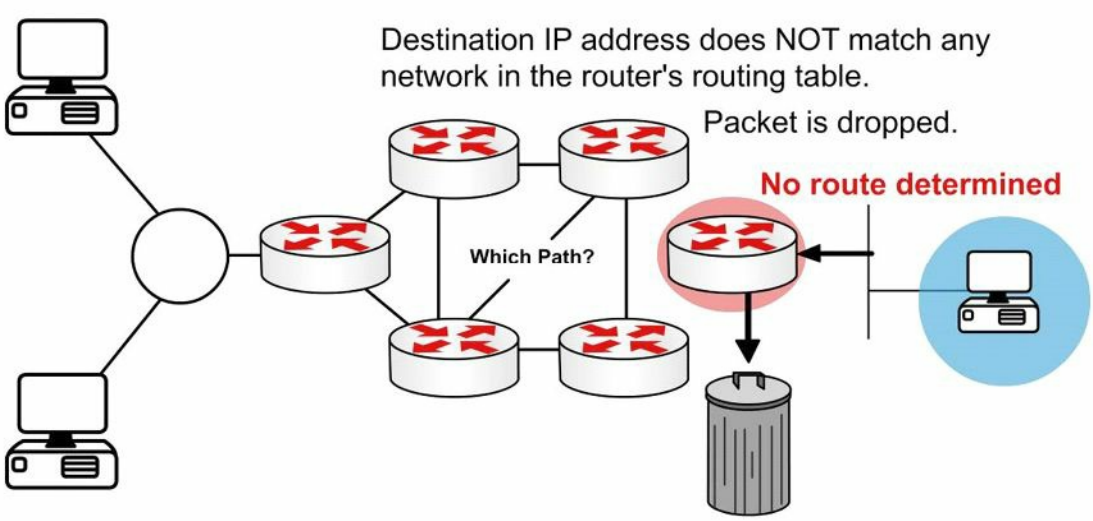


Figure 10.3 – No Route

The switching process allows the router to accept the packet via one interface and send it out of another. The router will also encapsulate the packet in the appropriate Data Link frame for the outgoing link.

You may be asked to explain what happens with a packet received from one network and destined for another network. Firstly, the router decapsulates the Layer 3 packet by removing the Layer 2 frame header and trailer. Next, it examines the destination IP address of the IP packet to find the best path in the routing table. Finally, it encapsulates the Layer 3 packet into a new Layer 2 frame and forwards the frame out of the exit interface, so the encapsulation could change from Ethernet to HDLC. This is illustrated in Figure 10.4 below:

https://t.me/learningnets

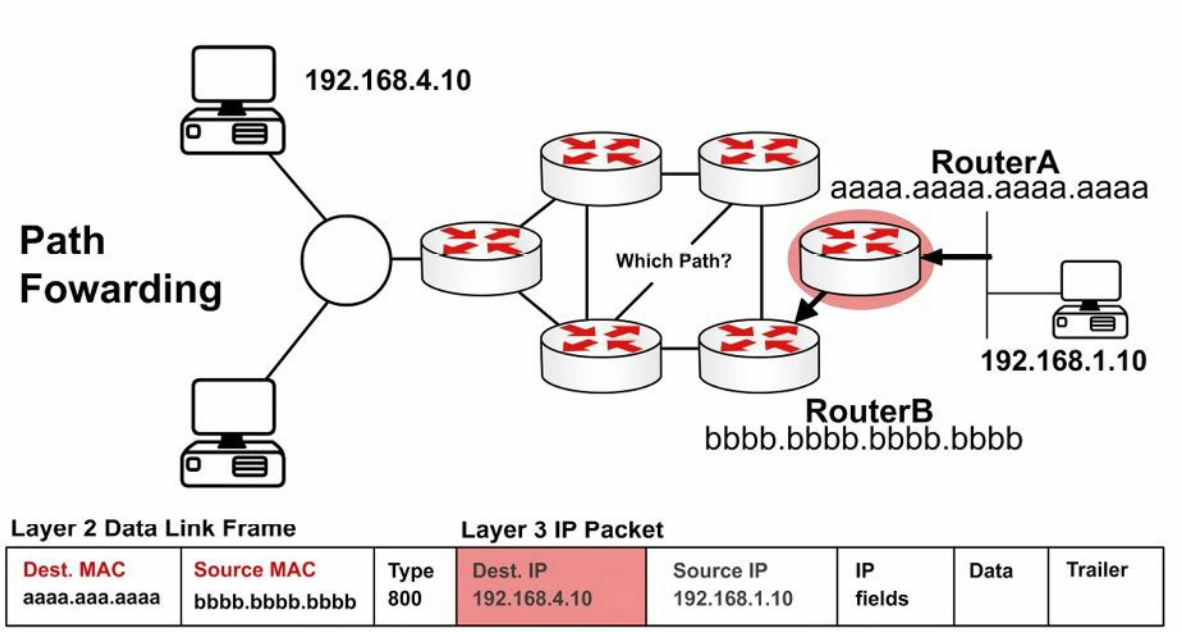


Figure 10.4 – Layer 3 Address in a Packet

Remember in an earlier module that the source and destination IP address will never change as the packet traverses towards its final destination. The MAC address, however, will change to permit transport between intermediary devices. This is illustrated in Figure 10.5 below:

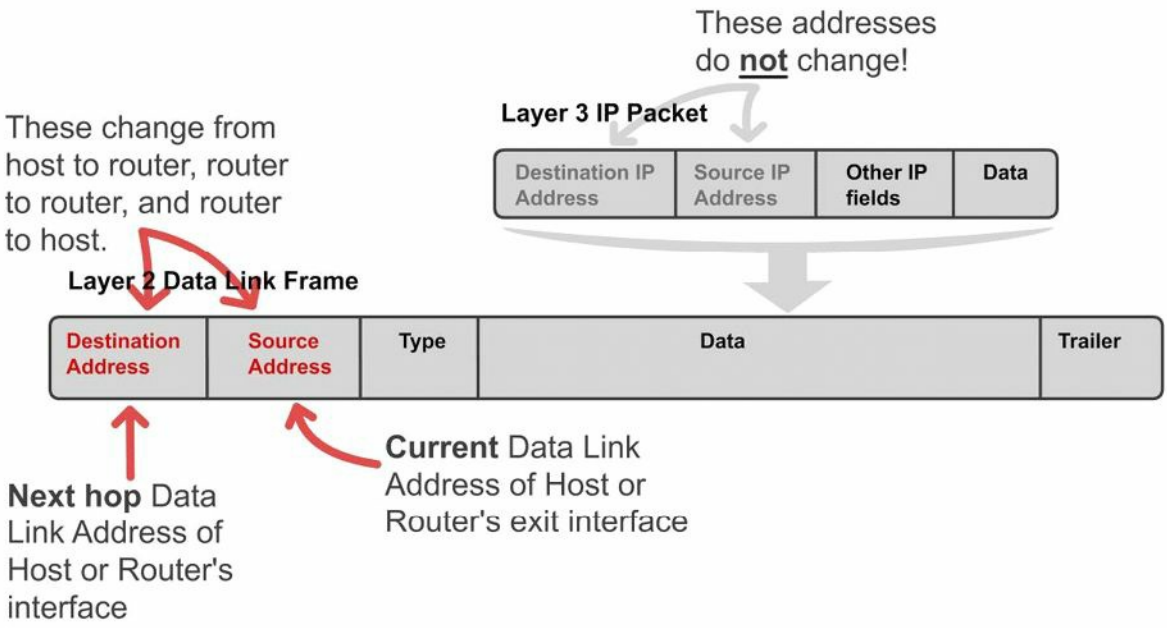


Figure 10.5 – Layer 2 Address Changes

Figure 10.6 shows a packet leaving Host X destined for Host Y. Note that the next-hop MAC address belongs to Router A (using proxy ARP); however, the IP address belongs to Host Y. When the frame reaches Router B, the Ethernet header and trailer will be exchanged for the WAN protocol, which you can presume is HDLC here.

https://t.me/learningnets

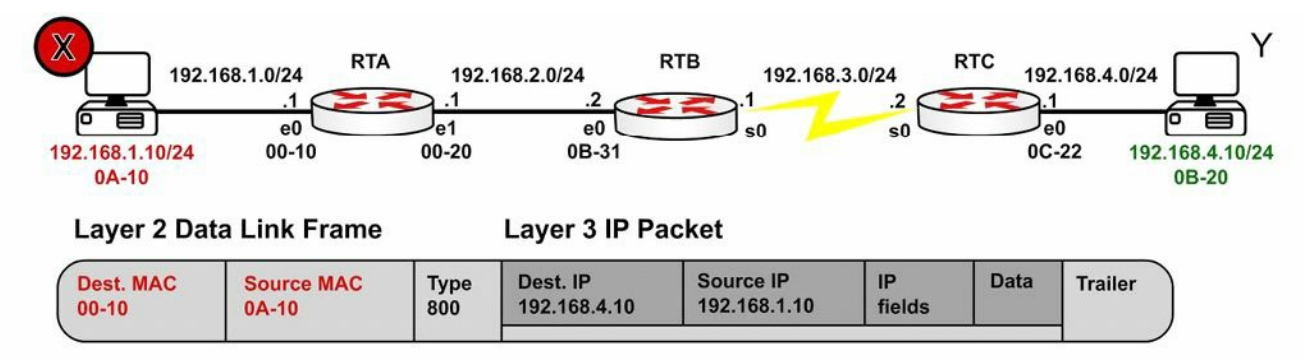


Figure 10.6 – Packet Leaving Host X

Figure 10.7 shows the same packet leaving Router A for Router B. There is a route lookup and then the packet is switched out of interface E1. Type 800 indicates that the packet is IPv4.

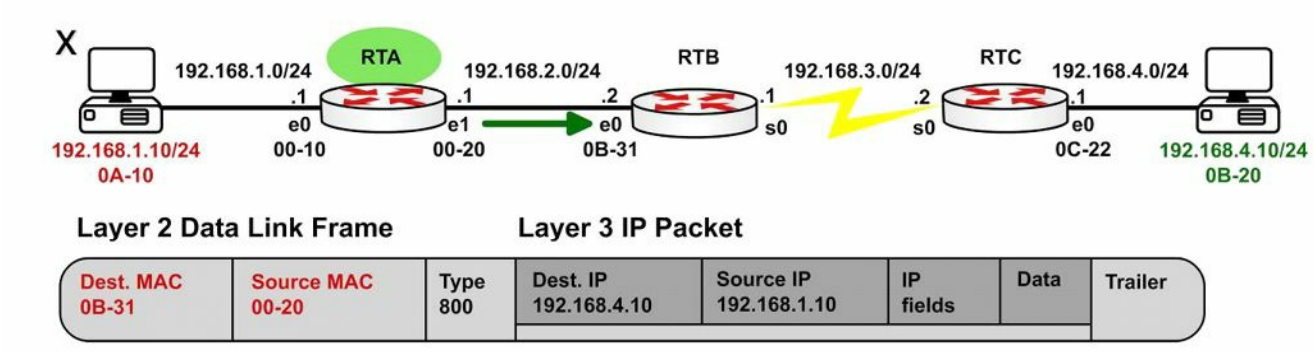


Figure 10.7 – Packet Leaving Router A

Figure 10.8 shows that the frame eventually reaches Router C and is forwarded to Host Y:

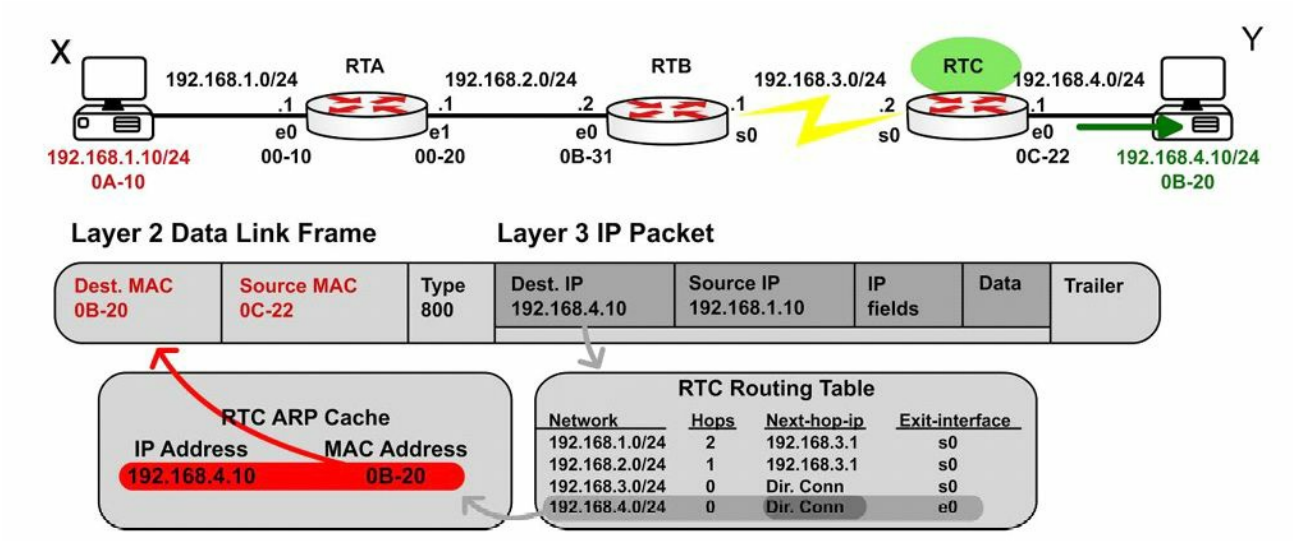


Figure 10.8 – Packet Leaving Router C

Internet Protocol Routing Fundamentals

A routing protocol allows a router to learn dynamically how to reach other networks. A routing protocol also allows the router to exchange learned network information with other routers or hosts. Routing protocols may be used for connecting interior (internal) campus networks, as well as for connecting different enterprises or routing domains. Therefore, in addition to understanding the intricacies of routing protocols, it is also important to have a solid understanding of when and in what situation one routing protocol would be used versus

https://tinglearnments

another.

Flat and Hierarchical Routing Algorithms

Routing protocol algorithms operate using either a flat routing system or a hierarchical routing system. A hierarchical routing system uses a layered approach wherein routers are placed in logical groupings referred to as domains, areas, or autonomous systems. This allows different routers within the network to perform specific tasks, optimising the functionality performed at those layers. Some routers in the hierarchical system can communicate with other routers in other domains or areas, while other routers can communicate only with routers in the same domain or area. This reduces the amount of information that routers in the domain or area must process, which allows for faster convergence within the network.

A flat routing system has no hierarchy. In such systems, routers must typically be connected to every other router in the network and each router essentially has the same function. Such algorithms work well in very small networks; however, they are not scalable. In addition, as the network grows, troubleshooting becomes much more difficult because instead of just focusing your efforts on certain areas, for example, you now have to look at the entire network.

The primary advantage afforded by hierarchical routing systems is their scalability. Hierarchical routing systems also allow for easier changes to the network, in much the same way afforded by the traditional hierarchical design comprised of the Core, Distribution, and Access Layers. In addition, hierarchical algorithms can be used to reduce routing update traffic, as well as routing table size, in certain areas of the network while still allowing full network connectivity.

IP Addressing and Address Summarisation

An IP address is divided into two parts. The first part designates the network address, while the second part designates the host address. When designing a network, an IP addressing scheme is used to uniquely identify hosts and devices within the network. The IP addressing scheme should be hierarchical and should build on the traditional logical hierarchical model. This allows the addressing scheme to provide designated points in the network where effective route summarisation can be performed.

Summarisation reduces the amount of information that routers must process, which allows for faster convergence within the network. Summarisation also restricts the size of the area that is affected by network changes by hiding detailed topology information from certain areas within the network. This concept is illustrated in Figure 10.9 below:

https://t.me/learningnets

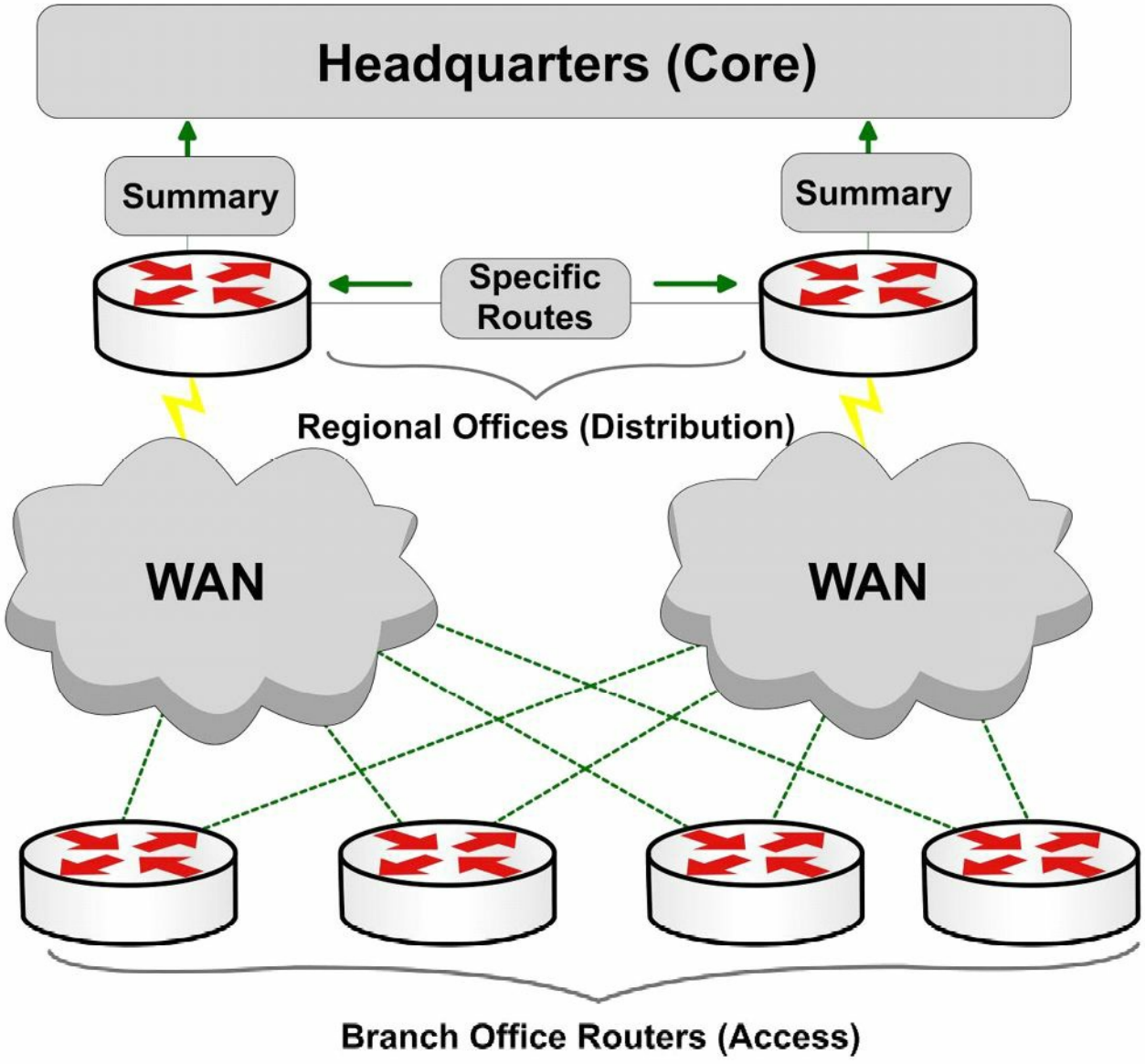


Figure 10.9 – Route Summarisation Using Cisco Design Model

Referencing Figure 10.9, the branch offices (Access Layer) are dual-homed to the regional office routers (Distribution Layer). Layers are defined using Cisco design models. Using a hierarchical addressing scheme allows the Distribution Layer routers to advertise a summary route for the branch office subnets to the Core Layer. This protects the Core Layer from the effects of any route flapping between the Distribution and the Access Layer routers, because a summary route will not flap until every last one of the more specific prefixes from which it is derived is removed from the routing table. This increases stability within the area. In addition, the routing table size at the Core Layer is further reduced.

Administrative Distance

Administrative distance is used to determine the reliability of one source of routing information from another. Some sources are considered more reliable than others are; therefore, administrative distance can be used to determine the best or preferred path to a destination network or network node when there are two or more different paths to the same destination from two or more different routing protocols.

In Cisco IOS software, all sources of routing information are assigned a default administrative distance value. This default value is an integer between 0 and 255, with a value of 0 assigned to

https://t.me/learningnets

the most reliable source of information and a value of 255 assigned to the least reliable source of information. Any routes that are assigned an administrative distance value of 255 are considered untrusted and will not be placed into the routing table.

The administrative distance is a locally significant value that affects only the local router. This value is not propagated throughout the routing domain. Therefore, manually adjusting the default administrative distance for a routing source or routing sources on a router affects the preference of routing information sources only on that router. Table 10.1 below shows the default administrative values used in Cisco IOS software (you need to learn these for the exam):

Table 10.1 – Router Administrative Distances (ADs)

Route Source	AD
Connected Interfaces	0
Static Routes	1
Enhanced Interior Gateway Routing Protocol (EIGRP) Summary Routes	5
External Border Gateway Protocol (eBGP) Routes	20
Internal Enhanced Interior Gateway Routing Protocol (EIGRP) Routes	90
Open Shortest Path First (OSPF) Internal and External Routes	110
Intermediate System-to-Intermediate System (IS-IS) Internal and External Routes	115
Routing Information Protocol (RIP) Routes	120
Exterior Gateway Protocol (EGP) Routes	140
On-Demand Routing (ODR) Routes	160
External Enhanced Interior Gateway Routing Protocol (EIGRP) Routes	170
Internal Border Gateway Protocol (iBGP) Routes	200
Unreachable or Unknown Routes	255

The default route source administrative distance is displayed in the output of the `show ip protocols` command. This is illustrated in the following output:

```
R1#show ip protocols
Routing Protocol is "isis"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: isis
  Address Summarization:
    None
  Maximum path: 4
  Routing for Networks:
    Serial0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.0.0.2             115      00:06:53
  Distance: (default is 115)
```

Routing protocol algorithms use metrics, which are numerical values that are associated with specific routes. These values are used to prioritise or prefer routes learned by the routing protocol, from the most preferred to the least preferred. In essence, the lower the route metric, the more preferred the route by the routing protocol. The route with the lowest metric is typically the route with the least cost or the best route to the destination network. This route will be placed into the routing table and will be used to forward packets to the destination network.

Different routing algorithms use different variables to compute the route metric. Some routing algorithms use only a single variable, while other advanced routing protocols may use more than one variable to determine the metric for a particular route. In most cases, the metrics that are computed by one routing protocol are incompatible with those used by other routing protocols. The different routing protocol metrics may be based on one or more of the following:

- Bandwidth
- Cost
- Delay
- Load
- Path length
- Reliability

Bandwidth

The term bandwidth refers to the amount of data that can be carried from one point to another in a given period. Routing algorithms may use bandwidth to determine which link type is preferred over another. For example, a routing algorithm might prefer a GigabitEthernet link to a FastEthernet link because of the increased capacity of the GigabitEthernet link over the FastEthernet link.

In Cisco IOS software, the `bandwidth` interface configuration command can be used to adjust the default bandwidth value for an interface, effectively manipulating the selection of one interface against another by a routing algorithm. For example, if the FastEthernet interface was configured with the `bandwidth 1000000` interface configuration command, both the FastEthernet and the GigabitEthernet links would appear to have the same capacity to the routing algorithm and would be assigned the same metric value. The fact that one of the links is actually a FastEthernet link while the other is actually a GigabitEthernet link is irrelevant to the routing protocol.

From a network administrator's point of view, it is important to understand that the `bandwidth` command does not affect the physical capability of the interface (so it is sometimes referred to as a cosmetic command). In other words, configuring the higher bandwidth on the FastEthernet interface does not mean that it is capable of supporting GigabitEthernet speeds. Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) use bandwidth in

https://t.me/learningnets

metric calculations.

Cost

The cost, as it pertains to routing algorithms, refers to communication cost. The cost may be used when, for example, a company prefers to route across private links rather than public links that include monetary charges for sending data across them or for the usage time. Intermediate System-to-Intermediate System (IS-IS) supports an optional expense metric that measures the monetary cost of link utilisation. Configuring cost varies depending upon the protocol.

Delay

There are many types of delay, all of which affect different types of traffic. In general, delay refers to the length of time required to move a packet from its source to its destination through the internetwork. In Cisco IOS software, the interface delay value is in microseconds (µs).

The interface value is configured using the `delay` interface configuration command. When you configure the interface delay value, it is important to remember that this does not affect traffic (another cosmetic command). For example, configuring a delay value of 5000 does not mean that traffic sent out of that interface will have an additional delay of 5000 µs. Table 10.2 below shows the default delay values for common interfaces in Cisco IOS software:

Table 10.2 – Interface Delay Values

Interface Type	Delay (µs)
10Mbps Ethernet	1000
FastEthernet	100
GigabitEthernet	10
T1 Serial	20000

EIGRP uses the interface delay value as part of its metric calculation. Manually adjusting the interface delay value results in the re-computation of the EIGRP metric.

Load

The term load means different things to different people. For example, in general computing terminology, load refers to the amount of work a resource, such as the CPU, is performing. Load, as it applies in this context, refers to the degree of use for a particular router interface. The load on the interface is a fraction of 255. For example, a load of 255/255 indicates that the interface is completely saturated, while a load of 128/255 indicates that the interface is 50% saturated. By default, the load is calculated as an average over a period of five minutes (in the real world this is often changed to a minimum of 30 seconds using the `load-interval 30` command). The interface load value can be used by EIGRP in its metric calculation.

Path Length

https://t.me/learningnets

The path length metric is the total length of the path that is traversed from the local router to

the destination network. Different routing algorithms represent this in different forms. For example, Routing Information Protocol (RIP) counts all intermediate routers (hops) between the local router and the destination network and uses the hop count as the metric, while Border Gateway Protocol (BGP) counts the number of traversed autonomous systems between the local router and the destination network and uses the autonomous system count to select the best path.

Reliability

Like load, the term reliability means different things depending upon the context in which it is used. Here, unless stated otherwise, it should always be assumed that reliability refers to the dependability of network links or interfaces. In Cisco IOS software, the reliability of a link or interface is represented as a fraction of 255. For example, a reliability value of 255/255 indicates that the interface is 100% reliable. Similar to the interface load, by default the reliability of an interface is calculated as an average over a period of five minutes.

Prefix Matching

Cisco routers use the longest prefix match rule when determining which of the routes placed into the routing table should be used to forward traffic to a destination network or node. Longer, or more specific, routing table entries are preferred over less specific entries, such as summary addresses, when determining which entry to use to route traffic to the intended destination network or node.

The longest prefix or the most specific route will be used to route traffic to the destination network or node, **regardless of the administrative distance of the route source**, or even the routing protocol metric assigned to the prefix if multiple overlapping prefixes are learned via the same routing protocol. Table 10.3 below illustrates the order of route selection on a router sending packets to the address 1.1.1.1. This order is based on the longest prefix match lookup:

Table 10.3 – Matching the Longest Prefix

Routing Table Entry	Order Used
1.1.1.1/32	First
1.1.1.0/24	Second
1.1.0.0/16	Third
1.0.0.0/8	Fourth
0.0.0.0/0	Fifth

NOTE: Although the default route is listed last in the route selection order in Table 10.3, keep in mind that a default route is not always present in the routing table. If that is the case, and no other entries to the address 1.1.1.1 exist, packets to that destination are simply discarded by the router. In most cases, the router will send the source host an ICMP message indicting that the destination is unreachable. A default route is used to direct packets addressed to networks not explicitly listed in the routing table.

Building the IP Routing Table

Without a populated routing table, or Routing Information Base (RIB), that contains entries for

https://t.me/learningnets

remote networks, routers will not be able to forward packets to those remote networks. The routing table may include specific network entries or simply a single default route. The information in the routing table is used by the forwarding process to forward traffic to the destination network or host. The routing table itself does not actually forward traffic.

Cisco routers use the administrative distance, the routing protocol metric, and the prefix length to determine which routes will actually be placed into the routing table, which allows the router to build the routing table. The routing table is built via the following general steps:

1. If the route entry does not currently exist in the routing table, add it to the routing table.
2. If the route entry is more specific than an existing route, add it to the routing table. It should also be noted that the less specific entry is still retained in the routing table.
3. If the route entry is the same as an existing one, but it is received from a more preferred route source, replace the old entry with the new entry.
4. If the route entry is the same as an existing one, and it is received from the same protocol, then:
    i. Discard the new route if the metric is higher than the existing route; or
    ii. Replace the existing route if the metric of the new route is lower; or
    iii. Use both routes for load balancing if the metric for both routes is the same.

When building the RIB by default, the routing protocol with the lowest administrative distance value will always be chosen when the router is determining which routes to place into the routing table. For example, if a router receives the 10.0.0.0/8 prefix via external EIGRP, OSPF, and internal BGP, the OSPF route will be placed into the routing table. If that route is removed or is no longer received, the external EIGRP route will be placed into the routing table. Finally, if both the OSPF and the external EIGRP routes are no longer present, the internal BGP route is used.

Once routes have been placed into the routing table, by default the most specific or longest match prefix will always be preferred over less specific routes. This is illustrated in the following example, which shows a routing table that contains entries for the 80.0.0.0/8, 80.1.0.0/16, and 80.1.1.0/24 prefixes. These three route prefixes are received via the EIGRP, OSPF, and RIP routing protocols, respectively.

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
R       80.1.1.0/24 [120/1] via 10.1.1.2, 00:00:04, Ethernet0/0.1
```

https://t.me/learningnets

```
D       80.0.0.0/8 [90/281600] via 10.1.1.2, 00:02:02, Ethernet0/0.1
O E2    80.1.0.0/16 [110/20] via 10.1.1.2, 00:00:14, Ethernet0/0.1
```

Referencing the output shown above, the first route is 80.1.1.0/24. This route is learned via RIP and therefore has a default administrative distance value of 120. The second route is 80.0.0.0/8. This route is learned via internal EIGRP and therefore has a default administrative distance value of 90. The third route is 80.1.0.0/16. This route is learned via OSPF and is an external OSPF route that has an administrative distance of 110.

NOTE: Because the routing protocol metrics are different, they are a non-factor in determining the best route to use when routes from multiple protocols are installed into the routing table. The following section will describe how Cisco IOS routers build the routing table.

Based on the contents of this routing table, if the router received a packet destined to 80.1.1.1, it would use the RIP route because this is the most specific entry, even though both EIGRP and OSPF have better administrative distance values and are therefore more preferred route sources. The `show ip route 80.1.1.1` command illustrated below can be used to verify this statement:

```
R1#show ip route 80.1.1.1
Routing entry for 80.1.1.0/24
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Last update from 10.1.1.2 on Ethernet0/0.1, 00:00:15 ago
  Routing Descriptor Blocks:
  * 10.1.1.2, from 10.1.1.2, 00:00:15 ago, via Ethernet0/0.1
      Route metric is 1, traffic share count is 1
```

Classful and Classless Protocols

Classful protocols can't use VLSM (i.e., RIPv1 and IGRP, which are no longer in the CCNA syllabus). This is because they don't recognise anything other than default network masks:

```
Router#debug ip rip
RIP protocol debugging is on
01:26:59: RIP: sending v1 update to 255.255.255.255 via Loopback0
192.168.1.1
```

Classless protocols use VLSM (i.e., RIPv2 and EIGRP):

```
Router#debug ip rip
RIP protocol debugging is on
01:29:15: RIP: received v2 update from 172.16.1.2 on Serial0
01:29:15:192.168.2.0/24 via 0.0.0.0
```

Passive Interfaces

An important routing protocol design and configuration consideration is to limit unnecessary peerings, as shown in Figure 10.10 below. This is done using passive interfaces, which prevents the router from forming routing adjacencies on the specific interface. This functions differently based on the specific routing protocol used but the behaviour usually falls within the following two categories:

https://t.me/learningnets

- The router does not send routing updates on the passive interface
- The router does not send Hello packets on the interface, so neighbour relationships are not formed

Passive interfaces are usually able to receive routing updates or Hello packets but are not allowed to send any kind of routing protocol information outbound.

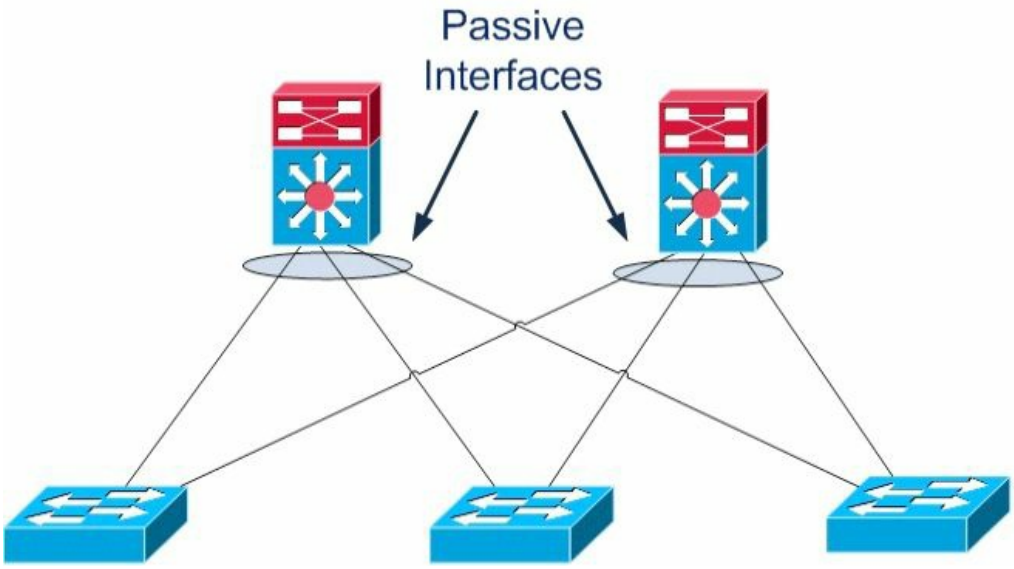


Figure 10.10 – Limit Unnecessary Peerings

A use case example for passive interfaces is avoiding routing protocol peerings from the Distribution Layer to the Access Layer, as presented in Figure 10.10 above. By having Layer 3 peering across the different Access Layer switches (i.e., having multiple hosts on different switches across switch blocks) you are basically adding memory load, routing protocol update overhead, and more complexity. Also, if there is a link failure, the traffic may transit through a neighbouring Access Layer switch to get to another VLAN member.

Basically, you want to eliminate unnecessary routing peering adjacencies, so you would configure the ports towards the Layer 2 switches as passive interfaces in order to suppress routing updates advertisements. If a Distribution Layer switch does not receive a routing update from a potential peer on one of these interfaces, it will not have to process the updates and will not form a neighbour adjacency across that interface. The command for accomplishing this is usually `passive-interface [interface number]` in the Routing Process Configuration mode. Please read a CCDA guide for more information on the Cisco design model.

Routing Protocol Classes

There are two major classes of routing protocols – Distance Vector and Link State. Distance Vector routing protocols traditionally use a one-dimensional vector when determining the most optimal path(s) through the network, while Link State routing protocols use the Shortest Path First (SPF) when determining the most optimal path(s) through the network. Before delving into the specifics of these two classes of routing protocols, we will first take a look at vectors, as well as at the elusive SPF algorithm.

Understanding Vectors

https://t.me/learningnets

A one-dimensional vector is a directed quantity. It is simply a quantity (number) in a particular direction or course. The vector concept is illustrated in Figure 10.11 below:

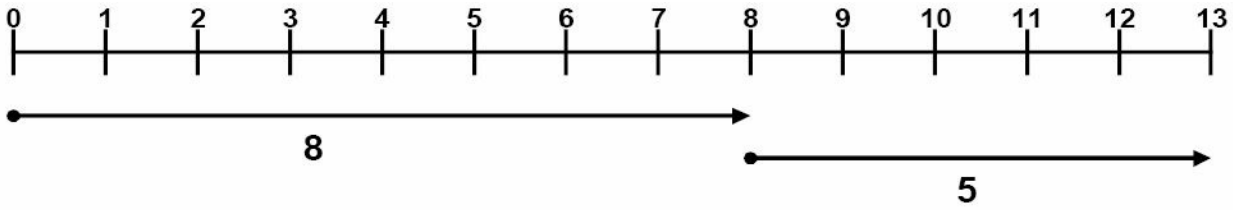


Figure 10.11 – Understanding Vectors

Referencing Figure 10.11, the first line starts at 0 and ends at 8, and the second line begins at 8 and ends at 13. The vector for the first line is 8, while the vector for the second line is 5. Using basic math, we know that 8 + 5 = 13. The starting and ending points of the vector are not relevant. Instead, the only thing that actually matters is how long the vector is and how far it travels.

NOTE: Vectors can also travel in the opposite direction (i.e., they represent negative numbers).

The Shortest Path First Algorithm

The SPF algorithm creates a shortest-path tree to all hosts in an area or in the network backbone with the router that is performing the calculation at the root of that tree. In order for the SPF algorithm to work in the correct manner, all routers in the area should have the same database information. In OSPF, this is performed via the database exchange process.

Distance Vector Routing Protocols

Distance Vector is a routing protocol that uses distance or hop count as its primary metric for determining the best forwarding path. Distance Vector routing protocols are primarily based on the Bellman-Ford algorithm. Distance Vector routing protocols periodically send their neighbour routers copies of their entire routing tables to keep them up to date on the state of the network. While this may be acceptable in a small network, it increases the amount of traffic that is sent across networks as the size of the network grows. All Distance Vector routing protocols share the following characteristics:

- Counting to infinity
- Split horizon
- Poison reverse
- Hold-down timers

Utilising the counting to infinity characteristic, if a destination network is farther than the maximum number of hops allowed for that routing protocol, the network would be considered unreachable. The network entry would therefore not be installed into the IP routing table.

Split horizon mandates that routing information cannot be sent back out of the same interface through which it was received. This prevents the re-advertising of information back to the source from which it was learned. While this characteristic is a great loop prevention mechanism, it is also a significant drawback, especially in hub-and-spoke networks.

https://t.me/learningnets

Poison reverse (or route poisoning) expands on split horizon. When used in conjunction with split horizon, poison reverse allows the networks to be advertised back out of the same interface on which they were received. However, poison reverse causes the router to advertise these networks back to the sending router with a metric of “unreachable” so that the router that receives those entries will not add them back into its routing table.

Hold-down timers are used to prevent networks that were previously advertised as down from being placed back into the routing table. When a router receives an update that a network is down, it begins its hold-down timer. This timer tells the router to wait for a specific amount of time before accepting any changes to the status of that network.

During the hold-down period, the router suppresses the network and prevents advertising false information. The router also does not route to the unreachable network, even if it receives information from another router (that may not have received the triggered update) that the network is reachable. This mechanism is designed to prevent black-holing traffic.

The two most common Distance Vector routing protocols are RIP and IGRP. EIGRP is an advanced Distance Vector routing protocol, using features from both Distance Vector and Link State (i.e., it’s a hybrid protocol).

Link State Routing Protocols

Link State routing protocols are hierarchical routing protocols that use the concept of areas to logically group routers within a network. This allows Link State protocols to scale better and operate in a more efficient manner than Distance Vector routing protocols. Routers running Link State routing protocols create a database that comprises the complete topology of the network. This allows all routers within the same area to have the same view of the network.

Because all routers in the network have the same view of the network, the most optimal paths are used for forwarding packets between networks and the possibility of routing loops is eliminated. Therefore, techniques such as split horizon and route poisoning do not apply to Link State routing protocols as they do to Distance Vector routing protocols.

Link State routing protocols operate by sending Link State Advertisements or Link State Packets to all other routers within the same area. These packets include information on attached interfaces, metrics, and other variables. As the routers accumulate this information, they run the SPF algorithm and calculate the shortest (best) path to each router and destination network. Using the received Link State information, routers build the Link State Database (LSDB). When the LSDBs of two neighbouring routers are synchronised, the routers are said to be adjacent.

Unlike Distance Vector routing protocols, which send their neighbours their entire routing table, Link State routing protocols send incremental updates when a change in the network topology is detected, which makes them more efficient in larger networks. The use of incremental updates also allows Link State routing protocols to respond much faster to network changes and thus converge in a shorter amount of time than Distance Vector routing protocols. Table 10.4 below lists the different Interior Gateway Protocols (IGPs) and their classification:

https://t.me/learningnets

Table 10.4 – IGP Classification

Protocol Name	Classful/Classless	Protocol Classification
RIP (version 1)	Classful	Distance Vector
IGRP	Classful	Distance Vector
RIP (version 2)	Classless	Distance Vector
EIGRP	Classless	Advanced Distance Vector
IS-IS	Classless	Link State
OSPF	Classless	Link State

The Objectives of Routing Protocols

Routing algorithms, while different in nature, all have the same basic objectives. While some algorithms are better than others are, all routing protocols have their advantages and disadvantages. Routing algorithms are designed with the following objectives and goals:

- Optimal routing
- Stability
- Ease of use
- Flexibility
- Rapid convergence

Optimal Routing

One of the primary goals of all routing protocols is to select the most optimal path through the network from the source subnet or host to the destination subnet or host. The most optimal route depends upon the metrics used by the routing protocols. A route that may be considered the best by one protocol may not necessarily be the most optimal route from the perspective of another protocol. For example, RIP might consider a path that is only two hops long as the most optimal path to a destination network, even though the links were 64Kbps links, while advanced protocols such as OSPF and EIGRP might determine that the most optimal path to that same destination is the one traversing four routers but using 10Gbps links.

Stability

Network stability, or a lack thereof, is another major objective for routing algorithms. Routing algorithms should be stable enough to accommodate unforeseen network events, such as hardware failures and even incorrect implementations. While this is typically a characteristic of all routing algorithms, the manner and time in which they respond to such events makes some better than others and thus more preferred in modern-day networks.

Ease of Use

Routing algorithms are designed to be as simple as possible. In addition to providing the capability to support complex internetwork deployments, routing protocols should take into

https://t.me/learningnets

consideration the resources required to run the algorithm. Some routing algorithms require more hardware or software resources (e.g., CPU and memory) to run than others do; however, they are capable of providing more functionality than alternative simple algorithms.

Flexibility

In addition to providing routing functionality, routing algorithms should also be feature-rich, allowing them to support the different requirements encountered in different networks. It should be noted that this capability typically comes at the expense of other features, such as convergence, which is described next.

Rapid Convergence

Rapid convergence is another primary objective of all routing algorithms. As stated earlier, convergence occurs when all routers in the network have the same view of and agree on optimal routes. When convergence takes a long time to occur, intermittent packet loss and loss of connectivity may be experienced between remote networks. In addition to these problems, slow convergence can result in network routing loops and outright network outages.

Routing Problems Avoidance Mechanisms

It is a known fact that Distance Vector routing protocols are prone to major problems as a result of their simplistic “routing by rumor” approach. Distance Vector and Link State protocols use different techniques to prevent routing problems. The most important mechanisms include the following:

- **Invalidation timers:** These are used to mark routes as unreachable when updates for those routes are not received for a long time.
- **Hop count limit:** This parameter marks routes as unreachable when they are more than a predefined number of hops away. The hop count limit for RIP is 15, as it is not usually used in large networks. Unreachable routes are not installed in the routing table as best routes. The hop count limit prevents updates from looping in the network, just like the TTL field in the IP header.
- **Triggered updates:** This feature allows the update timer to be bypassed in the case of important updates. For example, the RIP 30-second timer can be ignored if a critical routing update must be propagated through the network.
- **Hold-down timers:** If a metric for a particular route keeps getting worse, updates for that route are not accepted for a delayed period.
- **Asynchronous updates:** Asynchronous updates represent another safety mechanism that prevents the routers from flooding the entire routing information at the same time. As mentioned before, OSPF does this every 30 minutes. The asynchronous updates mechanism generates a small delay for every device so they do not flood the information exactly at the same time. This improves bandwidth utilisation and processing capabilities.
- **Route poisoning:** This feature prevents routers from sending packets through a route that has become invalid. Distance Vector protocols use this to indicate that a route is no

https://t.me/learningnets

longer reachable. This is accomplished by setting the route metric to a maximum value.

- **Split horizon:** Split horizon prevents updates from being sent out of the same interface they came from because routers in that area should already know about that specific update.
- **Poison reverse:** This mechanism is an exception to the split horizon rule for the poisoned routes.

Topology-Based (CEF) Switching

Matching a packet's intended destination address with the IP routing table requires router CPU cycles. Enterprise routers can contain tens of thousands of entries and can match the same number of incoming packets against these entries. In an attempt to make this process as efficient as possible, Cisco has created various switching methods. The first is called process switching and it uses the route lookup and best match method already outlined. This method was improved upon with fast switching. A list of IP addresses of recently forwarded packets is generated by the router as well as the Data Link Layer headers that were copied if the IP address matched. Cisco Express Forwarding (CEF) was created as an improvement on fast switching. CEF runs on current models of Cisco routers by default.

Cisco Express Forwarding (CEF)

CEF operates at the data plane and is a topology-driven proprietary switching mechanism that creates a forwarding table that is tied to the routing table (i.e., the control plane). CEF was developed to eliminate the performance penalty experienced due to the first-packet process-switched lookup method used by flow-based switching. CEF eliminates this by allowing the route cache used by the hardware-based Layer 3 routing engine to contain all the necessary information to the Layer 3 switch in the hardware before any packets associated with a flow are even received. Information that is conventionally stored in a route cache is stored in two data structures for CEF switching. These data structures provide optimised lookup for efficient packet forwarding and are referred to as the FIB and the adjacency table.

NOTE: It is important to remember that even with CEF, whenever there are routing table changes, the CEF forwarding table is also updated. While new CEF entries are being created, packets are switched in a slower switching path, using process switching, for example. All current models of Cisco routers and current IOS use CEF.

Forwarding Information Base (FIB)

CEF uses a FIB to make IP destination prefix-based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. In other words, the FIB contains all IP prefixes from the routing table.

When routing or topology changes occur in the network, the IP routing table is updated, and those changes are also reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table. Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with switching paths, such as fast

https://t.me/learningnets

switching and optimum switching.

Additionally, because the FIB lookup table contains all known routes that exist in the routing table, it eliminates route cache maintenance and the fast-switching and process-switching forwarding scenarios. This allows CEF to switch traffic more efficiently than typical demand-caching schemes.

The Adjacency Table

The adjacency table was created to contain all connected next hops. An adjacent node is a node that is one hop away (i.e., directly connected). The adjacency table is populated as adjacencies are discovered. As soon as a neighbour becomes adjacent, a Data Link Layer header, called a MAC string or a MAC rewrite, which will be used to reach that neighbour, is created and stored in the table. On Ethernet segments, this header information is the destination MAC address, the source MAC address, and the EtherType, in that specific order.

As soon as a route is resolved, it points to an adjacent next hop. If an adjacency is found in the adjacency table, a pointer to the appropriate adjacency is cached in the FIB element. If multiple paths exist for the same destination, a pointer to each adjacency is added to the load-sharing structure, which allows for load balancing. When prefixes are added to the FIB, prefixes that require exception handling are cached with special adjacencies.

Accelerated and Distributed CEF

By default, all CEF-based Cisco Catalyst switches use a central Layer 3 switching engine where a single processor makes all Layer 3 switching decisions for traffic received on all ports in the switch. Even though the Layer 3 switching engines used in Cisco Catalyst switches provide high performance, in some networks, having a single Layer 3 switching engine do all the Layer 3 switching does not provide sufficient performance. To address this issue, Cisco Catalyst 6500 series switches allow for CEF optimisation through the use of specialised forwarding hardware. This is performed using either Accelerated CEF (aCEF) or Distributed CEF (dCEF).

Accelerated CEF allows a portion of the FIB to be distributed to capable line card modules in the Catalyst 6500 switch. This allows the forwarding decision to be made on the local line card using the locally stored scaled-down CEF table. In the event that FIB entries are not found in the cache, requests are sent to the Layer 3 engine for more FIB information.

Distributed CEF refers to the use of multiple CEF tables distributed across multiple line cards installed in the chassis. When using dCEF, the Layer 3 engine (MSFC) maintains the routing table and generates the FIB, which is then dynamically downloaded in full to each of the line cards, allowing for multiple Layer 3 data plane operations to be performed simultaneously.

In summation, dCEF and aCEF are technologies that implement multiple Layer 3 switching engines so that simultaneous Layer 3 switching operations can occur in parallel, boosting overall system performance. CEF technology offers the following benefits:

- Improved performance – CEF is less CPU-intensive than fast-switching route caching. More CPU processing power can be dedicated to Layer 3 services, such as Quality of Service (QoS) and encryption, for example.

https://t.me/learningnets

- Scalability – CEF offers full switching capacity at each line card in high-end platforms, such as the Catalyst 6500 series switches, when dCEF mode is active.
- Resilience – CEF offers an unprecedented level of switching consistency and stability in large dynamic networks. In dynamic networks, fast-switching cache entries are frequently invalidated due to routing changes. These changes can cause traffic to be process-switched using the routing table rather than fast-switched using the route cache.

Configuring Cisco Express Forwarding

Enabling CEF requires the use of a single command, which is the `ip cef [distributed]` global configuration command. The `[distributed]` keyword is only applicable to high-end switches, such as the Catalyst 6500 series switches, that support dCEF. The following output shows how to configure CEF on a lower-end platform, such as the Catalyst 3750 series switch:

```
VTP-Server-1(config)#ip cef
VTP-Server-1(config)#exit
```

The following output illustrates how to enable dCEF on the Catalyst 6500 series switches:

```
VTP-Server-1(config)#ip cef distributed
VTP-Server-1(config)#exit
```

NOTE: There is no explicit command to configure or enable aCEF.

Troubleshooting Routing Issues

When configuring routing on your network devices, you have to carefully configure static or dynamic routing based on the design. If you have a problem and are not able to send/receive traffic across the network, then you probably have some kind of configuration issue. When you initially set up a router there will most likely be some type of configuration problem that you will have to troubleshoot. If the router has been running for a while and you suddenly have a complete failure of traffic (no communication), you should analyse the situation and figure out whether the routing protocol functions as expected.

Sometimes certain routes might intermittently disappear and appear from the routing table, causing intermittent connectivity to specific destinations. This may be because a certain network area has some kind of communication problem and routers along the path propagate new routing information every time that area becomes accessible. This process is called “route flapping,” and the specific routes can be blocked so the entire network is not affected using a feature called “route dampening.”

NOTE: When using static routing, the routing table never changes so you will have no idea about problems that occur in different network areas.

When troubleshooting routing issues the standard approach is to follow the routing table for every route along the path. You might perform a traceroute to find out exactly where the packets are going and to see the routers along the path. This way you would know exactly which device might be causing the issues and you can start investigating the routing tables of

https://t.me/learningnets

the specific routers.

A common mistake when performing such a troubleshooting process is investigating the issue in a single direction (for example, source to destination). Instead, you should perform the troubleshooting in both directions because you might come across situations in which packets are blocked in a single direction and you have no return traffic from the destination to the source. The routing tables on devices along the path between two points should correctly point in both directions in order to ensure an optimal traffic flow.

Often you will be using connections provided by third parties, so when you want to troubleshoot issues in a certain area you should communicate with the provider and synchronise the troubleshooting effort. This includes sharing routing table information.

Using dynamic routing protocols makes the troubleshooting process easier because you can inspect the routing updates as they are sent and received by the router. This can be done via packet capture or internal device mechanisms and will help you to see how and when the routing table is populated. Having a topology map and other documentation that lists where every prefix is located in the network would further help your understanding of the routing updates and would shorten the troubleshooting process. The general idea in such a troubleshooting process is deciding which path a specific packet should take, based on the network design, and investigating where exactly it is deviating from this path.

Different tools can be used to monitor network devices. A common network management protocol used by these tools is Simple Network Management Protocol (SNMP), which was designed to query network devices for different parameters from a management station (SNMP is covered in ICND2). Besides the standard “health” parameters checked (e.g., CPU, memory, disk space, etc.), SNMP can also query the router for things like:

- Interface packet counters
- Used bandwidth and throughput
- CRC or other types of errors on device interfaces
- Routing table information

Other types of tools you can use are standard ping and traceroute utilities in order to verify end-to-end connectivity. They can also show relevant output that might help you determine the point in the network where problems occur.

The steps to troubleshooting almost all routing issues include the following:

- Verifying that routing is enabled
- Verifying that the routing table is valid
- Verifying the correct path selection

Verifying That Routing Is Enabled

The first step in troubleshooting routing is verifying that the routing protocol is enabled and properly configured. This can be done either by inspecting the current running configuration

https://t.me/tuanhs

(i.e., the `show run` command) or by using `show` commands associated with each particular routing protocol. Some of these options are listed below:

```
Router#show ip ospf ?
  <1-65535>            Process ID number
  border-routers       Border and boundary router information
  database             Database summary
  flood-list            Link state flood list
  interface            Interface information
  max-metric           Max-metric origination information
  mpls                 MPLS related information
  neighbor             Neighbor list
  request-list         Link state request list
  retransmission-list  Link state retransmission list
  rib                  Routing information base (RIB)
  sham-links           Sham link information
  statistics           Various OSPF Statistics
  summary-address      Summary-address redistribution information
  timers               OSPF timers information
  traffic               Traffic related statistics
  virtual-links        Virtual link information
  |                    Output modifiers
  <cr>
Router#show ip eigrp ?
  <1-65535>   Autonomous System
  accounting  IP-EIGRP accounting
  interfaces  IP-EIGRP interfaces
  neighbors   IP-EIGRP neighbors
  topology    IP-EIGRP topology table
  traffic      IP-EIGRP traffic statistics
  vrf         Select a VPN routing/forwarding instance
Router#show ip bgp ?
  A.B.C.D            Network in the BGP routing table to display
  A.B.C.D/nn         IP prefix <network>/<length>, e.g., 35.0.0.0/8
  all                All address families
  cidr-only          Display only routes with non-natural netmasks
  community          Display routes matching the communities
  community-list     Display routes matching the community-list
  dampening          Display detailed information about dampening
  extcommunity-list  Display routes matching the extcommunity-list
  filter-list        Display routes conforming to the filter-list
```

https://t.me/learningnets

```
  inconsistent-as    Display only routes with inconsistent origin ASs
  injected-paths     Display all injected paths
  ipv4               Address family
  ipv6               Address family
  labels             Display labels for IPv4 NLRI specific information
  neighbors          Detailed information on TCP and BGP neighbor connections
  nsap               Address family
  oer-paths          Display all oer controlled paths
  paths              Path information
  peer-group         Display information on peer-groups
  pending-prefixes    Display prefixes pending deletion
  prefix-list         Display routes matching the prefix-list
  quote-regexp       Display routes matching the AS path "regular expression"
  regexp             Display routes matching the AS path regular expression
  replication        Display replication status of update-group(s)
  rib-failure        Display bgp routes that failed to install in the routing table (RIB)
  route-map          Display routes matching the route-map
  summary            Summary of BGP neighbor status
  template           Display peer-policy/peer-session templates
  update-group       Display information on update-groups
  vpnv4              Address family
  |                  Output modifiers
  <cr>
```

Verifying That the Routing Table Is Valid

After successfully determining that the routing process is enabled, the next step is to analyse the routing table and see whether the information listed there is valid. Some of the points you should focus on include:

- Verifying that the correct prefixes are being learned via the correct routing protocol
- Verifying the number of learned prefixes
- Verifying route metrics and next-hop information

Depending on the routing protocol, you should also verify that the correct prefixes are being advertised outbound from your device.

Verifying the Correct Path Selection

After verifying that the relevant prefixes are indeed present in the routing table, you should carefully analyse their attributes and the path selection method for each of them. This might include:

- Verifying all the routing protocols that advertise that specific prefix (including static routing)

https://t.me/learningnets

- Comparing and manipulating the AD in order to prefer it over the correct routing protocol
- Verifying and adjusting protocol metrics

By properly configuring the router in your network, documenting each step along the way, and constantly monitoring the path between different points in the network, you will have a solid understanding of exactly how the traffic should traverse all the devices in the network.

https://t.me/learningnets

Day 10 Questions

1. What is a routing protocol?
2. _____ is used to determine the reliability of one source of routing information from another.
3. If a router learns a route from both EIGRP (internal) and OSPF, which one would it prefer?
4. What is the RIP AD?
5. What is the eBGP AD?
6. Name at least four routing metrics.
7. Once routes have been placed into the routing table, by default the most specific or longest match prefix will always be preferred over less specific routes. True or false?
8. _____ operates at the data plane and is a topology-driven proprietary switching mechanism that creates a forwarding table that is tied to the routing table (i.e., the control plane).
9. CEF uses a _____ to make IP destination prefix-based switching decisions.
10. Link State routing protocols are those that use distance or hop count as its primary metric for determining the best forwarding path. True or false?

https://t.me/learningnets

Day 10 Answers

1. A protocol that allows a router to learn dynamically how to reach other networks.
2. Administrative distance.
3. EIGRP.
4. 120.
5. 20.
6. Bandwidth, cost, delay, load, reliability, and hop count.
7. True.
8. CEF.
9. FIB.
10. False.

https://t.me/learningnets

Day 10 Lab

Routing Concepts Lab

Use two directly connected routers and test the basic commands depicted in this module. RIP is no longer in the CCNA exam but it's a very easy protocol to use for a simple lab.

- ☐ Assign an IPv4 address to the directy connected interfaces (10.10.10.1/24 and 10.10.10.2/24)
- ☐ Test direct connectivity using ping
- ☐ Configure a Loopback interface on each router and assign addresses from two different ranges (11.11.11.1/32 and 12.12.12.2/32)
- ☐ Configure standard RIP and advertise all the local networks

R1:

```
router rip
version 2
no auto
network 10.10.10.0
network 11.11.11.0
```

R2:

```
router rip
version 2
no auto
network 10.10.10.0
network 12.12.12.0
```

- ☐ Ping R2 Loopback from R1 to test connectivity
- ☐ Issue a `show ip route` command to verify that routes are being received via RIP
- ☐ Issue a `show ip protocols` command to verify that RIP is configured and active on the devices

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 11 – Static Routing

Day 11 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's lab
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website

Your choices as a network administrator are to use dynamic routing protocols on your network or stick to static routing, which is where you manually add each route for your network onto each router.

I'm often asked which routing protocol is the "best." There is no method which will suit every network, as even a particular company's network requirements will change over time. Static routing will take time and effort to configure, but you will save on network bandwidth and CPU cycles. If a new route is added, then you will have to add this manually to every router. In addition, if a route goes down, static routing has no method to deal with this, so it will continue to send traffic to the down network (reliable static routing is outside the CCNA syllabus).

Today you will learn about the following:

- Configuring static routes
- Troubleshooting static routes

This module maps to the following CCNA syllabus requirements:

- Configure and verify the routing configuration for a static or default route given specific routing requirements
- Differentiate methods of routing and routing protocols
    - Static vs. dynamic
    - Next hop

If you look back at the administrative distances table in Day 10, you will see that manually configured networks are preferred over routing protocols. The reason for this is, as a network administrator, you will be expected to know your network better than any protocol can and to understand what you want to achieve. By now, it should be clear that you can use static routing with dynamic routing if your needs require it.

Configuring Static Routes

The commands to configure a static route (see Figure 11.1 below) include the following:

https://t.me/learningnets

- `network address/prefix mask`

- `address` or `exit interface`
- `distance` (optional)

Here is an example of these commands in use:

```
RouterA(config)#ip route network prefix mask {address | interface} [distance]
```



Figure 11.1 – Sample Network for Static Routes

To add a static route for the network above, you would write the following line of configuration on the router on the left:

```
Router(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.2
```

With static routes, you can specify a next-hop IP address the router needs to go to on the way to the destination address, or you can specify an exit interface. Often, you won't know your next hop because it is your ISP, or your IP address will change over time (see Figure 11.2 below). If this is the case, use an exit interface.



Figure 11.2 – You Might Not Always Know Your Next-Hop Address

```
Router(config)#ip route 192.168.1.0 255.255.255.0 s0/0
```

The command line above tells the router to send traffic destined for the 192.168.1.0 network out of the Serial interface. The next command tells the router to send all traffic for all networks out of the Serial interface:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 s0/0
```

The route above is actually a default route. Default routes are used to direct packets addressed to networks not explicitly listed in the routing table.

Configuring Static IPv6 Routes

The configuration of static IPv6 routes follows similar logic to that of static IPv4 routes. In Cisco IOS software, the `ipv6 route [ipv6-prefix/prefix-length] [next-hop-address | interface] [distance <1-254> | multicast | tag | unicast]` global configuration command is used to configure static IPv6 routes. While the other keywords are familiar, because they are also applicable to IPv4 static routes, the `[multicast]` keyword is exclusive to IPv6 and is used to configure an IPv6 static Multicast route. If this keyword is used, the route will not be entered into the Unicast routing table and will never be used to forward Unicast traffic. To ensure that

https://t.me/learningdets

the route is never installed into the Unicast RIB, Cisco IOS software sets the administrative distance value for the route to 255.

Inversely, the `[unicast]` keyword is used to configure an IPv6 static Unicast route. If this keyword is used, the route will not be entered into the Multicast routing table and will be used only to forward Unicast traffic. If neither the `[multicast]` keyword nor the `[unicast]` keyword is used, by default, the route will be used for both Unicast and Multicast packets.

The following configuration example illustrates how to configure three static IPv6 routes. The first route, to subnet 3FFF:1234:ABCD:0001::/64, will forward traffic out of the FastEthernet0/0 interface. This route will be used only for Unicast traffic. The second route, to subnet 3FFF:1234:ABCD:0002::/64, will forward packets to that subnet out of Serial0/0 using the Link-Local address of the next-hop router as the IPv6 next-hop address. This route will be used only for Multicast traffic. Finally, a default route pointing out of interface Serial0/1 is also configured. This default route will forward packets to unknown IPv6 destinations via Serial0/1 using the Link-Local address of the next-hop router as the IPv6 next-hop address. These routes are illustrated below:

```
R1(config)#ipv6 route 3FFF:1234:ABCD:0001::/64 Fa0/0 unicast
R1(config)#ipv6 route 3FFF:1234:ABCD:0002::/64 Se0/0 FE80::2222 multicast
R1(config)#ipv6 route ::/0 Serial0/1 FE80::3333
```

Following this configuration, the `show ipv6 route` command can be used to verify the static route configuration implemented on the local router, as illustrated below:

```
R1#show ipv6 route static
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS inter area, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via FE80::3333, Serial0/1
S   3FFF:1234:ABCD:1::/64 [1/0]
     via ::, FastEthernet0/0
S   3FFF:1234:ABCD:2::/64 [1/0]
     via FE80::2222, Serial0/0
```

In addition to using the `show ipv6 route` command, the `show ipv6 static [prefix] [detail]` command can also be used to view detailed information about all or just specified static routes. The following output illustrates how to use this command:

```
R1#show ipv6 static 3FFF:1234:ABCD:1::/64 detail
IPv6 static routes
Code: * - installed in RIB
* 3FFF:1234:ABCD:1::/64, via interface FastEthernet0/0, distance 1
```

https://t.me/learningnets

Troubleshooting Static Routes

Troubleshooting will almost always involve a configuration issue (unless your interface is down). If traffic isn't arriving at the destination, you can test the route with the `traceroute` command or `tracert` command for a Windows PC.

NOTE – Today is a very short day so please move ahead to Day 12 because it's a very meaty subject.

https://t.me/learningnets

Day 11 Questions

1. Name the three parameters needed to configure a static route.
2. What is the command used to configure a static route?
3. What is the command used to configure a default static route?
4. What is the command used to configure an IPv6 static route?
5. What is the command used to view IPv6 static routes?

https://t.me/learningnets

Day 11 Answers

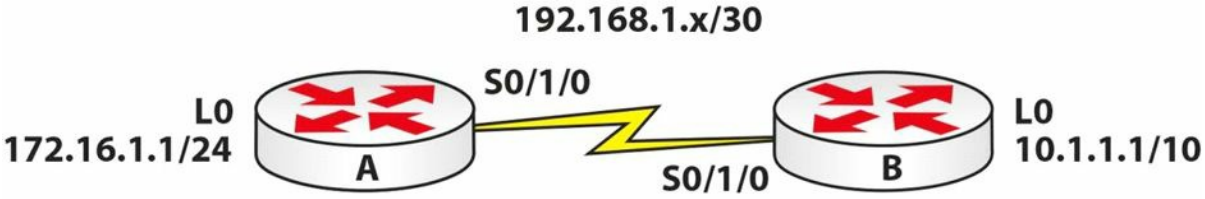
1. Network address, subnet mask (prefix length), and next-hop address or exit interface.
2. The `ip route` command.
3. The `ip route 0.0.0.0 0.0.0.0` command.
4. The `ipv6 route` command.
5. The `show ipv6 route static` command.

https://t.me/learningnets

Day 11 Lab

Static Routes Lab

Topology



Purpose

Learn how to assign static routes to a router with a next-hop address and exit interface.

Walkthrough

1. Assign all the IP addresses according to the above topology. Router A can be 192.168.1.1/30 and Router B can be .2.
2. Ping across the Serial link to ensure that it is working.
3. Assign a static route on Router A, sending all traffic for the 10.1.1.0/10 network out of the Serial interface. Use your own serial number, of course; don't just copy mine if yours has a different number!

```
RouterA(config)#ip route 10.0.0.0 255.192.0.0 Serial0/1/0
RouterA(config)#exit
RouterA#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/28/32 ms
RouterA#
RouterA#show ip route
Codes: C - Connected, S - Static, I - IGRP, R - RIP, M - Mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - Candidate default, U - Per-user static route, o - ODR
       P - Periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/10 is subnetted, 1 subnets
S       10.0.0.0 is directly connected, Serial0/1/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Loopback0
```

https://t.me/learningnets

```
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, Serial0/1/0
RouterA#
RouterA#show ip route 10.1.1.1
Routing entry for 10.0.0.0/10
Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/1/0
      Route metric is 0, traffic share count is 1
RouterA#
```

4. Configure a static route on Router B, sending all traffic for the 172.16.1.0/24 network to next-hop address 192.168.1.1.

```
RouterB(config)#ip route 172.16.1.0 255.255.255.0 192.168.1.1
RouterB(config)#exit
RouterB#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
RouterB#show ip route 172.16.1.1
Routing entry for 172.16.1.0/24
Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 192.168.1.1
      Route metric is 0, traffic share count is 1
RouterB#
```

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 12 – OSPF Basics

Day 12 Tasks

- Read today's theory notes
- Review yesterday's theory notes

Previous versions of the CCNA exam required only a basic understanding of OSPF. The current version now requires a deeper understanding of OSPFv2, v3, and multi-area OSPF. The requirements are split across the ICND1 and 2 exams and increase in difficulty on the second exam.

Today you will learn about the following:

- Link State fundamentals
- OSPF network types
- Configuring OSPF

This module maps to the following CCNA syllabus requirement:

- Configure and verify OSPF (single area)
  - Benefit of single area
  - Configure OSPFv2
  - Router ID
  - Passive interface

Open Shortest Path First

Open Shortest Path First (OSPF) is an open-standard Link State routing protocol. Link State routing protocols advertise the state of their links. When a Link State router begins operating on a network link, information associated with that logical network is added to its local Link State Database (LSDB). The local router then sends Hello messages on its operational links to determine whether other Link State routers are operating on the interfaces as well. OSPF runs directly over Internet Protocol using IP protocol number 89.

OSPF Overview and Fundamentals

Several Requests for Comments (RFCs) have been written for OSPF. In this section, we will learn about the history of OSPF based on some of the most common RFCs that pertain to OSPF. The OSPF working group was formed in 1987 and it has since released numerous RFCs. Some of the most common RFCs on OSPF are listed below:

- RFC 1131 – OSPF Specification
- RFC 1584 – Multicast Extensions to OSPF
- RFC 1587 – The OSPF NSSA Option

- RFC 1850 – OSPF Version 2 Management Information Base
- RFC 2328 – OSPF Version 2
- RFC 2740 – OSPF Version 3

RFC 1131 describes the first iteration of OSPF, and it was used in initial tests to determine whether the protocol worked.

RFC 1584 provides extensions to OSPF for the support of IP Multicast traffic. This is commonly referred to as Multicast OSPF (MOSPF). However, this standard is seldom used and, most importantly, it is not supported by Cisco.

RFC 1587 describes the operation of an OSPF Not-So-Stubby Area (NSSA). An NSSA allows for the injection of external routing knowledge by an Autonomous System Boundary Router (ASBR) using an NSSA External LSA. NSSAs will be described in detail later in this module.

RFC 1850 allows network management of OSPF using the Simple Network Management Protocol (SNMP). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. The implementation of this standard is beyond the scope of the CCNA exam requirements and is not described in this guide.

RFC 2328 details the latest update to OSPF version 2 (OSPFv2), which is the default version of OSPF in use today. OSPFv2 was initially described in RFC 1247, which addressed a number of issues discovered during the initial rollout of OSPF version 1 (OSPFv1) and modified the protocol to allow future modifications without generating backward-compatibility issues. Because of this, OSPFv2 is not compatible with OSPFv1.

Finally, RFC 2740 describes the modifications to OSPF to support IPv6. It should be assumed that all references to OSPF in this module are for OSPFv2.

Link State Fundamentals

When a Link State routing protocol is enabled for a particular link, information associated with that network is added to the local Link State Database (LSDB). The local router then sends Hello messages on its operational links to determine whether other Link State routers are operating on the interfaces as well. The Hello messages are used for neighbour discovery and to maintain adjacencies between neighbour routers. These messages will be described in detail later in this module.

When a neighbour router is located, the local router attempts to establish an adjacency, assuming both routers share the same common subnet, are in the same area, and that other parameters, such as authentication and timers, are identical. This adjacency enables the two routers to advertise summary LSDB information to each other. This exchange is not the actual detailed database information but is instead a summary of the data.

Each individual router evaluates the summary information against its local LSDB to ensure that it has the most up-to-date information. If one side of the adjacency realises that it requires an update, the router requests the new information from the adjacent router. The update from the neighbour includes the actual data contained in the LSDB. This exchange process continues until both routers have identical LSDBs. OSPF uses different types of messages to exchange the

https://t.me/learningnets

database information and to ensure that all routers have a consistent view of the network. These different packet types will be described in detail later in this module.

Following the database exchange, the SPF algorithm runs and creates a shortest-path tree to all hosts in an area or in the network backbone, with the router that is performing the calculation at the root of that tree. The SPF algorithm was described briefly in Day 10.

OSPF Fundamentals

Unlike EIGRP, which can support multiple Network Layer protocols, OSPF can only support the Internet Protocol (IP), specifically IPv4 and IPv6. Like EIGRP, OSPF supports VLSM and authentication and utilises IP Multicast when sending and receiving updates on Multi-Access networks, such as Ethernet.

OSPF is a hierarchical routing protocol that logically divides the network into subdomains referred to as areas. This logical segmentation is used to limit the scope of Link State Advertisements (LSAs) flooding throughout the OSPF domain. LSAs are special types of packets sent by routers running OSPF. Different types of LSAs are used within an area and between areas. By restricting the propagation of certain types of LSAs between areas, the OSPF hierarchical implementation effectively reduces the amount of routing protocol traffic within the OSPF network.

NOTE: OSPF LSAs will be described in detail in Day 39.

In a multi-area OSPF network, one area must be designated as the backbone area, or Area 0. The OSPF backbone is the logical centre of the OSPF network. All other non-backbone areas must be connected physically to the backbone. However, because it is not always possible or feasible to have a physical connection between a non-backbone area and the backbone, the OSPF standard allows the use of virtual connections to the backbone. These virtual connections are known as virtual links, but this concept is not included in the current CCNA syllabus.

Routers within each area store detailed topology information for the area in which they reside. Within each area, one or more routers, referred to as Area Border Routers (ABRs), facilitate inter-area routing by advertising summarised routing information between the different areas. This functionality allows for the following within the OSPF network:

- ☐ Reduces the scope of LSAs flooding throughout the OSPF domain
- ☐ Hides detailed topology information between areas
- ☐ Allows for end-to-end connectivity within the OSPF domain
- ☐ Creates logical boundaries within the OSPF domain

NOTE: Although the ICND1 syllabus makes reference only to single-area OSPF, it is necessary to discuss multi-area OSPF in order to put much of the theory into context.

The OSPF backbone area receives summarised routing information from the ABRs. The routing information is disseminated to all other non-backbone areas within the OSPF network. When a change to the network topology occurs, this information is disseminated throughout the entire OSPF domain, allowing all routers in all areas to have a consistent view of the network. The

https://t.me/learningnets

network topology illustrated in Figure 12.1 below is an example of a multi-area OSPF implementation:

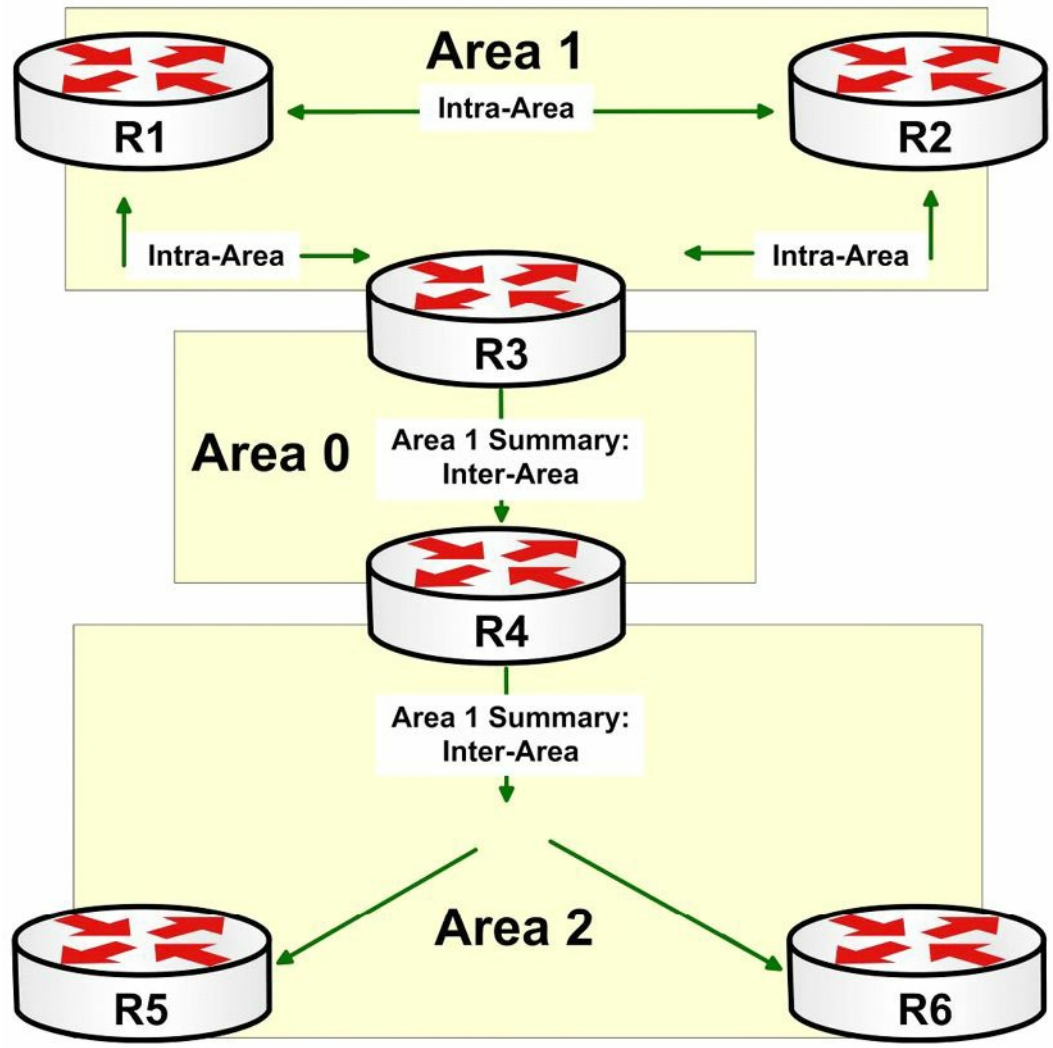


Figure 12.1 – A Multi-Area OSPF Network

Figure 12.1 illustrates a basic multi-area OSPF network. Areas 1 and 2 are connected to Area 0, the OSPF backbone. Within Area 1, routers R1, R2, and R3 exchange intra-area routing information and maintain detailed topology for that area. R3, the ABR, generates an inter-area summary route and advertises this to the OSPF backbone.

R4, the ABR for Area 2, receives the summary information from Area 0 and floods it into its adjacent area. This allows routers R5 and R6 to know of the routes that reside outside of their local area but within the OSPF domain. The same concept would also be applicable to the routing information within Area 2.

In summation, the ABRs maintain LSDB information for all the areas in which they are connected. All routers within each area have detailed topology information pertaining to that specific area. These routers exchange intra-area routing information. The ABRs advertise summary information from each of their connected areas to other OSPF areas, allowing for inter-area routing within the domain.

NOTE: OSPF ABRs and other OSPF router types will be described in detail later in this guide.

Network Types

https://t.me/learningnets

OSPF uses different default network types for different media, which are as follows:

- Non-Broadcast (default on Multipoint NBMA (FR and ATM))
- Point-to-Point (default on HDLC, PPP, P2P subinterface on FR and ATM, and ISDN)
- Broadcast (default on Ethernet and Token Ring)
- Point-to-Multipoint
- Point-to-Multipoint Non-Broadcast
- Loopback (default on Loopback interfaces)

Non-Broadcast networks are network types that do not support natively Broadcast or Multicast traffic. The most common example of a Non-Broadcast network type is Frame Relay. Non-Broadcast network types require additional configuration to allow for both Broadcast and Multicast support. On such networks, OSPF elects a Designated Router (DR) and/or a Backup Designated Router (BDR). These two routers are described later in this guide.

In Cisco IOS software, OSPF-enabled routers send Hello packets every 30 seconds by default on Non-Broadcast network types. If a Hello packet is not received in four times the Hello interval, or 120 seconds, the neighbour router is considered "dead." The following output illustrates the `show ip ospf interface` command on a Frame Relay Serial interface:

```
R2#show ip ospf interface Serial0/0
Serial0/0 is up, line protocol is up
  Internet Address 150.1.1.2/24, Area 0
  Process ID 2, Router ID 2.2.2.2, Network Type NON_BROADCAST, Cost: 64
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 2.2.2.2, Interface address 150.1.1.2
  Backup Designated Router (ID) 1.1.1.1, Interface address 150.1.1.1
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1  (Backup Designated Router)
  Suppress Hello for 0 neighbor(s)
```

A Point-to-Point (P2P) connection is simply a connection between two endpoints only. Examples of P2P connections include physical WAN interfaces using HDLC and PPP encapsulation, and Frame Relay (FR) and Asynchronous Transfer Mode (ATM) Point-to-Point subinterfaces. No DR or BDR is elected on OSPF Point-to-Point network types. By default, OSPF

https://t.me/learningnets

sends Hello packets out every 10 seconds on P2P network types. The “dead” interval on these network types is four times the Hello interval, which is 40 seconds. The following output illustrates the `show ip ospf interface` command on a P2P link:

```
R2#show ip ospf interface Serial0/0
Serial0/0 is up, line protocol is up
  Internet Address 150.1.1.2/24, Area 0
  Process ID 2, Router ID 2.2.2.2, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress Hello for 0 neighbor(s)
```

Broadcast network types are those that natively support Broadcast and Multicast traffic, the most common example being Ethernet. As is the case with Non-Broadcast networks, OSPF also elects a DR and/or a BDR on Broadcast networks. By default, OSPF sends Hello packets every 10 seconds on these network types and a neighbour is declared “dead” if no Hello packets are received within four times the Hello interval, which is 40 seconds. The following output illustrates the `show ip ospf interface` command on a FastEthernet interface:

```
R2#show ip ospf interface FastEthernet0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.2/24, Area 0
  Process ID 2, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 64
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 192.168.1.3, Interface address 192.168.1.3
  Backup Designated Router (ID) 2.2.2.2, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
```

https://t.me/learningnets

```
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.1.3  (Designated Router)
  Suppress Hello for 0 neighbor(s)
```

Point-to-Multipoint is a non-default OSPF network type. In other words, this network type must be configured manually using the `ip ospf network point-to-multipoint [non-broadcast]` interface configuration command. By default, this command defaults to a Broadcast Point-to-Multipoint network type. This default network type allows OSPF to use Multicast packets to discover dynamically its neighbour routers. In addition, there is no DR/BDR election held on Broadcast Point-to-Multipoint network types.

The `[non-broadcast]` keyword configures the Point-to-Multipoint network type as a Non-Broadcast Point-to-Multipoint network. This requires static OSPF neighbour configuration, as OSPF will not use Multicast to discover dynamically its neighbour routers. Additionally, this network type does not require the election of a DR and/or a BDR router for the designated segment. The primary use of this network type is to allow neighbour costs to be assigned to neighbours instead of using the interface-assigned cost for routes received from all neighbours.

The Point-to-Multipoint network type is typically used in partial-mesh hub-and-spoke Non-Broadcast Multi-Access (NBMA) networks. However, this network type can also be specified for other network types, such as Broadcast Multi-Access networks (e.g., Ethernet). By default, OSPF sends Hello packets every 30 seconds on Point-to-Multipoint networks. The default dead interval is four times the Hello interval, which is 120 seconds.

The following output illustrates the `show ip ospf interface` command on a Frame Relay Serial interface that has been configured manually as a Point-to-Multipoint network:

```
R2#show ip ospf interface Serial0/0
Serial0/0 is up, line protocol is up
  Internet Address 150.1.1.2/24, Area 0
Process ID 2, Router ID 2.2.2.2, Network Type POINT_TO_MULTIPOINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress Hello for 0 neighbor(s)
```

The primary reason for the OSPF requirement that the network type be the same on both routers (by the same token means that they either hold or don't hold elections) is because of the

https://t.me/learningnets

timer values. As illustrated in the outputs above, different network types use different Hello and Dead timer intervals. In order for an OSPF adjacency to be established successfully, these values must match on both routers.

Cisco IOS software allows the default OSPF Hello and Dead timers to be changed using the `ip ospf hello-interval <1-65535>` and the `ip ospf dead-interval [<1-65535>|minimal]` interface configuration commands. The `ip ospf hello-interval <1-65535>` command is used to specify the Hello interval in seconds. When issued, the software automatically configures the Dead interval to a value four times the configured Hello interval. For example, assume that a router was configured as follows:

```
R2(config)#interface Serial0/0
R2(config-if)#ip ospf hello-interval 1
R2(config-if)#exit
```

By setting the Hello interval to 1 on R2 above, Cisco IOS software automatically adjusts the default Dead timer to four times the Hello interval, which is 4 seconds. This is illustrated in the following output:

```
R2#show ip ospf interface Serial0/0
Serial0/0 is up, line protocol is up
  Internet Address 10.0.2.4/24, Area 2
  Process ID 4, Router ID 4.4.4.4, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 1, Dead 4, Wait 4, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
...
[Truncated Output]
```

OSPF Configuration

This section describes OSPF configuration fundamentals.

Enabling OSPF in Cisco IOS Software

OSPF is enabled in Cisco IOS software by issuing the `router ospf [process id]` global configuration command. The `[process id]` keyword is locally significant and does not need to be the same on all routers in the network in order to establish an adjacency. The use of the locally significant process ID allows you to configure multiple instances of OSPF on the same router.

The OSPF process ID is an integer between 1 and 65535. Each OSPF process maintains its own separate Link State Database; however, all routes are entered into the same IP routing table. In other words, there is no unique IP routing table for each individual OSPF process configured on the router.

In earlier versions of Cisco IOS software, OSPF would not be enabled if the router did not have at least one interface configured with a valid IP address in the up/up state. This restriction has

https://t.me/learningnets

been removed in current versions of Cisco IOS software. In the event that the router has no interfaces configured with a valid IP address and in the up/up state, Cisco IOS will create a Proximity Database (PDB) and allow the process to be created. However, it is important to remember that the process will be inactive until a router ID is selected, which can be performed in the following two ways:

- Configuring a valid IP address on an interface and bringing the interface up
- Configuring the router ID manually using the `router-id` command (see below)

As an example, consider the following router, which has all interfaces disabled:

```
R3#show ip interface brief
Interface         IP-Address   OK? Method Status                Protocol
FastEthernet0/0   unassigned   YES manual administratively down down
Serial0/0         unassigned   YES NVRAM  administratively down down
Serial0/1         unassigned   YES unset  administratively down down
```

Next, OSPF is enabled on the router using the `router ospf [process id]` global configuration command, as illustrated in the following output:

```
R3(config)#router ospf 1
R3(config-router)#exit
```

Based on this configuration, Cisco IOS software assigns the process a default router ID of 0.0.0.0, as illustrated in the following output of the `show ip protocols` command:

```
R3#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 0.0.0.0
  Number of areas in this router is 0. 0 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)
```

However, the `show ip ospf [process id]` command reveals that the process is not actually active and indicates that a router ID needs to be configured, as illustrated below:

```
R3#show ip ospf 1
%OSPF: Router process 1 is not running, please configure a router-id
```

Enabling OSPF Routing for Interfaces or Networks

After OSPF has been enabled, two actions can be performed to enable OSPF routing for one or more networks or interfaces on the router, as follows:

https://t.me/learningnets

- Using the `[network] [wildcard] area [area id]` router configuration command
- Using the `ip ospf [process id] area [area id]` interface configuration command

Unlike EIGRP, the wildcard mask is mandatory in OSPF and must be configured; however, as is the case with EIGRP, it serves the same function in that it matches interfaces within the range specified. As an example, the statement `network 10.0.0.0 0.255.255.255 area 0` would enable OSPF routing for interfaces with the IP address and subnet mask combination of 10.0.0.1/30, 10.5.5.1/24, and even 10.10.10.1/25. The interfaces would all be assigned to OSPF Area 0 based on the OSPF network configuration.

NOTE: The wildcard mask for OSPF can also be entered in the same format as a traditional subnet mask, for example, `network 10.0.0.0 255.0.0.0 area 0`. In this case, Cisco IOS software will invert the subnet mask and the wildcard mask will be entered into the running configuration. In addition, it is important to remember that OSPF also supports the use of the all ones or all zeros wildcard mask to enable OSPF routing for a specific interface. This configuration enables OSPF on a particular interface but the router advertises the actual subnet mask configured on the interface itself.

After the `network [network] [wildcard] area [area id]` command has been issued, the router sends out Hello packets on interfaces matching the specified network and wildcard mask combination and attempts to discover neighbours. The connected subnet is then advertised to one or more neighbour routers during the OSPF database exchange, and, finally, this information is then added to the OSPF Link State Database of the OSPF routers.

When the `network [network] [wildcard] area [area id]` command is issued, the router matches the most specific entry in order to determine the area the interface will be assigned to. Consider the following OSPF network statement configurations, as an example:

- First configuration statement: `network 10.0.0.0 0.255.255.255 Area 0`
- Second configuration statement: `network 10.1.0.0 0.0.255.255 Area 1`
- Third configuration statement: `network 10.1.1.0 0.0.0.255 Area 2`
- Fourth configuration statement: `network 10.1.1.1 0.0.0.0 Area 3`
- Fifth configuration statement: `network 0.0.0.0 255.255.255.255 Area 4`

Following this configuration on the router, the Loopback interfaces shown in Table 12.1 below are then configured on the same router:

Table 12.1 – Assigning Interfaces to OSPF Areas

Interface	IP Address/Mask
Loopback 0	10.0.0.1/32
Loopback 1	10.0.1.1/32
Loopback 2	10.1.0.1/32
Loopback 3	10.1.1.1/32
Loopback 4	10.2.0.1/32

As was previously stated, when the `network [network] [wildcard] area [area id]` command is

https://t.me/learningnets

issued, the router matches the most specific entry in order to determine the area in which the interface will be assigned. For the network statement configuration and the Loopback interfaces configured on the router, the `show ip ospf interface brief` command would show that the interfaces were assigned to the following OSPF areas:

```
R1#show ip ospf interface brief
Interface    PID   Area    IP Address/Mask    Cost  State Nbrs F/C
Lo4          1     0       10.2.0.1/32        1     LOOP  0/0
Lo1          1     0       10.0.1.1/32        1     LOOP  0/0
Lo0          1     0       10.0.0.1/32        1     LOOP  0/0
Lo2          1     1       10.1.0.1/32        1     LOOP  0/0
Lo3          1     3       10.1.1.1/32        1     LOOP  0/0
```

NOTE: Regardless of the order in which the network statements are entered, within the running configuration, the most specific entries are listed first in the output of the `show running-config` command on the router.

The `ip ospf [process id] area [area id]` interface configuration command negates the need to use the `network [network] [wildcard] area [area id]` router configuration command. This command enables OSPF routing for the specified interface and assigns the interface to the specified OSPF area. These two commands perform the same basic function and may be used interchangeably.

Additionally, if, for example, two routers are connected back to back, with one router configured using the `ip ospf [process id] area [area id]` interface configuration command and the neighbour router configured using the `network [network] [wildcard] area [area id]` router configuration command, then, assuming the area IDs are the same, the routers will successfully establish an OSPF adjacency.

OSPF Areas

The OSPF area ID may be configured either as an integer between 0 and 4294967295 or using dotted-decimal notation (i.e., using the IP address format). Unlike the OSPF process ID, the OSPF area ID must match in order for adjacency to be established. The most common type of OSPF area configuration is using an integer to specify the OSPF area. However, ensure that you are familiar with both supported methods of area configuration.

OSPF Router ID

In order for OSPF to operate on a network, each router must have a unique identifying number, and in the context of OSPF the router ID number is used.

When determining the OSPF router ID, Cisco IOS selects the highest IP address of configured Loopback interfaces. If no Loopback interfaces are configured, the software uses the highest IP address of all configured physical interfaces as the OSPF router ID. Cisco IOS software also allows administrators to specify the router ID manually using the `router-id [address]` router configuration command.

Loopback interfaces are very useful, especially during testing because they require no hardware and are logical, so they can never be down.

On the router below, I have configured IP address 1.1.1.1/32 for Loopback0 and 2.2.2.2/24 for F0/0. I then configured OSPF for all interfaces on the router:

```
Router(config-if)#router ospf 1
Router(config-router)#net 0.0.0.0 255.255.255.255 area 0
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    0.0.0.0 255.255.255.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:00:14
  Distance: (default is 110)
```

I want to hard code the router ID to 10.10.10.1. I could have done this by configuring another Loopback interface with this IP address, or I can simply add this at the OSPF router ID. I will have to either reload the router or clear the IP OSPF process on the router in order for this to take effect.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#router-id 10.10.10.1
Router(config-router)#Reload or use "clear ip ospf process" command, for this to take
effect
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#clear ip ospf process
Reset ALL OSPF processes? [no]: yes
Router#show ip prot
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.10.10.1
```

https://t.me/learningnets

```
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    0.0.0.0 255.255.255.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:03:15
  Distance: (default is 110)
```

The router ID is of particular importance when it comes to electing the DR and BDR as you will see in Day 39.

OSPF Passive Interfaces

Passive interfaces can be described as interfaces over which no routing updates are sent. In Cisco IOS software, an interface is configured as passive by using the `passive-interface [name]` router configuration command. If there are multiple interfaces on the router that need to be configured as passive, the `passive-interface default` router configuration command should be used. This command configures all interfaces that fall within the configured network range on the router to be passive. Interfaces on which adjacencies or neighbour relationships should be allowed can then be configured using the `no passive-interface [name]` router configuration command.

Passive interface configuration works the same for both OSPF and EIGRP in that if an interface is marked as passive, all neighbour relationships via that interface will be torn down and Hello packets will not send or receive packets via that interface. However, the interface will continue to be advertised based on the configured network statement configuration on the router:

```
Router(config)#router ospf 10
Router(config-router)#passive-interface f0/0
Router#show ip ospf int f0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 10,Router ID 172.16.1.1,Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured,Hello 10, Dead 40, Wait 40,Retransmit 5
    No Hellos (Passive interface)
```

https://t.me/learningnets

Day 12 Questions

1. What protocol does OSPF use?
2. How does OSPF determine whether other Link State routers are operating on the interfaces as well?
3. When a _____ routing protocol is enabled for a particular link, information associated with that network is added to the local Link State Database (LSDB).
4. OSPF utilises IP Multicast when sending and receiving updates on Multi-Access networks, such as Ethernet. True or false?
5. OSPF is a hierarchical routing protocol that logically divides the network into subdomains referred to as _____.
6. Name at least 4 OSPF network types.
7. Name the command used to enter OSPF configuration mode.
8. When determining the OSPF router ID, Cisco IOS selects the lowest IP address of the configured Loopback interfaces. True or false?
9. What command can you use to assign an interface to OSPF Area 2 (interface level command)?
10. _____ can be described as interfaces over which no routing updates are sent.

https://t.me/learningnets

Day 12 Answers

1. IP number 89.
2. By sending Hello packets.
3. Link State.
4. True.
5. Areas.
6. Non-Broadcast, Point-to-Point, Broadcast, Point-to-Multipoint, Point-to-Multipoint Non-Broadcast, and Loopback.
7. The `router ospf <id>` command.
8. False.
9. The `ip ospf <id> area 2` command.
10. Passive.

https://t.me/learningnets

Day 12 Lab

Basic OSPF Lab

Repeat the scenario from Day 10 (two routers directly connected, Loopback interface on each of them) but instead of configuring RIP and advertising the physical and Loopback interfaces, do this using OSPF Area 0:

- ☐ Assign an IPv4 address to the directly connected interfaces (10.10.10.1/24 and 10.10.10.2/24)
- ☐ Test direct connectivity using ping
- ☐ Configure a Loopback interface on each router and assign addresses from two different ranges (11.11.11.1/32 and 12.12.12.2/32)
- ☐ Configure standard OSPF process 1 and advertise all the local networks in Area 0. Also, configure a router ID for each device:

R1:

```
router ospf 1
router-id 1.1.1.1
network 10.10.10.0 0.0.0.255 area 0
network 11.11.11.1 0.0.0.0 area 0
```

R2:

```
router ospf 1
router-id 2.2.2.2
network 10.10.10.0 0.0.0.255 area 0
network 12.12.12.2 0.0.0.0 area 0
```

- ☐ Ping R2 Loopback from R1 to test connectivity
- ☐ Issue a `show ip route` command to verify that routes are being received via OSPF
- ☐ Issue a `show ip protocols` command to verify that OSPF is configured and active on the devices
- ☐ Verify the interface OSPF-specific parameters: `show ip ospf interface` and `show ip ospf interface brief`
- ☐ Change the OSPF Hello and Dead timers on both routers (directly connected interfaces): `ip ospf hello` and `ip ospf dead`
- ☐ Issue a `show ip ospf 1` command to see the routing process parameters
- ☐ Repeat the lab but this time advertise the networks in OSPF using the `ip ospf 1 area 0 interface specific` command instead of the `network` command under router OSPF

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 13 – OSPFv3

Day 13 Tasks

- Read today's theory notes
- Review yesterday's theory notes

Today we will look at OSPFv3, where you will learn about the following:

- OSPF fundamentals

This module maps to the following CCNA syllabus requirements:

- Configure OSPFv3
- Router ID
- Passive interface

OSPF Version 3

OSPFv3 is defined in RFC 2740 and is the counterpart of OSPFv2, but it is designed explicitly for the IPv6 routed protocol. The version is derived from the Version field in the OSPF packet, which has been updated to a value of 3. The OSPFv3 specification is based mainly on OSPFv2 but contains additional enhancements because of the added support for IPv6.

Both OSPFv2 and OSPFv3 can run on the same router. In other words, the same physical router can route for both IPv4 and IPv6 because each address family has a different SPF process. This does not mean that the SPF algorithm itself is different for OSPFv2 and OSPFv3; the statement simply means that a separate instance of the same SPF algorithm is run for OSPFv2 and OSPFv3. The similarities shared by OSPFv2 and OSPFv3 are as follows:

- OSPFv3 continues to use the same packets that are also used by OSPFv2. These packets include Database Description (DBD), Link State Requests (LSRs), Link State Updates (LSUs), and Link State Advertisements (LSAs).
- The mechanisms for dynamic neighbour discovery and the adjacency formation process (i.e., the different neighbour states that OSPF transitions through from the Init or Attempt state through to the Full state) remain the same in OSPFv3 as in OSPFv2.
- OSPFv3 still remains RFC-compliant on different technologies. For example, if OSPFv3 is enabled over a PPP link, the network type is still specified as Point-to-Point. In a similar manner, if OSPFv3 is enabled over Frame Relay, the default network type is still specified as Non-Broadcast. In addition, the default network type can still be changed manually using the different interface-specific commands in Cisco IOS software.
- Both OSPFv2 and OSPFv3 use the same LSA flooding and aging mechanisms.
- Like OSPFv2, the OSPFv3 router ID (RID) still requires the use of a 32-bit IPv4 address.
- When OSPFv3 is enabled on a router running dual-stack (i.e., both IPv4 and IPv6), the

https://t.me/learningnets

same RID selection process used by Cisco IOS routers for OSPFv2 is used to determine the router ID to be used. However, when OSPFv3 is enabled on a router that has no operational IPv4 interfaces, then it is mandatory that the OSPFv3 router ID be configured manually using the `router-id` router configuration command.

- The OSPFv3 link ID indicates that the links are not IPv6-specific and are still based on a 32-bit IPv4 address, as is the case in OSPFv2.

While there are similarities between OSPFv2 and OSPFv3, it is important to understand that some significant differences exist with which you must be familiar. These include the following:

- In a manner similar to EIGRP, OSPFv3 runs over a link. This negates the need to have a network statement for OSPFv3. Instead, the link is configured as part of an OSPF process by using the `ipv6 router ospf [process ID] area [area ID]` interface configuration command. However, like OSPFv2, the OSPF process ID is still specified in Global Configuration mode using the `ipv6 router ospf [process ID]` global configuration command.

- OSPFv3 uses Link-Local addresses to identify the OSPFv3 adjacencies. Like EIGRPv6, the next-hop IPv6 address for OSPFv3 routes will reflect the Link-Local address of the adjacent or neighbouring router(s).

- OSPFv3 introduces two new OSPF LSA types. These are the Link LSA, defined as LSA Type 0x0008 (or LSA Type 8), and the Intra-Area-Prefix LSA, defined as LSA Type 0x2009 (or LSA Type 9). The Link LSA provides the router's Link-Local address and provides all the IPv6 prefixes attached to the link. There is one Link LSA per link. There can be multiple Intra-Area-Prefix LSAs with different Link-State IDs. The Area flooding scope can therefore be an associated prefix with the transit network referencing a Network LSA or it can be an associated prefix with a router or Stub referencing a Router LSA.

- The transport used by OSPFv2 and OSPFv3 is different in that OSPFv3 messages are sent over (encapsulated in) IPv6 packets.

- OSPFv3 uses two standard IPv6 Multicast addresses. The Multicast address FF02::5 is the equivalent of the AllSPFRouters Multicast address 224.0.0.5 used in OSPFv2, while the Multicast address FF02::6 address is the AllDRRouters Multicast address and is the equivalent of the 224.0.0.6 group address used in OSPFv2. (This will be covered in the ICND2 section.)

- OSPFv3 leverages the built-in capabilities of IPSec and uses the AH and ESP extension headers as an authentication mechanism instead of the numerous authentication mechanisms configurable in OSPFv2. Therefore, the Authentication and AuType fields have been removed from the OSPF packet header in OSPFv3.

- Finally, the last significant difference is that the OSPFv3 Hello packet now contains no address information at all but includes an interface ID, which the originating router has assigned uniquely to identify its interface to the link. This interface ID becomes the

https://ine.com/learning

Network LSA's Link State ID, should the router become the Designated Router on the link.

Cisco IOS Software OSPFv2 and OSPFv3 Configuration Differences

There are some configuration differences in Cisco IOS software when configuring OSPFv2 versus OSPFv3. However, it should be noted that these differences are not as significant as those between other versions of IPv4 routing protocols and their IPv6 counterparts.

In Cisco IOS software, OSPFv3 routing is enabled using the `ipv6 router ospf [process ID]` global configuration command. As is the case with OSPFv2, the OSPF process ID is locally significant to the router and does not need to be the same on adjacent routers in order for an adjacency to be established.

As is required for EIGRPv6 (which will be covered in the ICND2 section), the router ID for OSPFv3 must be either specified manually or configured as an operational interface with an IPv4 address (e.g., a Loopback interface). Similar to EIGRPv6, there are no network commands used when enabling OSPFv3. Instead, OSPFv3 is enabled on a per-interface basis and multiple instances may be enabled on the same interface.

Finally, when configuring OSPFv3 over NBMA networks, such as Frame Relay and ATM, the neighbour statements are specified under the specific interface using the `ipv6 ospf neighbor [link local address]` interface configuration command. In OSPFv2, these would be configured in Router Configuration mode.

NOTE: When configuring OSPFv3 over NBMA technologies, you should create static Frame Relay map statements using Link-Local addresses. This is because the Link-Local address is used to establish adjacencies, not the global Unicast address. For example, to create a static Frame Relay map statement and specify an OSPF neighbour for a Frame Relay implementation, the following configuration would be implemented on the router (we will cover Frame Relay in the ICND2 section):

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 1
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
R1(config)#interface Serial0/0
R1(config-if)#frame-relay map ipv6 FE80::205:5EFF:FE6E:5C80 111 broadcast
R1(config-if)#ipv6 ospf neighbor FE80::205:5EFF:FE6E:5C80
R1(config-if)#exit
```

Configuring and Verifying OSPFv3 in Cisco IOS Software

Continuing from the previous section, which highlighted the configuration differences between OSPFv2 and OSPFv3, this section goes through the steps required to enable and verify OSPFv3 functionality and routing in Cisco IOS software. The following sequence of steps should be taken to enable OSPFv3 routing in Cisco IOS software:

1. Globally enable IPv6 routing using the `ipv6 unicast-routing` global configuration command. By default, IPv6 routing is disabled in Cisco IOS software.
2. Configure one or more OSPFv3 processes using the `ipv6 router ospf [process ID]` global

https://t.me/learningnets

configuration command.

3. If there are no operational interfaces with an IPv4 address configured on the router, then configure the OSPFv3 RID manually using the `router-id [IPv4 Address]` router configuration command.
4. Enable IPv6 on the desired interfaces using the `ipv6 address` and `ipv6 enable interface` configuration commands.
5. Enable one or more OSPFv3 processes under the interface using the `ipv6 ospf [process ID] area [area ID]` interface configuration command.

The first basic multi-area OSPFv3 configuration example is based on the topology that is illustrated in Figure 13.1 below:

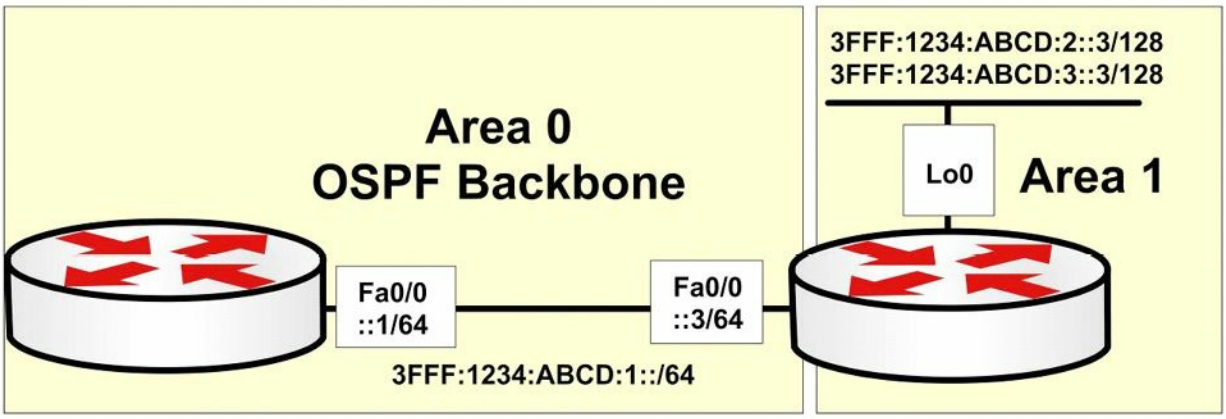


Figure 13.1 – Configuring Basic Multi-Area OSPFv3 in Cisco IOS Software

Following the sequence of configuration steps described in the previous section, OSPFv3 will be configured on router R1 as follows:

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 1
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
R1(config)#interface FastEthernet0/0
R1(config-if)#ipv6 address 3fff:1234:abcd:1::1/64
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 ospf 1 Area 0
R1(config-if)#exit
```

Following the same sequence of steps, OSPFv3 routing is configured on router R3 as follows:

```
R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router ospf 3
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#exit
R3(config)#interface FastEthernet0/0
R3(config-if)#ipv6 address 3fff:1234:abcd:1::3/64
R3(config-if)#ipv6 enable
```

https://t.me/learningnets

```
R3(config-if)#ipv6 ospf 3 Area 0
R3(config-if)#exit
R3(config)#interface Loopback0
R3(config-if)#ipv6 address 3fff:1234:abcd:2::3/128
R3(config-if)#ipv6 address 3fff:1234:abcd:3::3/128
R3(config-if)#ipv6 enable
R3(config-if)#ipv6 ospf 3 Area 1
R3(config-if)#exit
```

Following the configuration of OSPFv3 on both routers, you can use the `show ipv6 ospf neighbors` command to verify the state of the OSPFv3 adjacency, as illustrated below on R1:

```
R1#show ipv6 ospf neighbor
Neighbor   ID Pri   State       Dead Time   Interface ID    Interface
3.3.3.3         1   FULL/BDR    00:00:36    4               FastEthernet0/0
```

You can also view detailed neighbour information by appending the `[detail]` keyword to the end of this command:

```
R1#show ipv6 ospf neighbor detail
Neighbor 3.3.3.3
    In the area 0 via interface FastEthernet0/0
    Neighbor: interface-id 4, link-local address FE80::213:19FF:FE86:A20
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 1.1.1.1 BDR is 3.3.3.3
    Options is 0x000013 in Hello (V6-Bit E-Bit R-bit )
    Options is 0x000013 in DBD (V6-Bit E-Bit R-bit )
    Dead timer due in 00:00:39
    Neighbor is up for 00:06:40
    Index 1/1/1, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

In the output above, notice that the actual neighbour interface address is the Link-Local address, not the configured global IPv6 Unicast address.

https://t.me/learningnets

Day 13 Questions

1. Both OSPFv2 and OSPFv3 can run on the same router. True or false?
2. OSPFv2 and OSPFv3 use different LSA flooding and aging mechanisms. True or false?
3. Which is the equivalent of 224.0.0.5 in the IPv6 world?
4. As is required for EIGRPv6, the router ID for OSPFv3 must be either specified manually or configured as an operational interface with an IPv4 address. True or false?
5. Which command would you use to enable the OSPFv3 routing protocol?
6. Which command would you use to specify an OSPFv3 neighbour over an NBMA interface?
7. Which command would you use to see the OSPFv3 LSDB?
8. A significant difference between OSPFv2 and OSPFv3 is that the OSPFv3 Hello packet now contains no address information at all but includes an interface ID, which the originating router has assigned to uniquely identify its interface to the link. True or false?

https://t.me/learningnets

Day 13 Answers

1. True.
2. False.
3. FF02::5.
4. True.
5. The `ipv6 router ospf <id>` command.
6. The `ipv6 ospf neighbor` command.
7. The `show ipv6 ospf database` command.
8. True.

https://t.me/learningnets

Day 13 Lab

Basic OSPFv3 Lab

Repeat the scenario from Day 12 (two routers directly connected, Loopback interface on each of them) but instead of configuring OSPF for IPv4, configure IPv6 addresses and advertise them using OSPFv3 between the devices:

- ☐ Assign an IPv6 address to the directly connected interfaces (2001:100::1/64 and 2001:100::2/64)
- ☐ Test direct connectivity using ping
- ☐ Configure a Loopback interface on each router and assign addresses from two different ranges (2002::1/128 and 2002::2/128)
- ☐ Configure standard OSPFv3 process 1 and advertise all the local networks in Area 0. Also, configure a router ID for each device

R1:

```
ipv6 router ospf 1
router-id 1.1.1.1
```

`int fa0/0` (or the specific interface number)

```
ipv6 ospf 1 area 0
```

`int lo0` (or the specific interface number)

```
ipv6 ospf 1 area 0
```

R2:

```
ipv6 router ospf 1
router-id 2.2.2.2
```

`int fa0/0` (or the specific interface number)

```
ipv6 ospf 1 area 0
```

`int lo0` (or the specific interface number)

```
ipv6 ospf 1 area 0
```

- ☐ Ping R2 IPv6 Loopback from R1 to test connectivity
- ☐ Issue a `show ipv6 route` command to verify that routes are being received via OSPFv3
- ☐ Issue a `show ipv6 protocols` command to verify that OSPFv3 is configured and active on the devices
- ☐ Verify the interface OSPF-specific parameters: `show ipv6 ospf interface` and `show ipv6 ospf interface brief`
- ☐ Change the OSPF Hello and Dead timers on both routers (directly connected interfaces): `ipv6 ospf hello` and `ipv6 ospf dead`
- ☐ Issue a `show ipv6 ospf 1` command to see the routing process parameters

https://t.me/learningnets

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 14 – DHCP and DNS

Day 14 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's lab
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website

Dynamic Host Configuration Protocol (DHCP) is used by hosts to gather initial configuration information, which includes parameters such as IP address, subnet mask, and default gateway, upon boot up. Since each host needs an IP address to communicate in an IP network, DHCP eases the administrative burden of manually configuring each host with an IP address.

Domain Name System (DNS) maps host names to IP addresses, enabling you to type "www.in60days.com" into your web browser instead of the IP address of the server on which the site is hosted.

Today you will learn about the following:

- DHCP operations
- Configuring DHCP
- Troubleshooting DHCP issues
- DNS operations
- Configuring DNS
- Troubleshooting DNS issues

This lesson maps to the following CCNA syllabus requirement:

- Configure and verify DHCP (IOS router)
  - Configure router interfaces to use DHCP
  - DHCP options
  - Excluded addresses
  - Lease time

DHCP Functionality

DHCP Operations

DHCP simplifies network administrative tasks by automatically assigning IP information to hosts on a network. This information can include IP addresses, subnet masks, and default gateways, and is usually assigned when the host boots up.

https://t.me/learningnets

When the host first boots up, if it has been configured to use DHCP (which most hosts are), it will send a Broadcast message asking for IP information to be allocated. The Broadcast will be heard by the DHCP server and the information will be relayed.

> Farai says – "This is assuming that they are on the same subnet. If they are not, then see the `ip helper-address` command below."

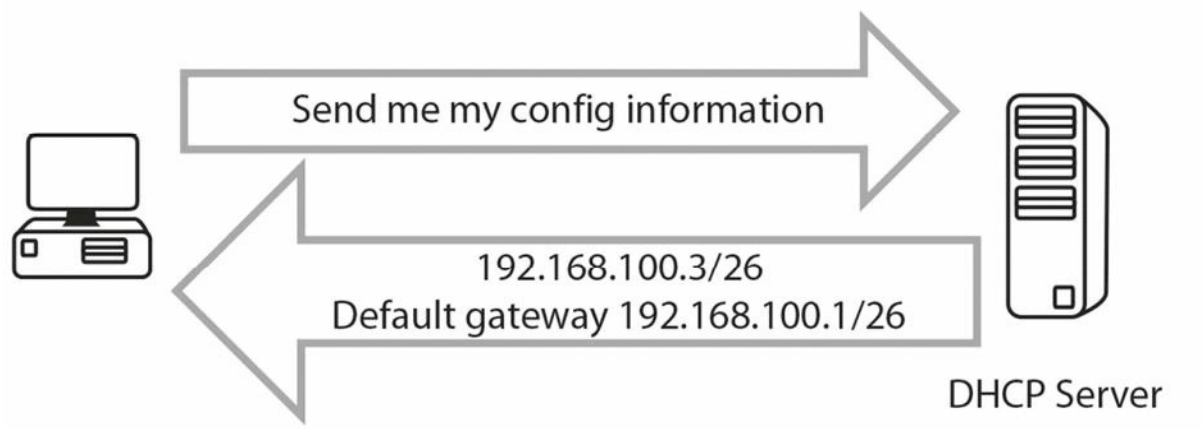


Figure 14.1 – Host Requests IP Configuration Information

DHCP actually uses UDP ports 67 and 68 to communicate over the network, and, of course, actual servers are usually used as DHCP servers, although routers can also perform this role, if required. Routers can also be configured to obtain their IP address from a DHCP server, if required, although this is rarely done. The command to configure this is:

```
Router(config-if)#ip address dhcp
```

DHCP states for clients are as follows:

- Initialising
- Selecting
- Requesting
- Bound
- Renewing
- Rebinding

DHCP servers can be configured to give an IP address to a host for a specified period called the lease time. This can be for hours or days. You can and should reserve IP addresses which cannot be allocated to hosts on the network. These IP addresses will already be in use on router interfaces or for servers. If you fail to do this, you may see duplicate IP address warnings on your network because the DHCP server has allocated your address to a host.

The full DHCP request and assign process can be seen in Figure 14.2 below:

https://t.me/learningnets

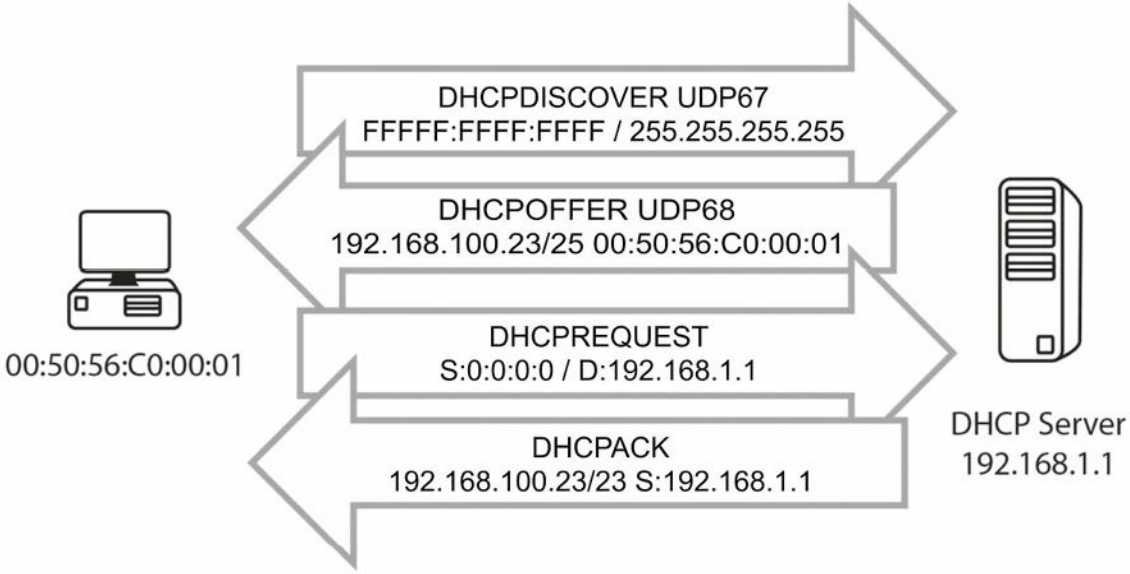


Figure 14.2 – DHCP Request and Allocation Process

1. **DHCP Discover packet:** When a device boots up and it is configured to obtain an address via DHCP, it sends a Broadcast sourced from UDP port 68 (bootpc) out to UDP port 67 (bootps). The packet will reach every device on the network, including any possible DHCP servers located there.

   DHCP Offer packet: The DHCP servers on the local network see the broadcasted Discover message sent by the client and send back a response (DHCP Offer packet) using UDP source port bootps 67 and destination port bootpc 68, also in the form of a Broadcast address, because the client still doesn't have an IP address so it cannot receive Unicast packets.

2. **DHCP Request packet:** Once the client workstation receives an offer made by the DHCP server, it will send a Broadcast (to let all DHCP servers learn that it has accepted an offer from a server) DHCP Request message to a specific DHCP server, again using UDP source port bootpc 68 and destination port bootps 67. The client might have received offers from multiple DHCP servers, but it only needs a single IP address so it must choose a DHCP server (based on an identifier), and this is usually done on a "first-come, first-served" basis.

3. **DHCP ACK packet:** The DHCP server sends another Broadcast message to confirm the IP address allocation to that specific client, again using UDP source port bootps 67 and destination port bootpc 68.

DHCP Reservations

A DHCP server can be configured to provide IP addresses in a number of different ways, including:

- Dynamic allocation
- Automatic allocation
- Static allocation

https://t.me/learningnets

A very common approach to assigning addresses via the DHCP server is using a dynamic

allocation process, in which the DHCP server is configured with a big pool of IP addresses and assigns one of them to clients based on their requests. When the device lease period expires or the device leaves the network, the particular IP address is handed back to the DHCP server, and then it can be assigned to another client.

Another method for assigning IP addresses using a DHCP server is called automatic allocation, which is a very similar process to dynamic allocation but using this approach, the DHCP server tries to keep a list of all the past assignments, and if an “old” client requests an IP address, it will be assigned the same one as before (i.e., the previous time it requested an IP address). Automatic allocation is a less efficient way of assigning IP addresses, but if you have a very large pool of IP addresses available, this is a very smart way to almost guarantee clients will get the same IP address every time they get active in a network.

Static allocation of IP addresses by a DHCP server implies defining the MAC addresses that you expect to see on the network and manually assigning a unique IP address for each of them, thus administratively building a MAC-to-IP association table. This is commonly used in a server environment because servers must use predictable IP addresses in order to be accessed.

DHCP Scopes

Network administrators who want to configure a DHCP server also need to configure DHCP scopes as part of this process. A scope is a grouping of IP addresses for a particular section of the network. Each subnet usually has its own scope.

A scope can also be a contiguous pool of addresses available for allocation by the DHCP server. Most servers also offer the functionality of excluding some addresses from the pool in order to avoid allocating them dynamically to clients. The excluded addresses are usually those IP addresses manually assigned to servers (and network devices) in the network.

Inside the defined DHCP scopes you can configure a number of parameters, such as:

- IP address range
- Subnet mask
- Lease duration
- Default gateway
- DNS server
- WINS server

Depending on the DHCP server used, you might be able to create different scopes with different parameters, usually associated with different subnets.

DHCP Leases

One of the major advantages offered by DHCP is the ability to lease an IP address, meaning assigning it on a temporary basis. Usually when a client leaves the network, that particular assigned IP address becomes free and can be allocated to another device by the DHCP server.

https://t.me/learningnets

DHCP leases are related to every DHCP allocation and define for how long a user is allowed to

use an allocated IP address. This parameter is usually administratively configured inside the DHCP scope. Whenever a client reboots it will have to ask the DHCP server again for an IP address. The DHCP server is usually configured to re-allocate the same address and extend the lease for the specific client.

Workstations can also manually release the IP address, for example, in these situations:

- The device is turned off indefinitely
- The device moves to another subnet (e.g, to a wireless network from a wired network)

The leasing process has a number of timers associated with it, so you can be sure that you are always going to have an IP address that is updated on every network device. The two important DHCP timers are as follows:

- **Renewal (T1) timer (default 50% of the lease time):** Whenever a workstation obtains an IP address, this timer starts up, and when 50% of the lease time has been reached, the DHCP client will try to renew its lease with the original DHCP server.
- **Rebinding (T2) timer (default: 87.5% of the lease time):** This second timer is used in situations in which the DHCP server does not answer or confirm the allocation extension after the renewal timer expires. This timer states that if 7/8ths of the lease time has passed, the client will try to find (send a DHCP Request) other DHCP servers which might be able to provide a DHCP address.

By having the lease process in place and correlated to the timers presented above, you can be assured that you will always have an IP address in a timely manner without any downtime associated with this and will automatically have a way to build redundancy into the DHCP process.

The T1 and T2 timers are presented in relation to the lease time in Figure 14.3 below:

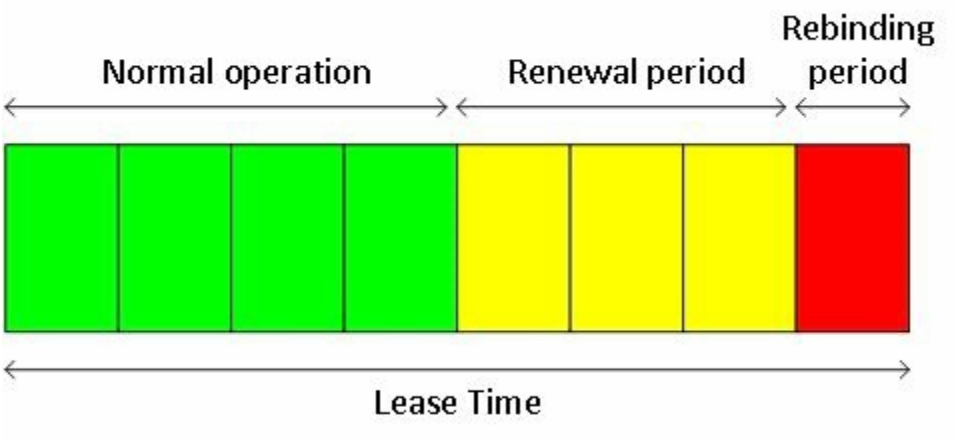


Figure 14.3 – DHCP Lease Timers

DHCP Options

In DHCP, there is a special field available that helps extend the capabilities of this automatic configuration process. You can put many different configuration options inside this field, which are also present in the DHCP RFC.

https://t.me/learningnets

NOTE: BOOTP options were called “vendor extensions.”

DHCP offers 256 option values, from which only 254 are usable because 0 is the pad option and 255 is the end option. Many DHCP options are commonly known parameters used often, including:

- Subnet mask
- Domain name server
- Domain name

Through the years, additional DHCP options have been added, especially for VoIP use, such as the following:

- Option 129: call server IP address
- Option 135: HTTP proxy for phone-specific applications

All of these options are configured directly on the DHCP server, but not all DHCP servers offer the ability to set DHCP options. If network administrators would like to use these features, they should utilise an enterprise-level DHCP server. When using small routers as DHCP servers for home offices, there may be no benefit from such functionalities.

Configuring DHCP

DHCP Servers on Cisco Routers

The first step is enabling the DHCP service on the router. This is done using the `service dhcp` command, as exemplified below:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#service dhcp
```

The next step is to create a DHCP pool which defines the IP address pool that will be allocated to clients. In this example, pool name “SUBNET_A” will offer IP addresses from the 192.168.1.0/24 range:

```
Router(config)#ip dhcp pool SUBNET_A
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#domain-name Network+
Router(dhcp-config)#lease 30
```

The DHCP Pool Configuration mode is also the place where you can configure other DHCP options. In the configuration output above, the following parameters were configured:

- Default gateway: 192.168.1.1 (the router interface assigned to the network it serves as a DHCP server)

https://t.me/learningnets

- DNS server: 8.8.8.8
- Domain name: Network+
- Lease time: 30 days

If needed, you can also configure some excluded addresses from the 192.168.1.0/24 range. Let's say you want to exclude the router interface IP address (192.168.1.1) and the 192.168.1.250 to 192.168.1.255 address range, from which you would manually assign addresses to servers in your network. This is done using the configuration below:

```
Router(config)#ip dhcp excluded-address 192.168.1.1
Router(config)#ip dhcp excluded-address 192.168.1.250 192.168.1.255
```

To verify the clients currently served by the router DHCP server, you can use the commands below:

```
Router#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address   Client-ID/  Lease expiration  Type  Hardware address/
192.168.1.2  Mar 02 2014 12:07 AM     Automatic 0063.6973.636f.2d63
```

In the output above, a single client was served by the DHCP server and was assigned the first non-excluded IP address from the DHCP scope: 192.168.1.2. You can also see the lease expiration date and the device MAC address.

DHCP Clients on Cisco Routers

In addition to DHCP server functionality, Cisco IOS routers also permit configuring the interfaces as DHCP clients. This means that interfaces will require an address using the standard DHCP process, and any server present on the specific subnet can allocate the IP addresses.

The commands to configure a router interface as a DHCP client are as follows:

```
Router(config)#int FastEthernet0/0
Router(config-if)#ip address dhcp
```

Once a DHCP server allocates an IP address, the following notification (which includes the address and mask) will be visible on the router console:

```
*Mar  1 00:29:15.779: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned DHCP
address 10.10.10.2, mask 255.255.255.0, hostname Router
```

The DHCP allocation method can be observed with the `show ip interface brief` command:

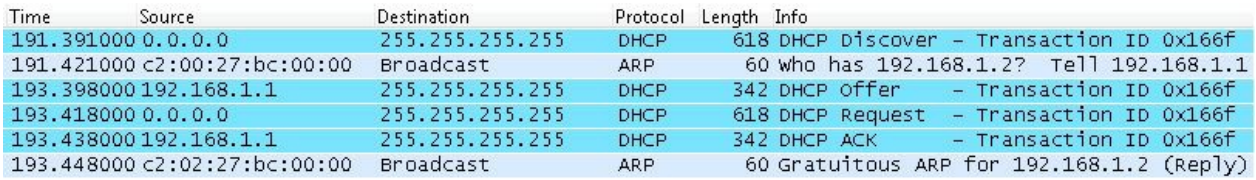
```
Router#show ip interface brief
Interface        IP-Address   OK? Method  Status                Protocol
FastEthernet0/0  10.10.10.2   YES  DHCP    up up
FastEthernet0/1  unassigned   YES  unset   administratively down down
```

DHCP Packet Analysis

In order to practically understand the topics presented in this module, some traffic captures on the devices involved in the examples above will be generated. After the DHCP server is configured and the client workstation boots up, the four-step DHCP process occurs, as can be

https://t.me/learningnets

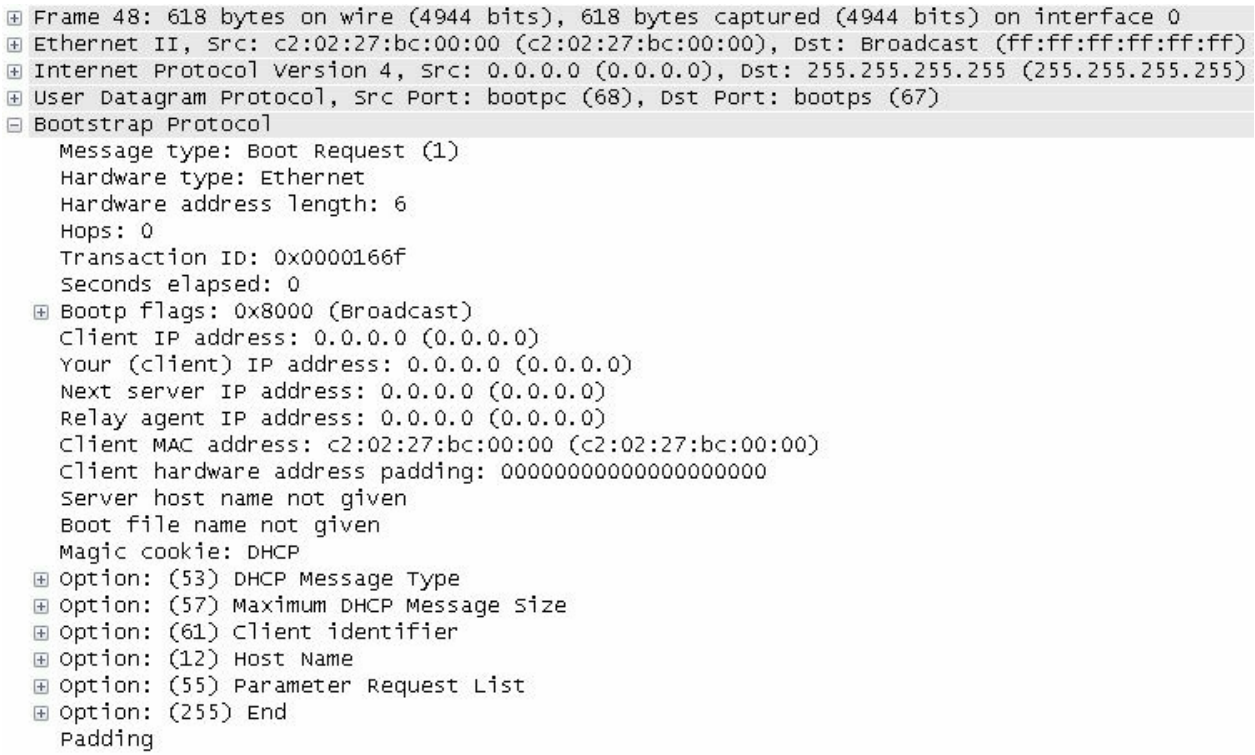
observed in the screenshot below:



Time	Source	Destination	Protocol	Length	Info
191.391000	0.0.0.0	255.255.255.255	DHCP	618	DHCP Discover - Transaction ID 0x166f
191.421000	c2:00:27:bc:00:00	Broadcast	ARP	60	Who has 192.168.1.2? Tell 192.168.1.1
193.398000	192.168.1.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x166f
193.418000	0.0.0.0	255.255.255.255	DHCP	618	DHCP Request - Transaction ID 0x166f
193.438000	192.168.1.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x166f
193.448000	c2:02:27:bc:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.1.2 (Reply)

Figure 14.4 – DHCP Four-Step Process

The DHCP Discover packet components can be observed below:



```
⊞ Frame 48: 618 bytes on wire (4944 bits), 618 bytes captured (4944 bits) on interface 0
⊞ Ethernet II, Src: c2:02:27:bc:00:00 (c2:02:27:bc:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0000166f
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: c2:02:27:bc:00:00 (c2:02:27:bc:00:00)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (53) DHCP Message Type
  ⊞ Option: (57) Maximum DHCP Message Size
  ⊞ Option: (61) Client identifier
  ⊞ Option: (12) Host Name
  ⊞ Option: (55) Parameter Request List
  ⊞ Option: (255) End
    Padding
```

Figure 14.5 – DHCP Discover Packet

As you can see in the screenshot, the packet was sent by the client who broadcasted it on the network (destination 255.255.255.255). You can also see the message type “Boot Request (1).”

The next packet is the DHCP Offer packet, presented below:

https://t.me/learningnets

```
⊞ Frame 50: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
⊞ Ethernet II, Src: c2:00:27:bc:00:00 (c2:00:27:bc:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0000166f
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.1.2 (192.168.1.2)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: c2:02:27:bc:00:00 (c2:02:27:bc:00:00)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (53) DHCP Message Type
  ⊞ Option: (54) DHCP Server Identifier
  ⊞ Option: (51) IP Address Lease Time
  ⊞ Option: (58) Renewal Time Value
  ⊞ Option: (59) Rebinding Time Value
  ⊞ Option: (1) Subnet Mask
  ⊞ Option: (3) Router
  ⊞ Option: (6) Domain Name Server
  ⊞ Option: (15) Domain Name
  ⊞ Option: (255) End
    Padding
```

Figure 14.6 – DHCP Offer Packet

This packet was sent by the server (source IP: 192.168.1.1) to the Broadcast address (destination: 255.255.255.255) and it contains the proposed IP address (192.168.1.2). You can also see the message type “Boot Reply (2).”

The third packet is the DHCP Request:

```
⊞ Frame 51: 618 bytes on wire (4944 bits), 618 bytes captured (4944 bits) on interface 0
⊞ Ethernet II, Src: c2:02:27:bc:00:00 (c2:02:27:bc:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0000166f
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: c2:02:27:bc:00:00 (c2:02:27:bc:00:00)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (53) DHCP Message Type
  ⊞ Option: (57) Maximum DHCP Message Size
  ⊞ Option: (61) Client identifier
  ⊞ Option: (54) DHCP Server Identifier
  ⊟ Option: (50) Requested IP Address
      Length: 4
      Requested IP Address: 192.168.1.2 (192.168.1.2)
  ⊞ Option: (51) IP Address Lease Time
  ⊞ Option: (12) Host Name
  ⊞ Option: (55) Parameter Request List
  ⊞ Option: (255) End
    Padding
```

https://t.me/learningnets

Figure 14.7 – DHCP Request Packet

The DHCP Request packet is sent by the client to the Broadcast address. You can see the message type “Boot Request (1).” This packet is similar to the initial DHCP Discover packet but contains a very important field, which is Option 50: Requested IP Address (192.168.1.2). This is exactly the same IP address offered by the DHCP server in the DHCP Offer packet, and the client confirms it and accepts it.

The last packet in the DHCP allocation process is the DCHP ACK packet sent by the server:

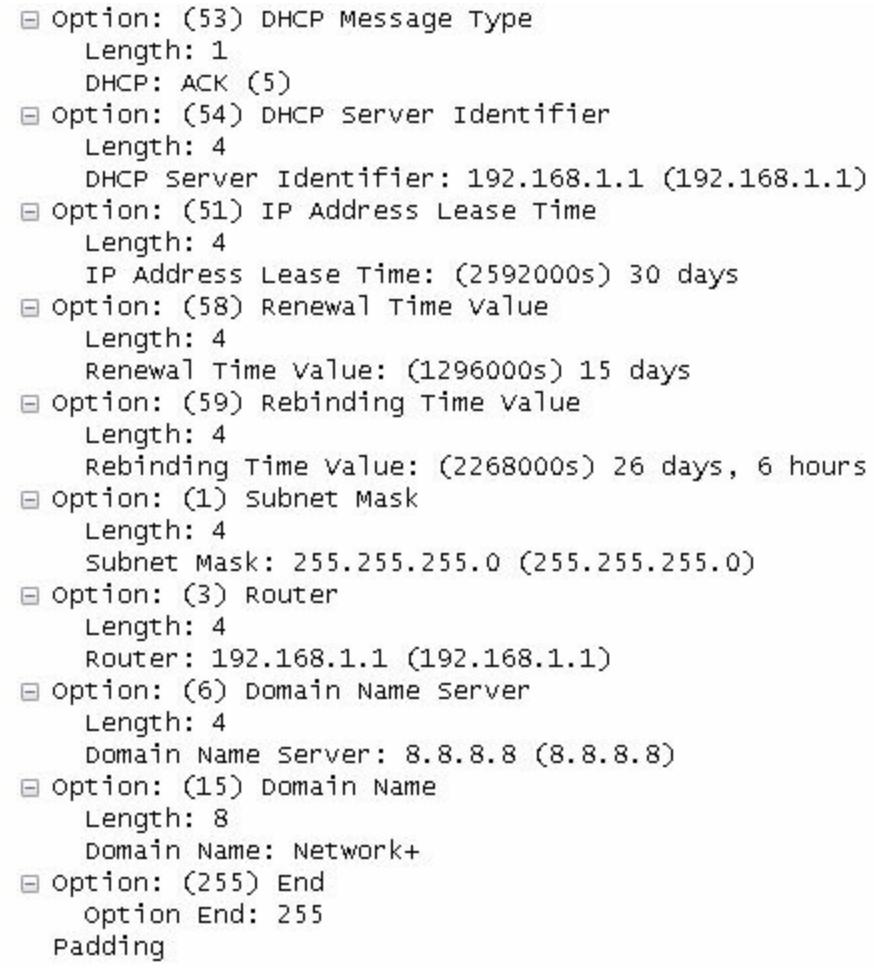


Figure 14.8 – DHCP ACK Options Packet

This packet is sourced by the DHCP server and broadcasted on the network; it also contains some extra fields as seen in the screenshot above:

- DHCP Server Identifier: the DHCP server IP address (192.168.1.1)
- All of the options configured on the router:
  - Lease time: 30 days (and the derived renewal time and rebinding time values discussed earlier)
  - Subnet mask: 255.255.255.0
  - Default gateway (router): 192.168.1.1
  - DNS server: 8.8.8.8
  - Domain name: Network+

Troubleshooting DHCP Issues

https://t.me/learningnets

As with NAT, DHCP issues are almost always due to an error in the configuration (jokingly referred to as a Layer 8 issue, meaning somebody messed up).

The `service dhcp` command is turned on by default, but sometimes it has been manually disabled by a network administrator for some reason. (I've seen network administrators call Cisco with urgent routing issues on their network after they entered the `no ip routing` command on their router – seriously!)

DHCP packets need to be permitted through your router if you are using a server on another subnet to administer DHCP configurations. DHCP uses Broadcast messages as part of its process (which routers won't forward), so the IP address of the DHCP server needs to be added to the router to allow it to forward the Broadcast message as a Unicast packet. The command `ip helper-address` achieves this. This is another exam-favourite question!

You can also use the following `debug` commands as part of your troubleshooting process:

```
debug ip dhcp server events
debug ip dhcp server packet
```

Please ensure that you type out ALL of these commands onto a router. There is no way on Earth that you will remember them by reading them on a page. Try out the configurations, make mistakes, post questions, break it on purpose (not on a live network), and fix it again.

DNS Operations

DNS maps hostnames to IP addresses (not the other way around). This allows you to browse a web address from your web browser instead of the server IP address.

DNS uses UDP port 53 when a host or a router wants to resolve a domain name to an IP address (or vice versa). TCP port 53 is used between two DNS servers when they want to sync or share their databases.

Configuring DNS

If you want to permit your router to find a DNS server on the web, then use the command `ip name-server 1.1.1.1`, or the relevant IP address of the server.

You can also set a hostname to the IP address table on your router to save time or to make it easier to remember which device to ping or connect to, as shown in the output below:

```
Router(config)#ip host R2 192.168.1.2
Router(config)#ip host R3 192.168.1.3
Router(config)#exit
Router#ping R2
Router#pinging 192.168.1.2
!!!!!
```

Troubleshooting DNS Issues

A default command on the router configuration will be `ip domain-lookup`. If this command has been disabled, then DNS won't work. Sometimes router administrators disable it because when

https://t.me/learningnets

you mistype a command you have to wait several seconds while the router performs a lookup. You can turn off DNS lookups with the following command:

```
Router(config)#no ip domain-lookup
```

Access control lists often block DNS, so this is another possible cause of problems. You can debug DNS on the router with the `debug domain` command.

https://t.me/learningnets

Day 14 Questions

1. DHCP simplifies network administrative tasks by automatically assigning _____ to hosts on a network.
2. DHCP uses UDP ports _____ and _____.
3. What are the six DHCP states for clients?
4. Which command will prevent IP addresses 192.168.1.1 to 192.168.1.10 from being used in the pool?
5. Which command will set a DHCP lease of 7 days, 7 hours, and 7 minutes?
6. Which command will enable the router to forward a DHCP Broadcast as a Unicast?
7. DNS uses UDP port _____.
8. Which command will set a DNS server address of 192.168.1.1 on your router?
9. If the _____ _____-_____ command has been disabled on your router, then DNS won't work.
10. Which command will debug DNS packets on your router?

https://t.me/learningnets

Day 14 Answers

1. IP information (IP addresses).
2. 67 and 68.
3. Initialising, Selecting, Requesting, Bound, Renewing, and Rebinding.
4. The `ip dhcp excluded-address 192.168.1.1 192.168.1.10` command.
5. The `lease 7 7 7` command under DHCP Pool Configuration mode.
6. The `ip helper-address` command.
7. 53.
8. The `ip name-server 192.168.1.1` command.
9. `ip domain-lookup`.
10. The `debug domain` command.

https://t.me/learningnets

Day 14 Labs

DHCP on a Router Lab

Topology

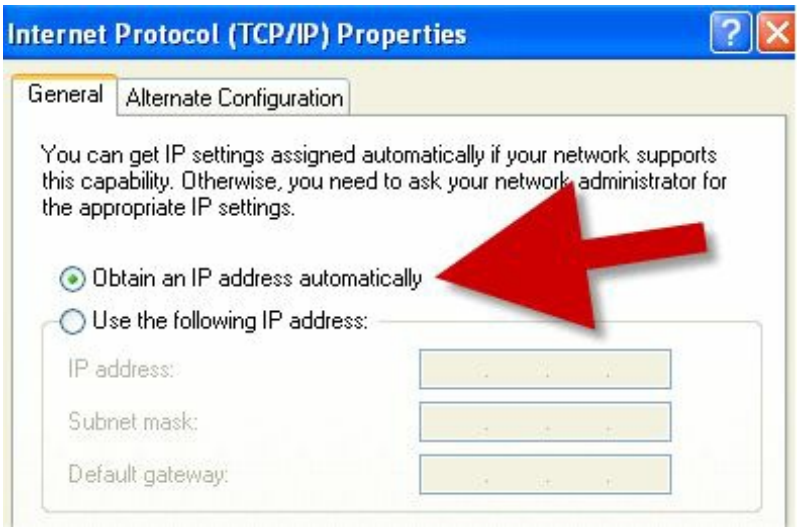


Purpose

Learn how routers can be used as DHCP servers.

Walkthrough

1. If you are using your home PC or laptop, set the network adapter to obtain the IP address automatically. You can also set this in Packet Tracer. Connect the PC to your router Ethernet port with a crossover cable.



2. Add the IP address 172.16.1.1 255.255.0.0 to your router interface. Please see previous labs

   if you can't remember how to do this. Make sure you `no shut` it.

3. Configure your DHCP pool. Then, configure a lease of 3 days, 3 hours, and 5 minutes for your address. Lastly, exclude all the addresses from 1 to 10 from being assigned to hosts. Presume that these are already in use for other servers or interfaces.

```
Router#conf t
Router(config)#ip dhcp pool 60days
Router(dhcp-config)#network 172.16.0.0 255.255.0.0
Router1(dhcp-config)#lease 3 3 5 ← command won't work on Packet Tracer
Router1(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.10
```

https://t.me/learningnets

```
Router(config)#
```

4. Issue an `ipconfig /all` command to check whether an IP address has been assigned to your PC. You may need to issue an `ipconfig /renew` command if an old IP address is still in use.

```
PC>ipconfig /all
Physical Address.....: 0001.C7DD.CB19
IP Address.....: 172.16.0.1
Subnet Mask.....: 255.255.0.0
Default Gateway.....: 0.0.0.0
DNS Servers.....: 0.0.0.0
```

5. If you wish, you can go back into the DHCP pool and add a default gateway and a DNS server address, which will also be set on the host PC.

```
Router(config)#ip dhcp pool 60days
Router(dhcp-config)#default-router 172.16.1.2
Router(dhcp-config)#dns-server 172.16.1.3
PC>ipconfig /renew
IP Address.....: 172.16.0.1
Subnet Mask.....: 255.255.0.0
Default Gateway.....: 172.16.1.2
DNS Server.....: 172.16.1.3
```

DNS on a Router Lab

Work this lab on a router that has some kind of connectivity to the Internet. Make sure it can ping a public IP address, like 8.8.8.8, which is a Google DNS server. Configure this as a name server:

```
ip name-server 8.8.8.8
```

Then try to resolve public website names, for example, by pinging www.cisco.com.

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 15 – Layer 1 and Layer 2 Troubleshooting

Day 15 Tasks

- ☐ Read today's lesson notes (below)
- ☐ Review yesterday's lesson notes
- ☐ Complete today's lab
- ☐ Read the ICND1 cram guide
- ☐ Spend 15 minutes on the subnetting.org website

We have covered much of the ICND1 troubleshooting requirements in previous lessons, particularly ACLs and IP addressing. Layers 1 and 2 cover a lot of possible issues and their causes, which will be the focus of today's lesson.

LAN switching is a form of packet switching that is used in Local Area Networks (LANs). LAN switching is performed in hardware at the Data Link Layer. Because LAN switching is hardware-based, it uses hardware addresses that are referred to as Media Access Control (MAC) addresses. The MAC addresses are then used by LAN switches to forward frames.

Today you will learn about the following:

- ☐ Troubleshooting at the Physical Layer
- ☐ VLAN, VTP, and trunking overview
- ☐ Troubleshooting VLANs
- ☐ Using the `show vlan` command

This module maps to the following CCNA syllabus requirements:

- ☐ Troubleshoot and resolve Layer 1 problems
  - Framing
  - CRC
  - Runts
  - Giants
  - Dropped packets
  - Late collisions
  - Input / Output errors
- ☐ Troubleshoot and resolve VLAN problems
  - Verify that VLANs are configured
  - Verify that port membership is correct
  - Verify that the IP address is configured

https://t.me/learningnets

- Troubleshoot and resolve trunking problems on Cisco switches
  - Verify that the trunk states are correct
  - Verify that encapsulation is configured correctly
  - Verify that VLANs are allowed

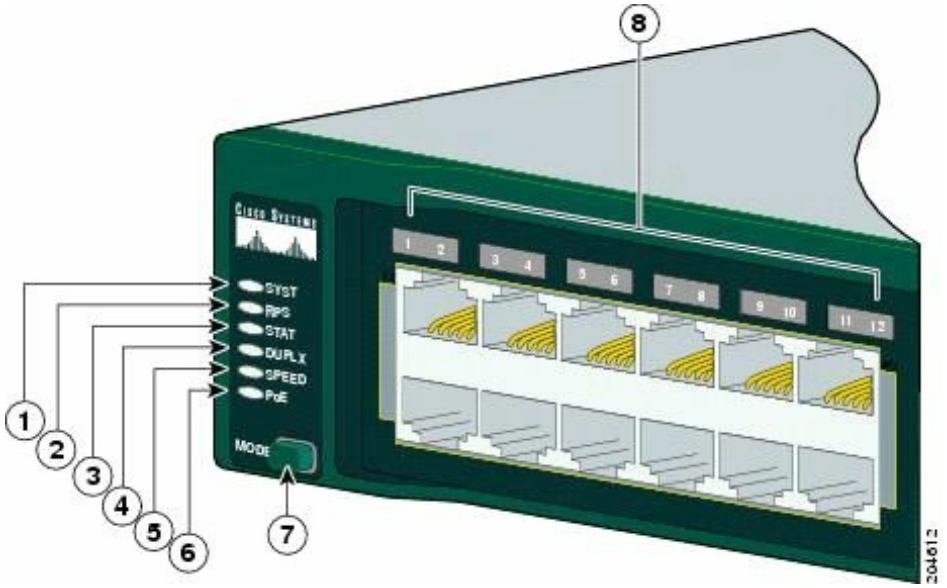
Troubleshooting at the Physical Layer

Cisco IOS switches support several commands that can be used to troubleshoot Layer 1, or at least suspected Layer 1, issues. However, in addition to being familiar with the software command suite, it is also important to have a solid understanding of physical indicators (i.e., LEDs) that can be used to troubleshoot link status or that indicate an error condition.

Troubleshooting Link Status Using Light Emitting Diodes (LEDs)

If you have physical access to the switch or switches, LEDs can be a useful troubleshooting tool. Different Cisco Catalyst switches provide different LED capabilities. Understanding the meaning of the LEDs is an integral part of Catalyst switch link status and system troubleshooting. Cisco Catalyst switches have front-panel LEDs that can be used to determine link status, as well as other variables such as system status.

Check Cisco documentation for the Catalyst 2960 switch model by Googling “Catalyst 2960 Switch Hardware Installation Guide.” The installation and configuration guides consist of many hundreds of pages of notes, advice, and technical information. It’s worth browsing through it but you shouldn’t be expected to know the contents of it for the CCNA exam beyond what is in the syllabus (which is covered in this guide).



1	System LED	5	Speed LED
2	RPS LED	6	PoE LED
3	Status LED	7	Mode button
4	Duplex LED	8	Port LEDs

Figure 15.1 – Cisco 2960 Switch LEDs. Image Copyright Cisco Systems

https://t.me/learningnets

The PoE LED is found only on the Catalyst 2960 switch model.

System LED

The system LED indicates that the system is receiving power (or is not) and is functioning properly.

Table 15.1 below lists the LED colours and the status that they indicate:

Table 15.1 – System LEDs

System LED Colour	System Status
Off	System is not powered on.
Green	System is operating normally.
Amber	System is powered on but is not functioning correctly.

RPS LED

The RPS LED is only present on switches featuring a redundant power supply. Table 15.2 below lists the LED colours and their meanings:

Table 15.2 – RPS LEDs

System LED Colour	System Status
Green	RPS is connected and ready to provide back-up power, if required.
Blinking Green	RPS is connected but is unavailable because it is providing power to another device (redundancy has been allocated to a neighbouring device).
Amber	The RPS is in standby mode or in a fault condition. Press the Standby/Active button on the RPS, and the LED should turn green. If it does not, the RPS fan could have failed. Contact Cisco Systems.
Blinking Amber	The internal power supply in a switch has failed, and the RPS is providing power to the switch (redundancy has been allocated to this device).

Port LEDs and Modes

Port LEDs give information about a group of ports or individual ports, as shown in Table 15.3 below:

Table 15.3 – Modes for Port LEDs

Selected Mode LED	Port Mode	Description
1 – System		
2 – RPS		Status of the RPS
3 – Status	Port status	The port status (default mode)
4 – Duplex	Port duplex	Duplex mode: full duplex or half duplex

https://t.me/learningnets

5 – Speed	Port speed	Port operating speed: 10, 100, or 1000Mbps
6 – PoE	PoE port power	PoE status
7 – Mode		Cycles through Status, Duplex, and Speed LEDs
8 – Port		Meaning differs according to mode

You can cycle through modes by pressing the Mode button until you reach the mode setting you require. This will change the meaning of the port LED colours, as shown in Table 15.4 below:

Table 15.4 – Mode Settings

Port Mode	LED Colour	System Status
Status	Off	No link or port was administratively shut down.
	Green	Link is present.
	Blinking Green	Activity: Port is sending or receiving data.
	Alternating Green-Amber	Link fault: Error frames can affect connectivity, and errors such as excessive collisions, cyclic redundancy check (CRC), and alignment and jabber are monitored for a link-fault indication.
	Amber	Port is blocked by Spanning Tree Protocol (STP) and is not forwarding data. **NOTE:** After a port is reconfigured, the port LED can remain amber for up to 30 seconds as STP checks the network topology for possible loops.
	Blinking Amber	Port is blocked by STP and is not sending or receiving packets.
Duplex	Off	Port is operating in half duplex.
	Green	Port is operating in full duplex.
Speed	10/100 and 10/100/1000 Ports	
	Off	Port is operating at 10Mbps.
	Green	Port is operating at 100Mbps.
	Blinking Green	Port is operating at 1000Mbps.
	SFP Ports	
	Off	Port is operating at 10Mbps.
	Green	Port is operating at 100Mbps.
	Blinking Green	Port is operating at 1000Mbps. **NOTE:** When installed in Catalyst 2960 switches, 1000BASE-T SFP modules can operate at 10, 100, or 1000Mbps in full-duplex mode or at 10 or 100Mbps in half-duplex mode.
PoE	Off	PoE is off. If the powered device is receiving power from an AC power source, the PoE port LED is off even if the powered device is connected to the switch port.
	Green	PoE is on. The port LED is green only when the switch port is providing power.
	Alternating Green-Amber	PoE is denied because providing power to the powered device will exceed the switch power capacity. The Catalyst 2960-24PC-L, 2960 48PST-L, 2960-48PST-S, and 2960-24PC-S switches provide up to 370 W of power. The Catalyst 2960-24LT-L and 2960-24LC-S switches provide up to 124 W of power.

https://t.me/learningnets

	Blinking Amber	PoE is off due to a fault. **CAUTION:** PoE faults are caused when non-compliant cabling or powered devices are connected to a PoE port. Only standard-compliant cabling can be used to connect Cisco prestandard IP phones, wireless access points, or IEEE 802.3af-compliant devices to PoE ports. You must remove the cable or device that caused the PoE fault from the network.
	Amber	PoE for the port has been disabled. By default, PoE is enabled.

In addition to understanding what the different LED colours mean, it is also important to have an understanding of what action to take to remedy the issue. For example, assume that you are troubleshooting a Catalyst 6500 Series switch and you notice that the status LEDs on the supervisor engine (or any switching modules) is red or off. In such cases, it is possible that the module might have shifted out of its slot, or, in the event of a new module, was not correctly inserted into the chassis. In this case, the recommended action is to reseat the module. In some cases, it also may be necessary to reboot the entire system.

While a link or port LED colour other than green typically indicates some kind of failure or other issue, it is important to remember that a green link light does not always mean that the cable is fully functional. For example, a single broken wire or one shut down port can cause the problem of one side showing a green link light while the other side does not. This could be because the cable encountered physical stress that caused it to be functional at a marginal level. In such cases, the CLI can be used to perform additional troubleshooting.

Troubleshooting Cable Issues

When troubleshooting cabling issues (Layer 1 troubleshooting), it can sometimes be very easy to find the problem because you can directly see and inspect the cable. However, sometimes cabling problems can be invisible, so you will have to engage in a systematic troubleshooting process to make sure the problem is really localised at Layer 1. A general recommendation is to properly test all cabling before engaging in a complex infrastructure implementation. Some common cabling problems include the following:

- Plugging in a cable but getting no connection
- Plugging in a cable and getting a connection but with very low throughput on that connection
- Everything is working normally but suddenly the connection goes away, and then comes back, and then goes away again (i.e., flapping)
- Intermittent connectivity, where it seems to work fine but the signal gets lost from time to time

Some of the recommended tests for these problems include:

- Verifying that the switch link light is on
- Verifying that the link light is not turning on and off intermittently
- Verifying that the cable is punched correctly

https://t.me/learningnets

- Verifying that the cable is not physically damaged
- Verifying that the cable is not too long (this may cause signal degradation)
- Verifying that the cable connectors are not faulty (you might need to use other connectors)
- Verifying that the wires are pinned in the correct order (in the case of copper cables)

If you want to be sure that you are not dealing with a cabling issue, one of the simplest things to do is to replace the cable and run the same tests again. This is very easy to do and might help in immediately fixing the issue without investing much time and resources into the troubleshooting process.

> **NOTE:** Sometimes even brand new cables can come with a defect, so do not assume that a new cable should function as expected.

Troubleshooting Module Issues

Most routers and switches used in an enterprise network offer copper port connectivity, but also dedicated ports that can be populated with different kind of transceivers. These transceivers are usually used for fibre connectivity, but there are also copper-compatible transceivers.

Fibre connections may run over very long distances, and generally those particular ports are modular and require a compatible SFP (small form-factor pluggable transceiver), like the one presented in Figure 15.2 below:



Figure 15.2 – SFP Module

Although they look similar, depending upon the type of connectivity used, the appropriate SFP module should be used based on several parameters, including:

- Type of media: optical fibre or copper
- Fibre type: single-mode or multi-mode fibre
- Bandwidth

https://t.me/learningnets

- Wavelength
- Core size
- Modal bandwidth
- Operating distance

NOTE: When purchasing transceivers for your network, you should always check the compatibility between the device ports, type of module, and type of fibre used.

Transceivers can be plugged into and unplugged from the network device (e.g., switch, router, firewall, etc.) at any time without restarting the device. When there is no connection you will see no activity on the SFP modules, and this is one of the easiest issues to troubleshoot if you have access to the device.

On the other hand, you might plug in a fibre cable that will activate that port but the connectivity suffers from different issues (e.g., performance degradation or intermittent connectivity) or simply does not exist. In this case, there are several approaches you could take:

- Verify that the correct cable types have been used (multi-mode vs. single-mode) depending upon the type of transceiver
- Verify that the cable is not broken, using dedicated fibre optic testing tools
- Verify that the correct type of transceiver has been used
- Verify that the transceiver does not have hardware issues (swap it and test the connection with another SFP)
- Verify that the device port is configured with the correct parameters based on the type of transceiver and cable used

To minimise connection downtime, you should monitor the ports populated with SFP modules in order to see possible errors that appear in the statistics. This can be done with standard monitoring tools, most often using SNMP.

Using the Command Line Interface to Troubleshoot Link Issues

Several Command Line Interface (CLI) commands can be used to troubleshoot Layer 1 issues on Cisco IOS Catalyst switches. Commonly used commands include the `show interfaces`, the `show controllers`, and the `show interface [name] counters errors` commands. In addition to knowing these commands, you also are required to be able to interpret accurately the output or information that these commands provide.

The `show interfaces` command is a powerful troubleshooting tool that provides a plethora of information, which includes the following:

- The administrative status of a switching port

https://t.me/learningnets

- ☐ The port operational state
- ☐ The media type (for select switches and ports)
- ☐ Port input and output packets
- ☐ Port buffer failures and port errors
- ☐ Port input and output errors
- ☐ Port input and output queue drops

The output of the `show interfaces` command for a GigabitEthernet switch port is illustrated below:

```
Catalyst-3750-1#show interfaces GigabitEthernet3/0/1
GigabitEthernet0/1 is up, line protocol is down (notconnect)
Hardware is GigabitEthernet, address is 000f.2303.2db1 (bia 000f.2303.2db1)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, Loopback not set
Keepalive not set
Auto-duplex, Auto-speed, link type is auto, media type is unknown
input flow-control is off, output flow-control is desired
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 PAUSE output
    0 output buffer failures, 0 output buffers swapped out
```

Most Cisco Catalyst switch ports default to the `notconnect` state, as illustrated in the first line of the output printed by this command. However, a port can also transition to this state if a cable

https://t.me/learningnets

is removed from the port or is not correctly connected. This status is also reflected when the connected cable is faulty or when the other end of the cable is not connected to an active port or device (e.g., if a workstation connected to the switch port is powered off).

NOTE: When troubleshooting GigabitEthernet ports, this port status may also be a result of incorrect Gigabit Interface Converters (GBICs) being used between the two ends.

The first part of the output in the first line printed by this command (i.e., `[interface] is up`) refers to the Physical Layer status of the particular interface. The second part of the output (i.e., `line protocol is down`) indicates the Data Link Layer status of the interface. If this indicates an "`up`," then it means that the interface can send and receive keepalives. Keep in mind that it is possible for the switch port to indicate that the Physical Layer is up while the Data Link Layer is down, for example, such as when the port is a SPAN destination port (for sniffer traffic) or if the local port is connected to a CatOS (older switch operating system) switch with its port disabled.

The Input queue indicates the actual number of frames dropped because the maximum queue size was exceeded. The flushes column counts Selective Packet Discard (SPD) drops on the Catalyst 6000 Series switches. SPD drops low-priority packets when the CPU is overloaded in order to save some processing capacity for high-priority packets. The flushes counter in the `show interfaces` command output increments as part of SPD, which implements a selective packet drop policy on the IP process queue of the router. Therefore, it applies only to process-switched traffic.

The total output drops indicates the number of packets dropped because the output queue is full. This is often seen when traffic from multiple inbound high-bandwidth links (e.g., GigabitEthernet links) is being switched to a single outbound lower-bandwidth link (e.g., a FastEthernet link). The output drops increment because the interface is overwhelmed by the excess traffic due to the speed mismatch between the inbound and outbound bandwidths.

Some of the other interface-specific terms that can be analysed from the `show interfaces` output and can be very useful during Layers 1 and 2 troubleshooting are:

- **Frame number:** This field describes the number of packets received incorrectly having a CRC error and a non-integer number of octets. This is usually the result of collisions due to a malfunctioning Ethernet device (hardware fault).
- **CRC:** This field indicates that the CRC (cyclic redundancy checksum) generated by the sending device does not match the checksum calculated at the receiving device. This usually indicates transmission problems on a LAN, collisions, or a system transmitting bad data.
- **Runts:** This field indicates the number of packets that are discarded due to being smaller than the minimum packet size. On Ethernet segments, packets smaller than 64 bytes are considered runts.
- **Giants:** This field indicates the number of packets that are discarded due to being larger than the maximum packet size. On Ethernet segments, packets larger than 1518 bytes are considered giants.

https://t.me/learningnets

- **Late collisions:** Late collisions usually occur when Ethernet cables are too long or when there are too many repeaters in the network. The number of collisions represents the number of messages retransmitted due to an Ethernet collision. This is usually caused by an overextended LAN.
- **Input errors:** This field provides the total sum of runts, giants, CRC, overruns, and ignored packets.
- **Output errors:** This field provides the total sum of all errors that prevented the final transmission of datagrams out of the interface.

In addition to the `show interfaces` command, the `show interfaces [name] counters errors` command can also be used to view interface errors and facilitate Layer 1 troubleshooting. The output that is printed by the `show interfaces [name] counters errors` command is as follows:

```
Catalyst-3750-1#show interfaces GigabitEthernet3/0/1 counters errors
Port        Align-Err    FCS-Err   Xmit-Err    Rcv-Err UnderSize
Gi3/0/1             0          0          0          0         0
Port      Single-Col Multi-Col  Late-Col Excess-Col Carri-Sen   Runs
Gi3/0/1        0         0         0          0         0        0
Port        Giants
Gi3/0/1        0
```

The following section describes some of the error fields included in the output of the `show interfaces [name] counters errors` command, and which issues or problems are indicated by non-zero values under these fields.

The `Align-Err` field reflects a count of the number of frames received that do not end with an even number of octets and that have a bad CRC. These errors are usually the result of a duplex mismatch or a physical problem, such as cabling, a bad port, or a bad network interface controller (NIC). When the cable is first connected to the port, some of these errors can occur. In addition, if there is a hub connected to the port, collisions between other devices on the hub can cause these errors.

The `FCS-Err` field reflects the number of valid-sized frames with Frame Check Sequence (FCS) errors but no framing errors. This is typically a physical issue, such as cabling, a bad port, or a bad NIC. Additionally, a non-zero value under this field could indicate a duplex mismatch.

A non-zero value in the `Xmit-Err` field is an indication that the internal send (Tx) buffer is full. This is commonly seen when traffic from multiple inbound high-bandwidth links (e.g., GigabitEthernet links) is being switched to a single outbound lower-bandwidth link (i.e., a FastEthernet link), for example.

The `Rcv-Err` field indicates the sum of all received errors. This counter is incremented when the interface receives an error such as a runt, a giant, or an FCS, for example.

The `UnderSize` field is incremented when the switch receives frames that are smaller than 64 bytes in length. This is commonly caused by a faulty sending device.

https://t.me/learningnets

The various `collision` fields indicate collisions on the interface. This is common for half-duplex

Ethernet, which is almost non-existent in modern networks. However, these counters should not increment for full-duplex links. In the event that non-zero values are present under these counters, this typically indicates a duplex mismatch issue. When a duplex mismatch is detected, the switch prints a message similar to the following on the console or in the log:

```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/1 (not full duplex),
with R2 FastEthernet0/0 (full duplex)
```

As will be described in the section pertaining to Spanning Tree Protocol (STP), duplex mismatches can cause STP loops in the switched network if a port is connected to another switch. These mismatches can be resolved by manually configuring the speed and the duplex of the switch ports.

The `Carri-Sen` (carrier sense) counter increments every time an Ethernet controller wants to send data on a half-duplex connection. The controller senses the wire and ensures that it is not busy before transmitting. A non-zero value under this field indicates that the interface is operating in half-duplex mode. This is normal for half-duplex.

Non-zero values can also be seen under the `Runts` field due to a duplex mismatch or because of other Physical Layer problems, such as a bad cable, port, or NIC on the attached device. Runts are received frames with a bad CRC that are smaller than the minimum IEEE 802.3 frame size, which is 64 bytes for Ethernet.

Finally, the `Giants` counter is incremented when frames are received that exceed the IEEE 802.3 maximum frame size, which is 1518 bytes for non-jumbo Ethernet, and that have a bad FCS. For ports or interfaces connected to a workstation, a non-zero value under this field is typically caused by a bad NIC on the connected device. However, for ports or interfaces that are connected to another switch (e.g., via a trunk link), this field will contain a non-zero value if 802.1Q encapsulation is used. With 802.1Q, the tagging mechanism implies a modification of the frame because the trunking device inserts a 4-byte tag and then re-computes the FCS.

Inserting a 4-byte tag into a frame that already has the maximum Ethernet size creates a 1522-byte frame that can be considered a baby giant frame by the receiving equipment. Therefore, while the switch will still process such frames, this counter will increment and contain a non-zero value. To resolve this issue, the 802.3 committee created a subgroup called 802.3ac to extend the maximum Ethernet size to 1522 bytes; however, it is not uncommon to see a non-zero value under this field when using 802.1Q trunking.

The `show controllers ethernet-controller <interface>` command can also be used to display traffic counter and error counter information similar to that printed by the `show interfaces` and `show interfaces <name> counters errors` commands. The output of the `show controllers ethernet-controller <interface>` command is shown below:

```
Catalyst-3750-1#show controllers ethernet-controller GigabitEthernet3/0/1
Transmit GigabitEthernet3/0/1       Receive
4069327795 Bytes                   3301740741 Bytes
  559424024 Unicast frames           376047608 Unicast frames
   27784795 Multicast frames           1141946 Multicast frames
    7281524 Broadcast frames           1281591 Broadcast frames
```

https://t.me/learningnets

```
        0 Too old frames           429934641 Unicast bytes
        0 Deferred frames          226764843 Multicast bytes
        0 MTU exceeded frames      137921433 Broadcast bytes
        0 1 collision frames               0 Alignment errors
        0 2 collision frames               0 FCS errors
        0 3 collision frames               0 Oversize frames
        0 4 collision frames               0 Undersize frames
        0 5 collision frames               0 Collision fragments
        0 6 collision frames
        0 7 collision frames          257477 Minimum size frames
        0 8 collision frames       259422986 65 to 127 byte frames
        0 9 collision frames        51377167 128 to 255 byte frames
        0 10 collision frames       41117556 256 to 511 byte frames
        0 11 collision frames        2342527 512 to 1023 byte frames
        0 12 collision frames        5843545 1024 to 1518 byte frames
        0 13 collision frames              0 Overrun frames
        0 14 collision frames              0 Pause frames
        0 15 collision frames
        0 Excessive collisions             0 Symbol error frames
        0 Late collisions                  0 Invalid frames, too large
        0 VLAN discard frames      18109887 Valid frames, too large
        0 Excess defer frames              0 Invalid frames, too small
   264522 64 byte frames                   0 Valid frames, too small
 99898057 127 byte frames
 76457337 255 byte frames                  0 Too old frames
  4927192 511 byte frames                  0 Valid oversize frames
 21176897 1023 byte frames                 0 System FCS error frames
127643707 1518 byte frames                 0 RxPortFifoFull drop frames
264122631 Too large frames
        0 Good (1 coll) frames
        0 Good (>1 coll) frames
```

NOTE: The output above will vary slightly depending upon the switch platform on which this command is executed. For example, Catalyst 3550 series switches also include a `Discarded frames` field, which shows the total number of frames whose transmission attempt is abandoned due to insufficient resources. A large number in this field typically indicates a network congestion issue. In the output above, you would look at the `RxPortFifoFull drop` frame field, which indicates the total number of frames received on an interface that are dropped because the ingress queue is full.

Troubleshooting Port Configuration

Each networking device can be configured in different ways. Most types of misconfigurations generate problems within the network, including:

- Port mismatch

https://thelearningnets

- Lack of connectivity

A device can be connected to the network, have a signal, and be able to communicate to the Internet and to other devices but the performance might be low, in a consistent and easily reproducible way. This can manifest during normal operations, including file transfer or other types of communications with the rest of the network.

With major configuration issues, the issue might manifest as complete lack of connectivity, including no link lights on the specific device ports. Sometimes the link lights are on but you still lack any kind of connectivity. This shows that the signal is passing through the cable, which means that you don't have a cabling issue but rather a port configuration issue on one port or the other. This requires problem investigation in the device's configuration.

There are a number of different settings when configuring a port, including:

- Speed
- Duplex
- Encapsulation/VLAN.

Most of these parameters have to be synchronised on both sides of the link, either by manually configuring them or by enabling port autoconfiguration. If detected, this method will send negotiation packets on the link to each device to detect the capabilities on the other end device and commonly agree on the best possible parameters supported by both of them to ensure an optimal transmission. The problem is that sometimes autoconfiguration does not select the best parameters for your needs, so you should also verify this and manually configure the ports according to each specific case.

If you are performing manual configuration on each port, one of the first parameters you have to take care of is the interface speed. This has to be identical on both sides of a link. If you configure it incorrectly on one side, the link might not be operational. Another related setting is port duplex, which can be configured to be either half duplex or full duplex. You can configure a link with half duplex on one side and full duplex on the other side, and even though the link will come up, the throughput will be highly affected because each side is expecting to handle communication in a different way. This will result in collisions which will affect the transmission on that particular link. Make sure that both sides use the same duplex settings in order for the traffic to be sent as efficiently as possible.

If you are operating in an enterprise-level environment, you might need to use different VLANs to segment the traffic. Each switch must be properly configured in this regard so each switch port is assigned to the correct VLAN. If you are directly connecting ports configured to use different VLAN IDs, the communication will be broken at Layer 2, even though the Physical Layer shows no issues.

By examining all the port configuration options presented above and making sure that you have everything synchronised at both ends of a link, you can be assured that the connectivity and throughput of the configured devices will be optimised.

https://t.me/learningnets

Troubleshooting VLANs and Trunking

In the previous section, we discussed the use of three CLI commands that can be used for troubleshooting Physical Layer issues. This section describes some common approaches to identifying and troubleshooting intra-VLAN connectivity issues. Some of the more common causes of intra-VLAN connectivity issues include the following:

- Duplex mismatches
- Bad NIC or cable
- Congestion
- Hardware issues
- Software issues
- Resource oversubscription
- Configuration issues

Duplex mismatches can result in very slow network performance and connectivity. While some improvements in auto-negotiation have been made, and the use of auto-negotiation is considered a valid practice, it is still possible for duplex mismatches to occur. As an example, when the NIC is set to 100/Full and the switch port is auto-negotiating, the NIC will retain its 100/Full setting, but the switch port will be set to 100/Half. Another example would be the inverse; that is, the NIC is set to auto-negotiate, while the switch port is set to 100/Full. In that case, the NIC would auto-negotiate to 100/Half, while the switch retained its static 100/Full configuration, resulting in a duplex mismatch.

It is therefore good practice to specify manually the speed and duplex settings for 10/100 Ethernet connections, where feasible, to avoid duplex mismatches with auto-negotiation. Duplex mismatches can affect not only users directly connected to the switch but also network traffic that traverses inter-switch links that have mismatched duplex settings. The port interface speed and duplex settings can be viewed using the `show interfaces` command.

NOTE: Because Catalyst switches support only full-duplex for 1Gbps links, this is not commonly an issue for GigabitEthernet connections.

Multiple counters in Cisco IOS software can be used to identify a potentially bad NIC or cabling issue. NIC or cabling issues can be identified by checking the values of certain counters in different `show` commands. For example, if the switch port counters show an incrementing number of frames with a bad CRC or with FCS errors, this can most likely be attributed either to a bad NIC on the workstation or machine or to a bad network cable.

Network congestion can also cause intermittent connectivity issues in the switched network. The first sign that your VLAN is overloaded is if the Rx or Tx buffers on a port are oversubscribed. Additionally, excessive frame drops on a port can also be an indication of network congestion. A common cause of network congestion is due to underestimating aggregate bandwidth requirements for backbone connections. In such cases, congestion issues

https://t.me/learningnets

can be resolved by configuring EtherChannels or by adding additional ports to existing EtherChannels. While network congestion is a common cause of connectivity issues, it is also important to know that the switch itself can experience congestion issues, which can have a similar impact on network performance.

Limited switch bandwidth can result in congestion issues, which can severely impact network performance. In LAN switching, bandwidth refers to the capacity of the switch fabric. Therefore, if the switch fabric is on 5Gbps and you attempt to push 7Gbps worth of traffic through the switch, the end result is packet loss and poor network performance. This is a common issue in oversubscribed platforms, where the aggregate capacity of all ports can exceed the total backplane capacity.

Hardware problems can also cause connectivity issues in the switched LAN. Examples of such issues include bad ports or bad switch modules. While you could troubleshoot such issues by looking at physical indicators such as LEDs, if possible, such issues are sometimes difficult to troubleshoot and diagnose. In most cases, you should seek the assistance of the Technical Assistance Centre (TAC) when you suspect potentially faulty hardware issues.

Software bugs are even more difficult to identify because they cause deviation, which is hard to troubleshoot. In the event that you suspect a software bug may be causing connectivity issues, you should contact the TAC with your findings. Additionally, if error messages are printed on the console or are in the logs, you can also use some of the online tools available from Cisco to implement a workaround or get a recommendation for a version of software in which the issue has been resolved and verified.

As with any other hardware device, switches have limited resources, such as physical memory. When these resources are oversubscribed, this can lead to severe performance issues. Issues such as high CPU utilisation can have a drastic impact on both switch and network performance.

Finally, as with any other technology, incorrect configurations may also cause connectivity issues, either directly or indirectly. For example, the poor placement of the Root Bridge may result in slow connectivity for users. Directly integrating or adding an incorrectly configured switch into the production network could result in an outright outage for some or all users. The following sections describe some common VLAN-related issues, their probable causes, and the actions that can be taken to remedy them.

Troubleshooting Dynamic VLAN Advertisements

Cisco Catalyst switches use VLAN Trunk Protocol (VTP) to propagate VLAN information dynamically throughout the switched domain. VTP is a Cisco proprietary Layer 2 messaging protocol that manages the addition, deletion, and renaming of VLANs for switches in the same VTP domain.

There are several reasons why a switch might not be able to receive any VLAN information dynamically when added to the VTP domain. Some common causes include the following:

- Layer 2 trunking misconfigurations

https://t.me/learningnets

- ☐ Incorrect VTP configuration
- ☐ Configuration revision number
- ☐ Physical Layer issues
- ☐ Software or hardware issues or bugs
- ☐ Switch performance issues

In order for switches to exchange VLAN information using VTP, a trunk must be established between the switches. Cisco IOS switches support both ISL and 802.1Q trunking mechanisms. While some switches default to ISL, which is a Cisco proprietary trunking mechanism, the current Cisco IOS Catalyst switches default to 802.1Q. When provisioning trunking between switches, it is considered good practice to specify manually the trunking encapsulation protocol. This is accomplished using the `switchport trunk encapsulation [isl|dot1q]` interface configuration command when configuring the link as a trunk port.

There are several commands that you can use to troubleshoot trunk connectivity issues. You can use the `show interfaces` command to verify basic port operational and administrative status. Additionally, you can append the `[trunk]` or `[errors]` keyword to perform additional troubleshooting and verification. The `show interfaces [name] counters trunk` command can be used to view the number of frames transmitted and received on trunk ports.

The output of this command also includes encapsulation errors, which can be used to verify 802.1Q and ISL, and trunking encapsulation mismatches, as illustrated in the following output:

```
Cat-3550-1#show interfaces FastEthernet0/12 counters trunk
Port        TrunkFramesTx  TrunkFramesRx  WrongEncap
Fa0/12               1696          32257           0
```

Referencing the output above, you can repeat the same command to ensure that both the Tx and Rx columns are incrementing and perform additional troubleshooting from there. For example, if the switch is not sending any frames, then the interface might not be configured as a trunk, or it might be down or disabled. If the Rx column is not incrementing, then it may be that the remote switch is not configured correctly.

Another command that can be used to troubleshoot possible Layer 2 trunk misconfigurations is the `show interfaces [name] trunk` command. The output of this command includes the trunking encapsulation protocol and mode, the native VLAN for 802.1Q, the VLANs that are allowed to traverse the trunk, the VLANs that are active in the VTP domain, and the VLANs that are pruned. A common issue with VLAN propagation is that the upstream switch has been configured to filter certain VLANs on the trunk link using the `switchport trunk allowed vlan` interface configuration command. The output of the `show interfaces [name] trunk` command is shown below:

```
Cat-3550-1#show interfaces trunk
Port        Mode             Encapsulation  Status        Native vlan
Fa0/12      desirable        n-802.1q       trunking      1
Fa0/13      desirable        n-802.1q       trunking      1
```

https://t.me/learningnets

```
Fa0/14      desirable        n-isl          trunking      1
Fa0/15      desirable        n-isl          trunking      1
Port        Vlans allowed on trunk
Fa0/12      1-4094
Fa0/13      1-4094
Fa0/14      1-4094
Fa0/15      1-4094
Port        Vlans allowed and active in management domain
Fa0/12      1-4
Fa0/13      1-4
Fa0/14      1-4
Fa0/15      1-4
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/12      1-4
Fa0/13      none
Fa0/14      none
Fa0/15      none
```

Another common trunking misconfiguration issue is native VLAN mismatches. When you are configuring 802.1Q trunks, the native VLAN must match on both sides of the trunk link; otherwise, the link will not work. If there is a native VLAN mismatch, then STP places the port in a port VLAN ID (PVID) inconsistent state and will not forward on the link. In such cases, an error message similar to the following will be printed on the console or in the log:

```
*Mar  1 03:16:43.935: %SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer
vlan id 1 on FastEthernet0/11 VLAN2.

*Mar  1 03:16:43.935: %SPANTREE-2-BLOCK_PVID_PEER: Blocking FastEthernet0/11 on VLAN0001.
Inconsistent peer vlan.

*Mar  1 03:16:43.935: %SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/11 on
VLAN0002. Inconsistent local vlan.

*Mar  1 03:16:43.935: %SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer
vlan id 1 on FastEthernet0/12 VLAN2.

*Mar  1 03:16:43.935: %SPANTREE-2-BLOCK_PVID_PEER: Blocking FastEthernet0/12 on VLAN0001.
Inconsistent peer vlan.

*Mar  1 03:16:43.939: %SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/12 on
VLAN0002. Inconsistent local vlan.
```

While STP troubleshooting will be described later in this guide, this inconsistent state could be validated using the `show spanning-tree` command, as illustrated below:

```
Cat-3550-1#show spanning-tree interface FastEthernet0/11
Vlan                Role Sts  Cost      Prio.Nbr Type
------------------- ---- ---  --------- -------- ----------------
VLAN0001            Desg BKN* 19        128.11   P2p *PVID_Inc
VLAN0002            Desg BKN* 19        128.11   P2p *PVID_Inc
```

https://t.me/learningnets

If you have checked and validated that the trunk is indeed correctly configured and operational

between the two switches, then the next step would be to validate VTP configuration parameters. These parameters include the VTP domain name, the correct VTP mode, and the VTP password, if one has been configured for the domain, using the `show vtp status` and `show vtp password` commands, respectively. The output of the `show vtp status` command is shown below:

```
Cat-3550-1#show vtp status
VTP Version                     : running VTP2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : TSHOOT
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x26 0x99 0xB7 0x93 0xBE 0xDA 0x76 0x9C
...
[Truncated Output]
```

When using the `show vtp status` command, ensure that the switches are running the same version of VTP. By default, Catalyst switches run VTP version 1. A switch running VTP version 1 cannot participate in a VTP version 2 domain. If the switch is incapable of running VTP version 2, then all VTP version 2 switches should be configured to run version 1 instead using the `vtp version` global configuration command.

NOTE: If you change the VTP version on the server, then the change will be propagated automatically to client switches in the VTP domain.

VTP propagation is enabled for VTP client/server or server/server devices. If VTP is disabled on a switch (i.e., transparent mode), then the switch will not receive VLAN information dynamically via VTP. However, be mindful of the fact that with version 2, transparent mode switches will forward received VTP advertisements out of their trunk ports and act as VTP relays. This happens even if the VTP version is not the same. The VTP domain name should also be consistent on the switches.

Finally, the output of the `show vtp status` command also includes the MD5 hash used for authentication purposes. This hash, which is derived from the VTP domain name and password, should be consistent on all switches in the domain. If the VTP passwords or domain names are different on the switches, then the calculated MD5 will also be different. If the domain name or password is different, then the `show vtp status` command will indicate an MD5 digest checksum mismatch, as illustrated in the following output:

```
Cat-3550-1#show vtp status
VTP Version                     : running VTP2
Configuration Revision          : 0
```

https://t.me/learningnets

```
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : TSHOOT
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 Digest                      : 0x26 0x99 0xB7 0x93 0xBE 0xDA 0x76 0x9C
*** MD5 digest checksum mismatch on trunk: Fa0/11 ***
*** MD5 digest checksum mismatch on trunk: Fa0/12 ***
...
[Truncated Output]
```

Finally, the configuration revision number can wreak havoc when using VTP. Switches use the configuration revision number to keep track of the most recent information in the VTP domain. Every switch in the domain stores the configuration revision number that it last heard from a VTP advertisement, and this number is incremented every time new information is received. When any switch in the VTP domain receives an advertisement message with a higher configuration revision number than its own, it will overwrite any stored VLAN information and synchronise its own stored VLAN information with the information received in the advertisement message.

Therefore, if you are wondering why the switch that you integrated into the VTP domain is not receiving any VLAN information, it may be that the same switch had a higher configuration revision number and caused all other switches to overwrite their local VLAN information and replace it with the information received in the advertisement message from the new switch. To avoid such situations, always ensure that the configuration revision number is set to 0 prior to integrating a new switch into the domain. This can be done by changing the VTP mode or changing the VTP domain name on the switch. The configuration revision number is included in the output of the `show vtp status` command.

Troubleshooting Loss of End-to-End Intra-VLAN Connectivity

There are several possible reasons for a loss of end-to-end connectivity within a VLAN. Some of the most common causes include the following:

- Physical Layer issues
- VTP pruning
- VLAN trunk filtering
- New switches
- Switch performance issues
- Network congestion

https://www.teagents.net

- Software or hardware issues or bugs

NOTE: For brevity, only trunking, VTP pruning, trunk filtering, and the integration of new switches into the domain will be described in this section. Software or hardware issues or bugs and switch performance issues are described throughout this guide. Physical Layer troubleshooting was described earlier in this module.

VTP pruning removes VLANs from the VLAN database of the local switch when no local ports are a part of that VLAN. VTP pruning increases the efficiency of trunks by eliminating unnecessary Broadcast, Multicast, and unknown traffic from being flooded across the network.

While VTP pruning is a desirable feature to implement, incorrect configuration or implementation can result in a loss of end-to-end VLAN connectivity. VTP pruning should be enabled only in client/server environments. Implementing pruning in a network that includes transparent mode switches may result in a loss of connectivity. If one or more switches in the network are in VTP transparent mode, you should either globally disable pruning for the entire domain or ensure that all VLANs on the trunk link(s) to the upstream transparent mode switch(es) are pruning ineligible (i.e., they are not pruned), using the `switchport trunk pruning vlan` interface configuration command under the applicable interfaces.

Verify Allowed VLANs and Trunk Status

In addition to VTP pruning, incorrectly filtering VLANs on switch trunk links can result in a loss of end-to-end VLAN connectivity. By default, all VLANs are allowed to traverse all trunk links; however, Cisco IOS software allows administrators to remove (or add) VLANs selectively to specific trunk links using the `switchport trunk allowed vlan` interface configuration command. You can use the `show interfaces [name] trunk` and the `show interfaces [name] switchport` commands to view pruned and restricted VLANs on trunk links. The output of the `show interfaces [name] trunk` command, which is the easiest way to verify the allowed VLANs on a trunk, is shown below:

```
Cat-3550-1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/1       1,10,20,30,40,50
Fa0/2       1-99,201-4094
Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,40,50
Fa0/2       1,10,20,30,40,50,60,70,80,90,254
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,40,50
Fa0/2       1,40,50,60,70,80,90,254
```

You should also check that the correct VLANs are advertised on your trunk links. Inproper VLANs allowed on the link can lead to a lack of functionality or security issues. Also, you want to make sure the same VLANs are allowed on both ends of a trunk.

NOTE: You should be very careful not to forget the [add] keyword when adding another VLAN(s) that should be allowed over a trunk link. For example, if you already have `switchport trunk allowed vlan 10, 20` configured and you want to allow VLAN 30 as well, you need to enter the command `switchport trunk allowed vlan add 30`. If you simply configured `switchport trunk allowed vlan 30`, previously permitted VLANs 10 and 20 would be removed from the trunk, which would cause a break of communication for VLANs 10 and 20.

Another important piece of information that is offered by the `show interface trunk` command is the trunk status. This confirms whether the trunk is formed or not and has to be checked at both ends of the link. If the interface is not in "trunking" mode, one of the most important things that have to be verified is the mode of operation (on, auto, etc.) to see whether it allows forming a trunking state with the other end of the link.

Verify Encapsulation Type

Another important step in resolving trunking problems is verifying that the correct encapsulation is configured at both ends of a trunk link. Most Cisco switches allow both ISL and dot1Q encapsulation types. Althouth most modern network designs use dot1Q, there might be situations in which ISL is the preferred method. The encapsulation type is configured using the `switchport trunk encapsulation <type>` command. Some of the commands that can be used to verify the encapsulation types are:

- `show interface trunk`
- `show interface <number> switchport`

The output of the `show interfaces [name] switchport` command on a port that has been configured statically as an 802.1Q trunk link is shown below:

```
Cat-3550-2#show interfaces FastEthernet0/7 switchport
Name: Fa0/7
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
```

https://t.me/learningnets

```
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 3,5,7
Pruning VLANs Enabled: 2-8
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

As was described in the previous section, the integration of a new switch into the network can result in a loss of VLAN information in the management domain. This loss of VLAN information can result in a loss of connectivity between devices within the same VLAN. Ensure that the configuration revision number is reset prior to integrating a new switch into the LAN.

Using the "show vlan" Command

In addition to the commands that were described in the previous sections, there are additional Cisco IOS software commands that are useful for both verifying and troubleshooting VLAN configurations. One of the most commonly used VLAN verification and troubleshooting commands is the `show vlan` command. This command displays parameters for all VLANs within the administrative domain, as illustrated in the following output:

```
Cat-3550-1#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/11, Fa0/12,
                                                Fa0/13, Fa0/14,
                                                Fa0/20, Fa0/21,
                                                Fa0/22, Fa0/23,
                                                Fa0/24
150  VLAN_150                         active    Fa0/2, Fa0/3, Fa0/4,
                                                Fa0/5, Fa0/6, Fa0/7,
                                                Fa0/8, Fa0/9, Fa0/10
160  VLAN_160                         active    Fa0/15, Fa0/16,
                                                Fa0/17, Fa0/18,
                                                Fa0/19
170  VLAN_170                         active    Gi0/1, Gi0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

https://t.me/learningnets

```
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode
---- ----- ---------- ----- ------ ------ -------- ---- --------
1    enet  100001     1500  -      -      -        -    -
150  enet  100150     1500  -      -      -        -    -
160  enet  100160     1500  -      -      -        -    -
170  enet  100170     1500  -      -      -        -    -
1002 fddi  101002     1500  -      -      -        -    -
1003 tr    101003     1500  -      -      -        -    -
1004 fdnet 101004     1500  -      -      -        ieee -
1005 trnet 101005     1500  -      -      -        ibm  -
Trans1 Trans2
------ ------
0      0
0      0
0      0
0      0
0      0
0      0
0      0
0      0
Remote SPAN VLANs
------------------------------------------------------------
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------
```

This command prints all available VLANs, along with the ports that are assigned to each of the individual VLANs. Only access ports, regardless of whether they are up or down, will be included in the output of this command. Trunk links will not be included, as these belong to all VLANs. The `show vlan` command also provides information on RSPAN VLANs, as well as Private VLAN (PVLAN) configuration on the switch (this is a CCNP subject). The `show vlan` command can be used with additional keywords to provide information that is more specific. The following output displays the supported additional keywords that can be used with this command:

```
Cat-3550-1#show vlan ?
  brief         VTP all VLAN status in brief
  id            VTP VLAN status by VLAN id
  ifindex       SNMP ifIndex
  name          VTP VLAN status by VLAN name
  private-vlan  Private VLAN information
  remote-span   Remote SPAN VLANs
  summary       VLAN summary information
  |             Output modifiers
```

https://t.me/learningnets

```
  <cr>
```

The `brief` field prints a brief status of all active VLANs. The output that is printed by this command is the same as the output above, with the only difference being that the last two sections will be omitted. The `id` field provides the same information as the `show vlan` command, but only for the specified VLAN, as shown in the following output:

```
Switch-1#show vlan id 150

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------
150  VLAN_150                         active    Fa0/1, Fa0/2, Fa0/3,
                                                Fa0/4, Fa0/5, Fa0/6,
                                                Fa0/7, Fa0/8, Fa0/9,
                                                Fa0/10
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode
---- ----- ---------- ----- ------ ------ -------- ---- --------
150  enet  100150     1500  -      -      -        -    -
Trans1 Trans2
------ ------
0      0
0      0
Remote SPAN VLAN
----------------
Disabled
Primary Secondary Type              Ports
------- --------- ----------------- --------------------------------
```

Again, the VLAN name is included in the output, as are all of the access ports that belong to the VLAN. Trunk ports are not included in this output because they belong to all VLANs. Additional information also includes the VLAN MTU, RSPAN configuration (if applicable), and PVLAN configuration parameters (if applicable).

The `name` field allows the VLAN name to be specified instead of the ID. This command prints the same information as the `show vlan id <number>` command. The `ifindex` field displays the SNMP IfIndex for the VLAN (if applicable), while the `private-vlan` and `remote-span` fields print PVLAN and RSPAN configuration information, respectively. Finally, the `summary` field prints a summary of the number of VLANs that are active in the management domain. This includes standard and extended VLANs.

The `show vlan` command, with or without parameters, is the most useful command in the following aspects of the troubleshooting process:

- Identifying that VLANs are configured on the device
- Verifying port membership

Another useful VLAN troubleshooting command is the `show vtp counters` command. This

https://t.me/learningnets

command prints information on VTP packet statistics. The output of the `show vtp counters` command on a switch configured as a VTP server (default) is shown below:

```
Cat-3550-1#show vtp counters
VTP statistics:
Summary advertisements received    : 15
Subset advertisements received     : 10
Request advertisements received    : 2
Summary advertisements transmitted : 19
Subset advertisements transmitted  : 12
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0
VTP pruning statistics:
Trunk   Join Transmitted  Join Received   Summary advts received
                                          from non-pruning-
                                          capable device
-----   ----------------  --------------  -----------------------
Fa0/11                0                1                         0
Fa0/12                0                1                         0
```

The first six lines of the output printed by the `show vtp counters` command provide the statistics for the three types of VTP packets: advertisement requests, summary advertisements, and subset advertisements. These different messages will be described in the following section.

VTP advertisement requests are requests for configuration information. These messages are sent by VTP clients to VTP servers to request VLAN and VTP information they may be missing. A VTP advertisement request is sent out when the switch resets, the VTP domain name changes, or in the event that the switch has received a VTP summary advertisement frame with a higher configuration revision number than its own. VTP servers should show only the received counters incrementing, while any VTP clients should show only the transmitted counters incrementing.

VTP summary advertisements are sent out by servers every five minutes, by default. These types of messages are used to tell an adjacent switch of the current VTP domain name the configuration revision number and the status of the VLAN configuration, as well as other VTP information, which includes the time stamp, the MD5 hash, and the number of subset advertisements to follow. If these counters are incrementing on the server, then there is more than one switch acting or configured as a server in the domain.

VTP subset advertisements are sent out by VTP servers when a VLAN configuration changes, such as when a VLAN is added, suspended, changed, deleted, or other VLAN-specific parameters (e.g., VLAN MTU) have changed. One or more subset advertisements will be sent following the VTP summary advertisement. A subset advertisement contains a list of VLAN information. If

https://t.me/learningnets

there are several VLANs, more than one subset advertisement may be required in order to advertise all the VLANs.

The `Number of config revision errors` field shows the number of advertisements that the switch cannot accept because it received packets with the same configuration revision number but with a different MD5 hash value. This is common when changes are made to two or more server switches in the same domain at the same time and an intermediate switch receives these advertisements at the same time. This concept is illustrated in Figure 15.3 below, which illustrates a basic switched network:

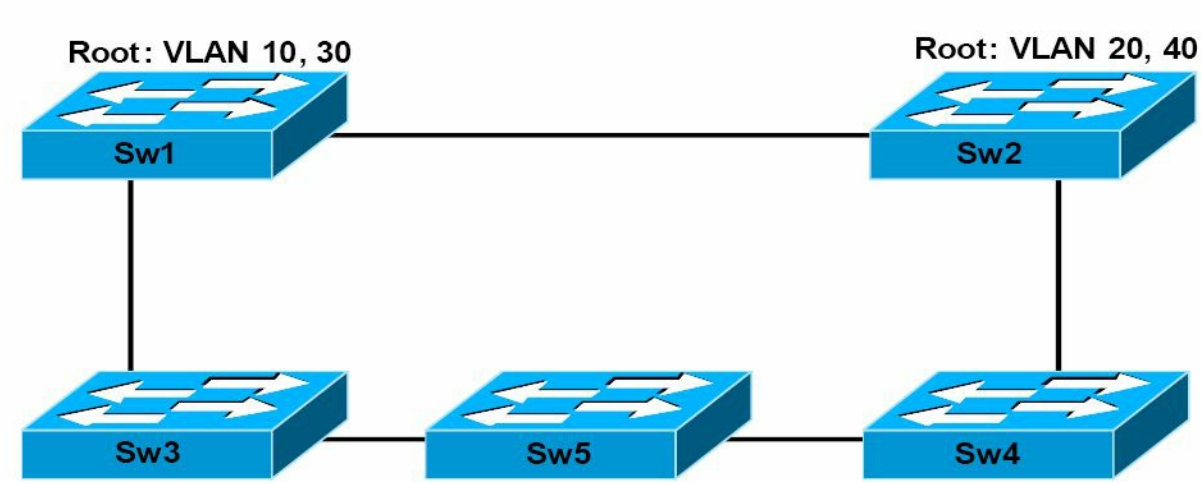


Figure 15.3 – Troubleshooting Configuration Revision Number Errors

Figure 15.3 illustrates a basic network that incorporates redundancy and load sharing. It should be assumed that Sw1 and Sw2 are configured as servers, while Sw3 is configured as a client. Sw1 is the root for VLANs 10 and 30, while Sw2 is the root for VLANs 20 and 40. Assume that a simultaneous change is implemented on Sw1 and Sw2, adding VLAN 50 to Sw1 and VLAN 60 to Sw2. Both switches send out an advertisement following the change to the database.

The change is propagated throughout the domain, overwriting the previous databases of the other switches that receive this information. Assume that Sw5 receives the same information from neighbours at the same time and both advertisements contain the same configuration revision number. In such situations, the switch will not be able to accept either advertisement because they have the same configuration revision number but different MD5 hash values.

When this occurs, the switch increments the `Number of config revision errors counter` field and does not update its database. This situation can result in a loss of connectivity within one or more VLANs because VLAN information is not updated on the switch. To resolve this issue and ensure that the local database on the switch is updated, configure a dummy VLAN on one of the server switches, which results in another update with an incremented configuration revision number. This will overwrite the local database of all switches, allowing Sw5 to update its database as well. Keep in mind that this is not a common occurrence; however, it is possible, hence, the reason for this counter.

The `Number of config digest errors counter` field increments whenever the switch receives an advertisement with a different MD5 hash value than it calculated. This is the result of different VTP passwords configured on the switches. You can use the `show vtp password` command to verify that the configured VTP password is correct. It is also important to remember that the

https://t.me/learningnets

passwords may be the same, but hardware or software issues or bugs could be causing data corruption of VTP packets, resulting in these errors.

Finally, the `VTP pruning statistics` field will only ever contain non-zero values when pruning is enabled for the VTP domain. Pruning is enabled on servers and this configuration is propagated throughout the VTP domain. Servers will receive joins from clients when pruning has been enabled for the VTP domain.

https://t.me/learningnets

Day 15 Questions

1. What is the colour of the system LED under normal system operations?
2. What is the colour of the RPS LED during a fault condition?
3. You can cycle through modes by pressing the Mode button until you reach the mode setting you require. This changes the status of the port LED colours. True or false?
4. What port speed is represented by a blinking green LED?
5. If you want to be sure that you are not dealing with a cabling issue, one of the simplest things to do is to _____ the cable and run the same tests again.
6. Which command is generally used to troubleshoot Layer 1 issues (besides `show interfaces`)?
7. The _____ status is reflected when the connected cable is faulty or when the other end of the cable is not connected to an active port or device (e.g., if a workstation connected to the switch port is powered off).
8. What are runts?
9. The _____ command can also be used to view interface errors and facilitate Layer 1 troubleshooting.
10. Which command prints a brief status of all active VLANs?

https://t.me/learningnets

Day 15 Answers

1. Green.
2. Amber.
3. True.
4. 1000Mbps.
5. Replace.
6. The `show controllers` command.
7. `notconnect`.
8. Packets that are smaller than the minimum packet size (less than 64 bytes on Ethernet).
9. `show interfaces [name] counters errors`.
10. The `show vlan brief` command.

https://t.me/learningnets

Day 15 Labs

Layer 1 Troubleshooting Lab

Test the relevant Layer 1 troubleshooting commands presented in this module on real devices:

- ☐ Examine switch system and port LED status for different scenarios, as described in the module
- ☐ Issue a `show interface` command and examine all the related information as per the description in this module
- ☐ Issue the same for `show controllers` and `show interface counters errors` commands

Layer 2 Troubleshooting Lab

Test the relevant Layer 2 troubleshooting commands presented in this module on real devices:

- ☐ Configure VTP between the switches and advertise some VLANs from the VTP server to the VTP client (see the VTP lab in Day 3)
- ☐ Configure a trunk between two switches and generate some traffic (ping)
- ☐ Test the `show vlan` command
- ☐ Test the `show interface counters trunk` command
- ☐ Test the `show interface switchport` command
- ☐ Test the `show interface trunk` command
- ☐ Test the `show VTP status` command
- ☐ Test the `show VTP counter` command

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 16 – Review 1

Welcome to your first review day. I told you that you'd have plenty of time for going over previous lessons!

We have covered pretty much everything you need to know to get through the ICND1 exam. If you are doing the full CCNA exam, then you still need to review everything you have learned so far. I don't want to dwell on the more ambiguous areas, such as the OSI model or CSMA/CD, because they are less likely to come up in the exam, and because the few facts you need to know should be easily remembered AND you can review them in the cram guide.

Day 16 Tasks

- Take the OSI exam below
- Complete the switching and switch security challenge labs
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website

Day 16 Exam

1. Data take the form of segments at which OSI layer?
2. Which OSI layer deals with compression?
3. Which OSI layer sets up, manages, and terminates dialogues across the network?
4. Logical addressing takes place at which OSI layer?
5. Flow control, windowing, and acknowledgements take place at which OSI layer?
6. What are the typical types of Layer 1 network issues?
7. Name the four layers of the TCP (DoD) model.
8. Which TCP layer maps to the Transport Layer of the OSI model?
9. MAC addresses correspond to which OSI layer?
10. Name two protocols used at the Transport Layer.

Day 16 Answers

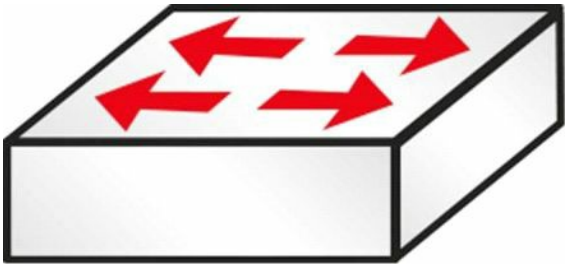
1. The Transport Layer.
2. The Presentation Layer.
3. The Session Layer.
4. The Network Layer.
5. The Transport Layer.
6. Bad cables and hub issues.
7. Network Interface/Internet/Transport/Application Layers.

https://t.me/learningnets

8. The Transport Layer.
9. The Data Link Layer.
10. TCP and UDP.

Day 16 Lab 1 – Switch Configuration

Topology



Instructions

Follow Day 2 Lab.

Day 16 Lab 2 – Switch Security

Topology



Instructions

Connect to the switch using a console connection. Connect a PC to the switch or connect the switch to the FastEthernet port on a router:

1. Add port security to an interface on the switch
2. Hard set the MAC address of the PC/router interface as the permitted address
3. Ensure that the switch interface is up (and an IP address is on the PC)
4. Set the port security violation action to “restrict”
5. Change the MAC address of the PC, or plug in another machine
6. Issue a `show port-security interface x` command on the switch

Solution Hints and Commands

- Before configuring port security, it is recommended that the switch port be statically configured as a Layer 2 access port. This configuration is illustrated in the following output:

```
VTP-Server-1(config)#interface FastEthernet0/1
```

https://t.me/learningnets

```
VTP-Server-1(config-if)#switchport
VTP-Server-1(config-if)#switchport mode access
```

- ☐ Use the `switchport port-security` command to enable port security on a switch interface
- ☐ Use the `switchport port-security mac-address xxxx.xxxx.xxxx` command to hard set the MAC address as the permit address
- ☐ Use the `show ip interface brief` command to verify interface status
- ☐ Use the `switchport port-security violation restrict` command to configure violation action
- ☐ Use the `show port-security` command

https://t.me/learningnets

Day 17 – Review 2

In this review session, we will be going over the earlier lessons to cement in hands-on knowledge. I know you have been choosing which labs to follow, but I'm going to suggest which ones to do here. Whatever you do, don't keep repeating the same labs once you have mastered them. Mix up the IP addresses and the router interfaces and do it all from memory.

If you have to look up commands to remember them, you won't get through the exam, so, as fast as possible, commit the configuration commands to memory.

Day 17 Tasks

- Take the cables exam below
- Review all switching theory
- Review the labs in Days 1 to 5
- Complete some of the previous switching labs
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website

Day 17 Exam

1. You are trying to find a crossover cable. When you look at the pin colours, what are you looking for?
2. What is the minimum category of cable which can support 100Mbps?
3. You want to configure an Ethernet interface to enable traffic to pass in both directions at the same time. In `Switch(config-if)#` mode, what do you type?
4. At the `Switch(config-if)#` prompt, you want to change the speed from auto to 100. What do you type?
5. What could you connect to using a crossover cable?
6. You can easily use a straight-through Ethernet cable to connect to a router console port if a rollover/console cable is not available. True or false?
7. Switches contain a memory chip known as an _____, which builds a table listing which device is plugged into which port.
8. The `show` _____-_____-_____ command displays a list of which MAC addresses are connected to which ports.
9. Which two commands add an IP address to the VLAN?
10. Which commands will enable Telnet and will add a password to the switch Telnet lines?

Day 17 Answers

1. The wire pin 1 at one end needs to connect to pin 3 on the other end, and pin 2

needs to connect to pin 6 on the other end.

2. Cat5.
3. `duplex full`.
4. `speed 100`.
5. PC-to-PC, switch-to-switch, and router-to-router.
6. False.
7. ASIC.
8. `mac-address-table`.
9. The `interface vlan x` and `ip address x.x.x.x` commands.
10. The `Switch1(config)#line vty 0 15`, `Switch1(config-line)#password cisco`, and `Switch1(config-line)#login` commands.

https://t.me/learningnets

Day 18 – Review 3

Day 18 Tasks

- Read IP addressing theory notes
- Take the subnetting exam below
- Complete today's three NAT challenge labs
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website
- Watch the network design videos on www.in60days.com

Day 18 Exam

1. Which subnet is host 200.200.100.103/27 in?
2. Which subnet is host 190.100.23.45/28 in?
3. Which subnet is host 19.200.12.120/13 in?
4. Which subnet is host 100.123.45.12/15 in?
5. Which subnet is host 130.23.34.3/18 in?
6. Network 192.168.1.0 needs subnetting to create three subnets, each with at least 20 hosts. Which subnet mask needs to be applied? (You need to watch the design videos first.)
7. Network 200.100.1.0 needs subnetting to create five subnets, each with at least 30 hosts. Which subnet mask needs to be applied?
8. Network 30.0.0.0 needs subnetting to create 200 subnets, with as many hosts as possible. Which subnet mask needs to be applied?
9. Network 192.168.1.0 needs subnetting to create subnets that will contain only two hosts. Which subnet mask needs to be applied?
10. Network 170.24.0.0 needs subnetting to create 100 subnets, each with at least 500 hosts. Which subnet mask needs to be applied?

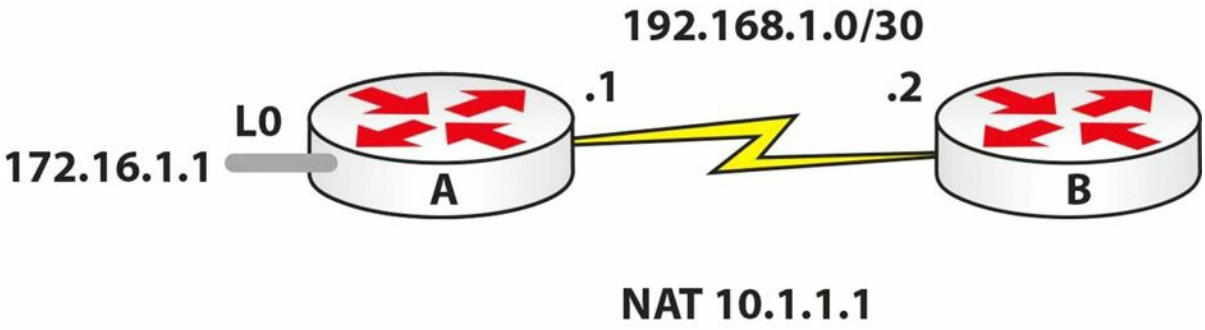
Day 18 Answers

1. 200.200.100.96
2. 190.100.23.32
3. 19.200.0.0
4. 100.122.0.0
5. 130.23.0.0
6. 255.255.255.192

7. 255.255.255.224
8. 255.255.0.0
9. 255.255.255.252
10. 255.255.254.0

Day 18 Lab 1 – Static NAT

Topology



Instructions

Connect two routers together with a serial or crossover cable:

1. Add IP addresses to the routers and a Loopback interface on Router A, according to the diagram; the 172 network can use the default subnet mask
2. Designate NAT inside and outside interfaces
3. Add a static route on Router B to send all traffic back to Router A
4. Ping between Router A and Router B to test the serial line (remember clock rates)
5. Create a static NAT for 172.16.1.1 to 10.1.1.1 and turn on NAT debugging
6. Do an extended ping source from Loopback 0
7. Check the NAT translation table

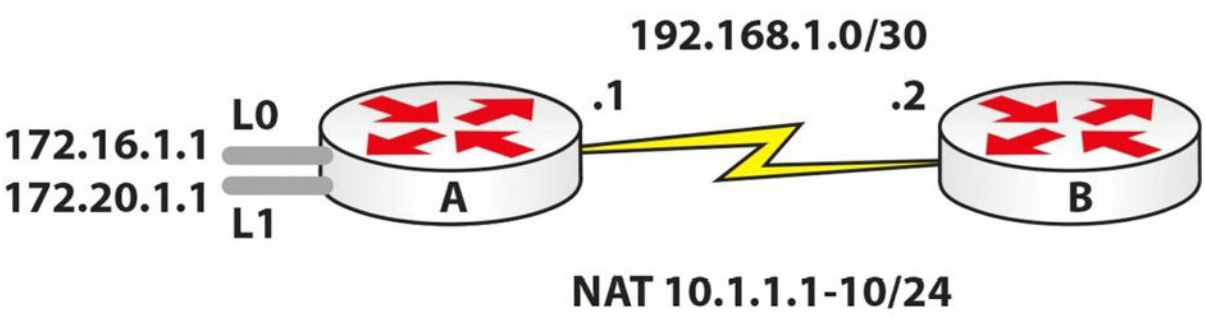
Solution Hints and Commands

- `ip nat inside` command and `ip nat outside` command on the interfaces
- `ip route` global configuration command to add static route
- Static NAT: `ip nat inside source static x.x.x.x  y.y.y.y` command
- `show ip nat translations` command to check the NAT translation table

Day 18 Lab 2 – NAT Pool

Topology

https://t.me/learningnets



Instructions

Connect two routers together with a serial or crossover cable:

1. Add IP addresses to the routers and a Loopback interface on Router A, according to the diagram
2. Designate NAT inside and outside interfaces
3. Add a static route on Router B to send all traffic back to Router A
4. Ping between Router A and Router B to test the serial line (remember clock rates)
5. Create a NAT pool of 10.1.1.1 to 10, inclusive
6. Create two ACL lines to permit the Loopback networks (/16)
7. Configure the NAT pool, using the defined pool and ACL
8. Turn on NAT debugging
9. Source two extended pings, one each from L0 and L1
10. Check the NAT translation table

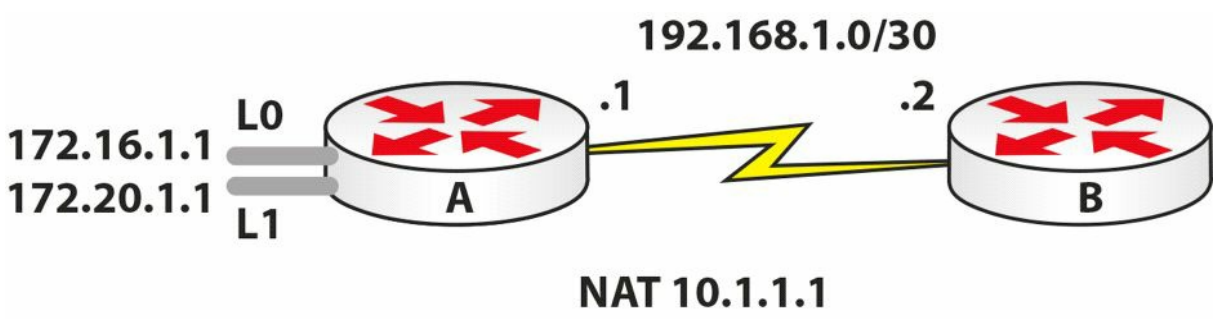
Solution Hints and Commands

- ☐ `ip nat inside` command and `ip nat outside` command on the interfaces
- ☐ `ip route` global configuration command to add static route
- ☐ `ip nat pool name <start_ip> <end_ip> netmask <mask>` command
- ☐ `access-list x permit y.y.y.y` command
- ☐ `ip nat inside source list x pool <name>` command
- ☐ `debug ip nat [detailed]` command
- ☐ `show ip nat translations` command to check the NAT translation table

Day 18 Lab 3 – NAT Overload

Topology

https://t.me/learningnets



Instructions

Connect two routers together with a serial or crossover cable:

1. Add IP addresses to the routers and a Loopback interface on Router A, according to the diagram
2. Designate NAT inside and outside interfaces
3. Add a static route on Router B to send all traffic back to Router A
4. Ping between Router A and Router B to test the serial line (remember clock rates)
5. Create a NAT pool of address 10.1.1.1 only and overload this pool (address)
6. Create two ACL lines to permit the Loopback networks (/16)
7. Configure NAT overload using the defined pool and ACL
8. Turn on NAT debugging
9. Source two extended pings, one each from L0 and L1
10. Check the NAT translation table

Solution Hints and Commands

- ☐ Hint: `Router(config)#ip nat pool <name> 10.1.1.1 10.1.1.1 prefix-length 24` command
- ☐ `ip nat inside source list x pool <name> overload` command

https://t.me/learningnets

Day 19 – Review 4

Day 19 Tasks

- Review switch security
- Take the subnetting exam below
- Follow the DHCP lab in Day 14
- Complete the DHCP challenge lab below
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website

Day 19 Exam

1. Which subnet is host 200.200.100.103/29 in?
2. Which subnet is host 190.100.23.45/25 in?
3. Which subnet is host 19.200.12.120/15 in?
4. Which subnet is host 100.12.45.12/15 in?
5. Which subnet is host 130.23.34.3/27 in?
6. Network 192.168.1.0 needs subnetting to create five subnets, each with at least 20 hosts. Which subnet mask needs to be applied?
7. Network 200.100.1.0 needs subnetting to create eight subnets, each with at least 15 hosts. Which subnet mask needs to be applied?
8. Network 30.0.0.0 needs subnetting to create 260 subnets, each with at least 1000 hosts. Which subnet mask needs to be applied?
9. Network 200.168.1.0 needs subnetting to create subnets that will contain only two hosts. Which subnet mask needs to be applied?
10. Network 170.24.0.0 needs subnetting to create 10 subnets, each with at least 500 hosts. Which subnet mask needs to be applied?

Day 19 Answers

1. 200.200.100.96
2. 190.100.23.0
3. 19.200.0.0
4. 100.12.0.0
5. 130.23.34.0
6. 255.255.255.224
7. 255.255.255.224

https://t.me/learningnets

8. 255.255.128.0
9. 255.255.255.252
10. 255.255.240.0

Day 19 Lab – DHCP

Topology



Instructions

Connect a PC to a router Ethernet interface:

1. Configure IP address 10.0.0.1/8 onto the router
2. Create a DHCP pool for the 10.0.0.0/8 network
3. Add an excluded address of the router interface
4. Add a default router address of 192.168.1.1
5. Configure the PC to obtain the IP address via DHCP
6. Check the IP configuration of the PC for the IP address assignment
7. Check the router to verify that an IP address is assigned to the PC

Solution Hints and Commands

- ☐ `Service dhcp` command to enable DHCP service
- ☐ `Router(config)#ip dhcp pool SUBNET_A` command
- ☐ `Router(dhcp-config)#network x.x.x.x` command
- ☐ `Router(dhcp-config)#default-router x.x.x.x` command
- ☐ `Router(dhcp-config)#dns-server x.x.x.x` command
- ☐ `Router(dhcp-config)#domain-name xxxx` command
- ☐ `Router(dhcp-config)#lease x` command
- ☐ `ip dhcp excluded-address <start_ip> <end_ip>` command
- ☐ `Show ip dhcp binding` command

https://t.me/learningnets

Day 20 – Review 5

We are a few short days away from completing the ICND1 part of the course. I hope you have the exam booked if you are doing the two-exam route. There are lots of free challenge labs on www.in60days.com.

Day 20 Tasks

- Take the exam below
- Review routing and ACLs
- Complete the static routes challenge lab below
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website

Day 20 Exam

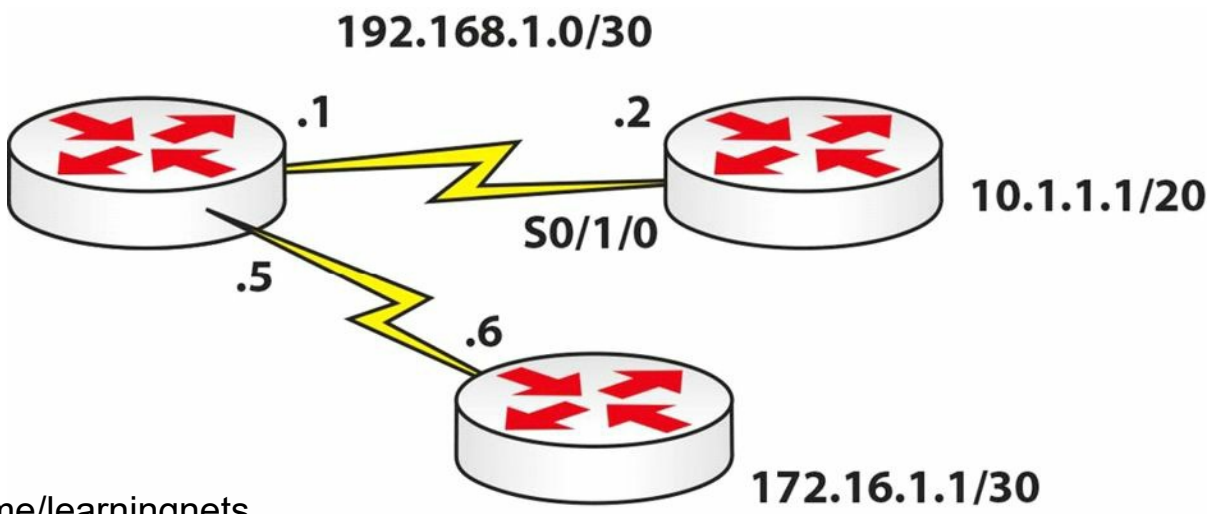
1. _____ operates at the data plane and is a topology-driven proprietary switching mechanism that creates a forwarding table that is tied to the routing table (i.e., the control plane).
2. CEF uses a _____ to make IP destination prefix-based switching decisions.
3. The Link State routing protocol is a routing protocol that uses distance or hop count as its primary metric for determining the best forwarding path. True or false?

Day 20 Answers

1. CEF
2. FIB
3. False

Day 20 Lab – Static Routes

Topology



https://t.me/learningnets

Instructions

Connect three routers together with Serial or Ethernet connections:

1. Configure the connections between the routers and ping
2. Add Loopback addresses to the two spoke routers, as per the diagram
3. Add a static route exit interface on the hub router for the 10.1.1.0/20 subnet
4. Add a next-hop address for network 172.16.1.0/30
5. Ping both networks
6. Issue a `show ip route 172.16.1.1` command and a `show ip route 10.1.1.1` command
7. Confirm that you have the exit interface and next hop listed

Solution Hints and Commands

- `ip route <network> <mask> serial <int_name>` command

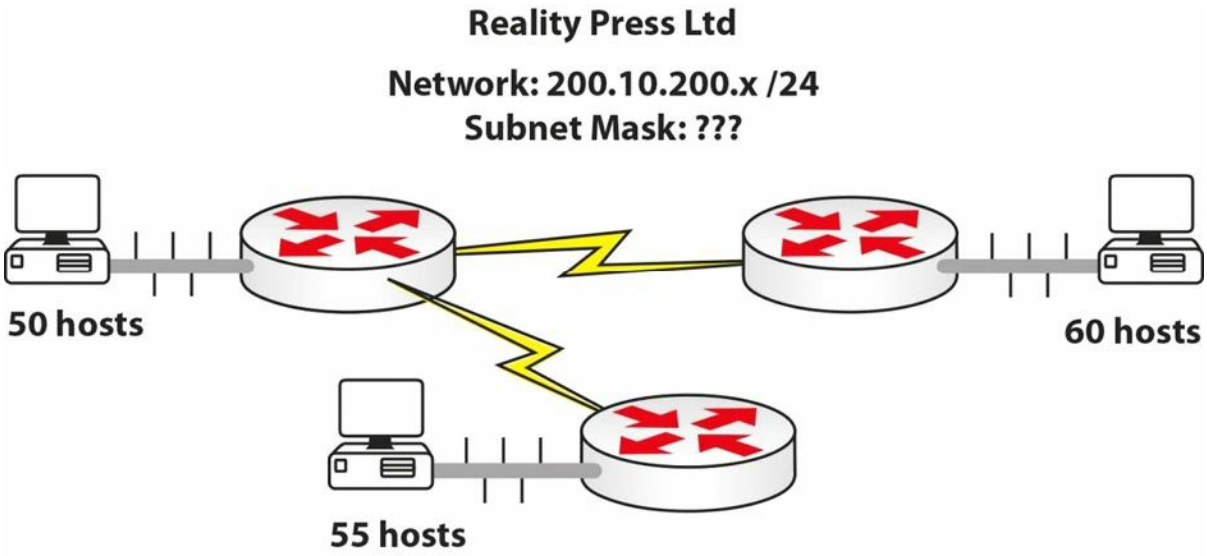
https://t.me/learningnets

Day 21 – Review 6

Day 21 Tasks

- Take the VLSM exam below
- Review VLSM (if required)
- Complete any challenge lab you wish
- Read the ICND1 cram guide
- Review the IP addressing lesson
- Spend 15 minutes on the subnetting.org website

Day 21 Exam



You are the network administrator for the network 200.10.200.0/24. You are asked to redesign the network to cater for a change in the company. Now they require the network to be broken into three smaller networks. One requires 55 hosts, one requires 50, and another 60. There will also be two WAN connections required.

Day 21 Answers

One proposal could be like this:

55 hosts: 200.10.200.0/26

50 hosts: 200.10.200.128/26

60 hosts: 200.10.200.64/26

Spare network: 200.10.200.192/26. This can be further subnetted for the WAN links:

Point-to-Point network 1: 200.10.200.192/30

Point-to-Point network 2: 200.10.200.196/30

https://t.me/learningnets

Day 22 – Review 7

Day 22 Tasks

- Take the exam below
- Review any theory (if required)
- Complete any challenge lab
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website

Day 22 Exam

1. What is the administrative distance (AD) for RIP?
2. Which protocol has an AD of 90?
3. Which protocol has an AD of 110?
4. What is the AD for a next-hop address?
5. Is RIPv2 classful or classless?
6. Which TCP service uses port 22?
7. Name port 53.
8. UDP port 69 is used by _____.
9. SMTP uses which port?

Day 22 Answers

1. 120.
2. EIGRP.
3. OSPF.
4. 1.
5. Classless.
6. SSH.
7. DNS.
8. TFTP.
9. TCP 25.

https://t.me/learningnets

Day 23 – Review 8

Day 23 Tasks

- Take the exam below
- Review any theory (if required) or NAT
- Complete the challenge lab below
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website

Day 23 Exam

1. Write down the commands to configure a DHCP pool on a router for network addresses 172.16.1.0 to 10. Exclude one of the addresses. Add a lease of two days and a DNS IP address.
2. Which command will turn off CDP for the entire router? Which command will turn off CDP for the interface only?
3. Convert 192.160.210.177 into binary (without using a calculator).
4. Convert 10010011 into decimal.
5. What is the private range of IP addresses?
6. Write out the subnet mask from CIDR /20.
7. Write out the subnet mask from CIDR /13.
8. 192.168.1.128/26 gives you how many available addresses?
9. What is the last host of the 172.16.96.0/19 network?
10. Starting with 192.168.1.0/24, with VLSM you can use a /26 mask and generate which subnets?

Day 23 Answers

1.
```
ip dhcp excluded-address 172.16.1.11 172.16.1.255
    ip dhcp pool CCNA
network 172.16.0.0 255.255.0.0
dns-server 8.8.8.8
lease 2
```
2. The `no cdp run` command turns off CDP for the entire router and the `no cdp enable` command turns off CDP on the interface only.
3. 11000000.10100000.11010010.10110001.
4. 147.
5. 10.x.x.x – any address starting with a 10

https://t.me/learningnets

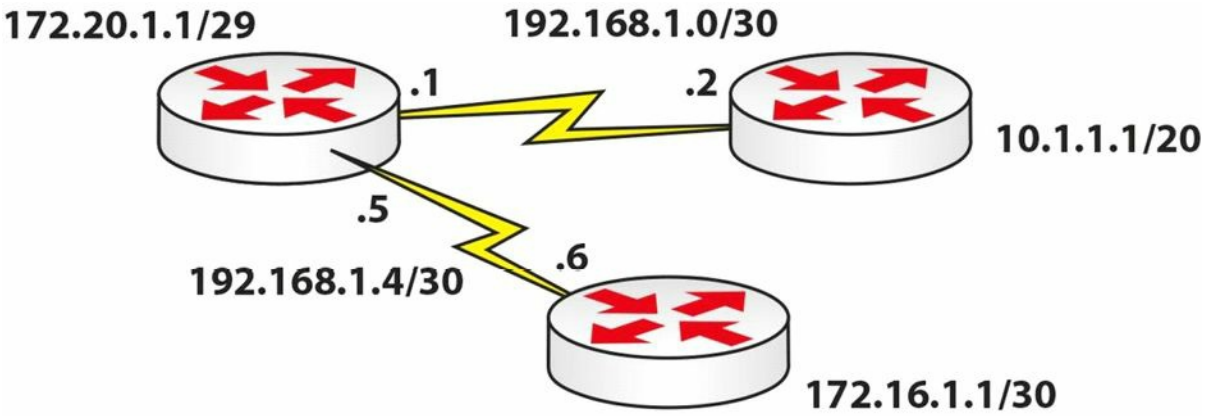
172.16.x.x to 172.31.x.x – any address starting with 172.16 to 172.31, inclusive

192.168.x.x – any address starting with 192.168

6. 255.255.240.0.
7. 255.248.0.0.
8. 62.
9. 172.16.127.254.
10. 192.168.1.0/26, 192.168.1.0.64/26, 192.168.1.0.128/26, and 192.168.1.0.192/26.

Day 23 Lab – Multi-technology

Topology



Instructions

Connect three routers together with Serial or Ethernet connections. We are using RIP for convenience, although it isn't tested in the exam:

1. Configure the connections between the routers and ping
2. Add Loopback addresses to the three routers, as per the diagram
3. Put 172.16.1.0/30 and 10.1.1.0/20 and both 192 networks into RIPv2
4. Add a static route on the two spoke routers for network 192.168.20.0/24 to go to the hub
5. Configure a NAT pool on the hub router for network 172.20.1.0/29 to perform NAT to pool 192.168.20.0/24
6. Check to ensure that all RIP routes are in the routing table with their correct networks
7. Source a ping from 172.20.1.1 to the Loopback addresses on the spoke routers; turn on a NAT debug first and check the NAT table afterwards

Solution Hints and Commands

- `router rip`
  `no auto`
  `ver 2`

  `network x.x.x.x`
- Static route: `ip route` command

https://t.me/learningnets

- `ip nat pool <name> <start_ip> <end_ip> netmask <mask>` command
- `ip nat inside source list x pool <name>` command
- `show ip route` command to check the networks in the routing table
- `debug ip nat [detailed]` command

https://t.me/learningnets

Day 24 – Review 9

Day 24 Tasks

- Take the exam below
- Review any theory (if required) or NAT
- Complete the ACL module labs
- Complete any earlier lab (without looking at the solution)
- Read the ICND1 cram guide
- Spend 15 minutes on the subnetting.org website

Day 24 Exam

1. You can have a named, extended, and standard ACL on one incoming interface. True or false?
2. You want to test why your ping is blocked on your Serial interface. You ping out from the router but it is permitted. What went wrong? (Hint: See ACL Rule 4.)
3. Write a wildcard mask to match subnet mask 255.255.224.0.
4. What do you type to apply an IP access control list to the Telnet lines on a router?
5. How can you verify per interface ACL statistics (name the command)?
6. How do you apply an ACL to an interface?
7. Write the configuration command for NAT 192.168.1.1 to 200.1.1.1.
8. Which command do you add to a NAT pool to enable PAT?
9. NAT most often fails to work because the _____ _____ _____ command is missing.
10. Which `debug` command shows live NAT translations occurring?

Day 24 Answers

1. False. You can only configure a single ACL on an interface per direction.
2. A router won't filter traffic it generated itself.
3. 0.0.31.255.
4. The `access-class` command.
5. With the `show ip access-list interface` command.
6. With the `ip access-group <ACL_name> [in|out]` command.
7. `ip nat inside source static 192.168.1.1 200.1.1.1`.
8. The `overload` command.
9. `ip nat inside` or `ip nat outside`.

https://t.me/learningnets

10. The d`ebug ip nat [detailed]`command.

https://t.me/learningnets

Day 25 – Review 10

Is there anything else you need to cover from the ICND1 syllabus? You should have nailed all of your weak areas by now.

You should be able to do the following:

- Recite the entire cram guide
- Configure static routes, NAT, and IP addressing
- Configure basic switch security and VLANs
- Configure DHCP
- Answer VLSM and subnetting questions very quickly
- Understand TCP, OSI, cables, and specifications
- Understand the routing process including OSPF, OSPFv3
- IPv6 addressing and IPv4.

Day 25 Tasks

- Take the exam below
- Review any theory (if required)
- Complete any lab you wish
- Write the ICND1 cram guide from memory
- Spend 15 minutes on the subnetting.org website

Day 25 Exam

1. Write out the two ways of configuring console passwords. Write the actual commands.
2. Which command will permit only SSH traffic into the VTY lines?
3. Which command will encrypt a password with level 7 encryption?
4. Name the eight levels of logging available on the router.
5. Why would you choose SSH access over Telnet?
6. Your three options upon violation of your port security are protect, _____, and _____.
7. How would you hard set a port to accept only MAC 0001.c74a.0a01?
8. Which command turns off CDP for a particular interface?
9. Which command turns off CDP for the entire router or switch?
10. Which command adds a password to your VTP domain?
11. Which command would permit only VLANs 10 to 20 over your interface?

https://t.me/learningnets

Day 25 Answers

1. `password xxx` and `login local` (username and password previously configured).
2. The `transport input ssh` command.
3. The `service password-encryption` command.
4. Alerts, critical, debugging, emergencies, errors, informational, notifications, and warnings.
5. It offers secure, encrypted traffic.
6. Shutdown, restrict.
7. With the `switchport port-security mac-address 0001.c74a.0a01` command.
8. The `no cdp enable` command.
9. The `no cdp run` command.
10. The `vtp password xxx` command.
11. The `switchport trunk allowed vlan 10-20` command.

https://t.me/learningnets

Day 26 – Review 11

Day 26 Tasks

- Take the exam below
- Review any theory (if required), especially the IPv6-related sections
- Complete any lab you wish
- Write the ICND1 cram guide from memory
- Spend 15 minutes on the subnetting.org website

Day 26 Exam

1. IPv6 addresses must always be used with a subnet mask. True or false?
2. Name the three types of IPv6 addresses.
3. Which command enables IPv6 on your router?
4. The 0002 portion of an IPv6 address can be shortened to just 2. True or false?
5. How large is the IPv6 address space?
6. With IPv6, every host in the world can have a unique address. True or false?
7. IPv6 does not have natively integrated security features. True or false?
8. IPv6 implementations allow hosts to have multiple addresses assigned. True or false?
9. How can the broadcast functionality be simulated in an IPv6 environment?
10. How many times can the double colon (::) notation appear in an IPv6 address?

Day 26 Answers

1. False.
2. Unicast, Multicast, and Anycast.
3. The `ipv6 unicast-routing` command.
4. True.
5. 128 bits.
6. True.
7. False.
8. True.
9. By using Anycast.
10. Only one time.

https://t.me/learningnets

Day 27 – Review 12

Day 27 Tasks

- Take the exam below
- Review any theory (if required)
- Complete any lab you wish
- Write the ICND1 cram guide from memory
- Spend 15 minutes on the subnetting.org website

Day 27 Exam

Can you do the following?

- Secure a switch with Telnet passwords/SSH and switch ports
- Put switch ports into VLANs
- Troubleshoot simple switch and VLAN issues
- Configure static routes
- Configure static NAT, dynamic NAT, and PAT
- Carve a network down using VLSM
- Find the correct subnet for a host
- Configure a DHCP pool
- Configure IPv6 basic addressing

https://t.me/learningnets

Day 28 – Review 13

Day 28 Tasks

- Take the exam below
- Review any theory (if required)
- Complete any lab you wish
- Spend 30 minutes on the subnetting.org website

Day 28 Exam

1. What are the three methods used to control data flow at Layer 4?
2. Switches contain a memory chip known as an _____, which builds a table listing of which device is plugged into which port.
3. Name the two trunk link encapsulation types.
4. Which command will encrypt a password with level 7 encryption?
5. Convert 192.160.210.177 into binary (without using a calculator).
6. NAT converts the _____ headers for incoming and outgoing traffic and keeps track of each session.
7. Name the three types of IPv6 addresses.
8. Name three IPv4-to-IPv6 transaction mechanism classes.
9. What do you type to apply an IP access control list to the Telnet lines on a router?
10. _____ is used to determine the reliability of one source of routing information from another.

Day 28 Answers

1. Flow control, windowing, and acknowledgements.
2. ASIC.
3. 802.1Q and ISL.
4. The `service password-encryption` command.
5. 11000000.10100000.11010010.10110001.
6. Packet.
7. Unicast, Multicast, and Anycast.
8. Dual-stack, tunnelling, and protocol translation.
9. The `access-class` command.
10. Administrative distance.

https://t.me/learningnets

Day 29 – Review 14

Day 29 Tasks

- Take the exam below
- Review any theory (if required), especially the IPv6-related sections
- Complete any lab you wish
- Write the ICND1 cram guide from memory
- Spend 15 minutes on the subnetting.org website

Day 29 Exam

1. By default, the _____ _____ command shows the last 10 commands entered on the CLI.
2. The `show` _____-_____-_____ command displays a list of which MAC addresses are connected to which ports.
3. VTP Client mode allows you to configure VLANs. True or false?
4. Which command turns off CDP for the entire router or switch?
5. What is the private range of IP addresses?
6. Which `show` command displays a list of your NAT table?
7. How large is the IPv6 address space?
8. While IPv4 routing is enabled by default in Cisco IOS software, IPv6 routing is disabled by default and must be explicitly enabled. True or false?
9. FTP uses which port number(s)?
10. Name at least four routing metrics.

I know I'm repeating some questions but there is a good reason for that.

Day 29 Answers

1. `show history`.
2. `mac-address-table`.
3. False.
4. The `no cdp run` command.
5. 10.x.x.x – any address starting with a 10

   172.16.x.x to 172.31.x.x – any address starting with 172.16 to 172.31, inclusive

   192.168.x.x – any address starting with 192.168.
6. The `show ip nat translations` command.

https://t.me/learningnets

7. 128 bits.
8. True.
9. Port 20 and port 21.
10. Bandwidth, cost, delay, load, reliability, and hop count.

https://t.me/learningnets

Day 30 – Exam Day

Today you should be taking the ICND1 exam. If you are doing the full CCNA route, then take a day off. You have earned it. We have a lot of hard work to come.

https://t.me/learningnets

Day 31 – Spanning Tree Protocol

Day 31 Tasks

- Read today's lesson notes (below)
- Complete today's lab
- Read the ICND2 cram guide
- Spend 15 minutes on the subnetting.org website

The role of Spanning Tree Protocol (STP) is to prevent loops from occurring on your network by creating a loop-free logical topology, while allowing physical links in redundant switched network topologies. With the huge growth in the use of switches on networks, and the main goal of propagating VLAN information, the problem of frames looping endlessly around the network began to occur.

The previous CCNA exam required only a basic understanding of STP. The current version, however, expects you to have a very good grasp of the subject.

Today you will learn about the following:

- The need for STP
- STP Bridge ID
- STP Root Bridge election
- STP cost and priority
- STP Root and Designated Ports
- STP enhancements
- Troubleshooting STP

This lesson maps to the following CCNA syllabus requirement:

- Configure and verify PVSTP operation
  - Describe root bridge election
  - Spanning tree mode

The Need for STP

STP is defined in the IEEE 802.1D standard. In order to maintain a loop-free logical topology, every two seconds, switches pass Bridge Protocol Data Units (BPDUs). BPDUs are data messages used within a spanning tree topology to pass information about ports, addresses, priorities, and costs. The BPDUs are tagged with the VLAN ID.

Figure 31.1 below shows how loops can be created in a network. Because each switch learns about VLAN 20, it also advertises to other switches that it can reach VLAN 20. Soon enough, each switch thinks it is the source for VLAN 20 traffic and a loop is caused, so any frame

https://t.me/learningnets

destined for VLAN 20 is passed from switch to switch.

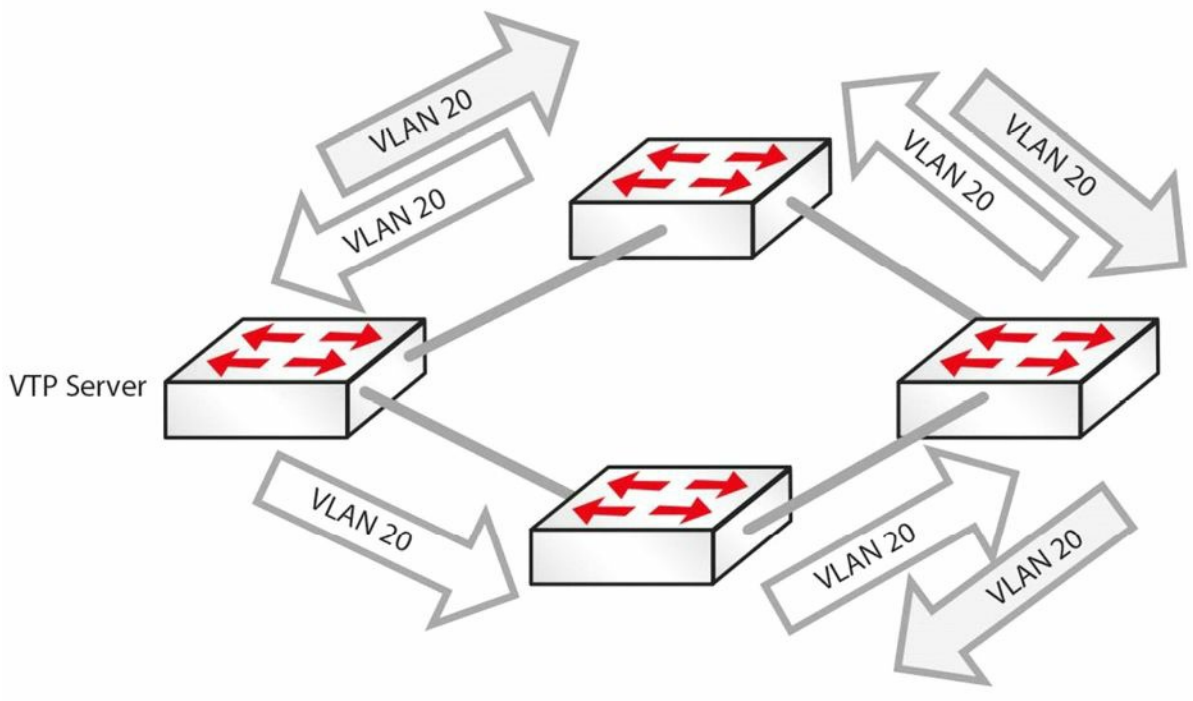


Figure 31.1 – How Loops Are Created

STP runs an algorithm to decide which switch ports stay open, or active, as far as a particular VLAN is concerned, and which ones need to be shut for that particular VLAN.

All switches that reside in the Spanning Tree domain communicate and exchange messages using BPDUs. STP uses the exchange of BPDUs to determine the network topology, which is determined by the following three variables:

- The unique MAC address (switch identifier) that is associated with each switch
- The path cost to the Root Bridge associated with each switch port
- The port identifier (MAC address of the port) associated with each switch port

BPDUs are sent every two seconds, which allows for rapid network loop detection and topology information exchanges. The two types of BPDUs are Configuration BPDUs and Topology Change Notification BPDUs; only Configuration BPDUs will be covered here.

IEEE 802.1D Configuration BPDUs

Configuration BPDUs are sent by LAN switches and are used to communicate and compute the Spanning Tree topology. After the switch port initialises, the port is placed into the Blocking state and a BPDU is sent to each port in the switch. By default, all switches initially assume that they are the Root of the Spanning Tree, until they exchange Configuration BPDUs with other switches. As long as a port continues to see its Configuration BPDU as the most attractive, it will continue sending Configuration BPDUs. Switches determine the best Configuration BPDU based on the following four factors (in the order listed):

1. Lowest Root Bridge ID
2. Lowest Root path cost to Root Bridge

https://t.me/learningnets

3. Lowest sender Bridge ID
4. Lowest sender Port ID

The completion of the Configuration BPDU exchange results in the following actions:

- A Root Switch is elected for the entire Spanning Tree domain
- A Root Port is elected on every Non-Root Switch in the Spanning Tree domain
- A Designated Switch is elected for every LAN segment
- A Designated Port is elected on the Designated Switch for every segment (all active ports on the Root Switch are also designated)
- Loops in the network are eliminated by blocking redundant paths

NOTE: These characteristics will be described in detail as you progress through this module.

Once the Spanning Tree network has converged, which happens when all switch ports are in a Forwarding or Blocking state, Configuration BPDUs are sent by the Root Bridge every Hello time interval, which defaults to two seconds. This is referred to as the origination of Configuration BPDUs. The Configuration BPDUs are forwarded to downstream neighbouring switches via the Designated Port on the Root Bridge.

When a Non-Root Bridge receives a Configuration BPDU on its Root Port, which is the port that provides the best path to the Root Bridge, it sends an updated version of the BPDU via its Designated Port(s). This is referred to as the propagation of BPDUs.

The Designated Port is a port on the Designated Switch that has the lowest path cost when forwarding packets from that LAN segment to the Root Bridge.

Once the Spanning Tree network has converged, a Configuration BPDU is always transmitted away from the Root Bridge to the rest of the switches within the STP domain. The simplest way to remember the flow of Configuration BPDUs after the Spanning Tree network has converged is to memorise the following four rules:

1. A Configuration BPDU originates on the Root Bridge and is sent via the Designated Port.
2. A Configuration BPDU is received by a Non-Root Bridge on a Root Port.
3. A Configuration BPDU is transmitted by a Non-Root Bridge on a Designated Port.
4. There is only one Designated Port (on a Designated Switch) on any single LAN segment.

Figure 31.2 below illustrates the flow of the Configuration BPDU in the STP domain, demonstrating the four simple rules listed above:

https://t.me/learningnets

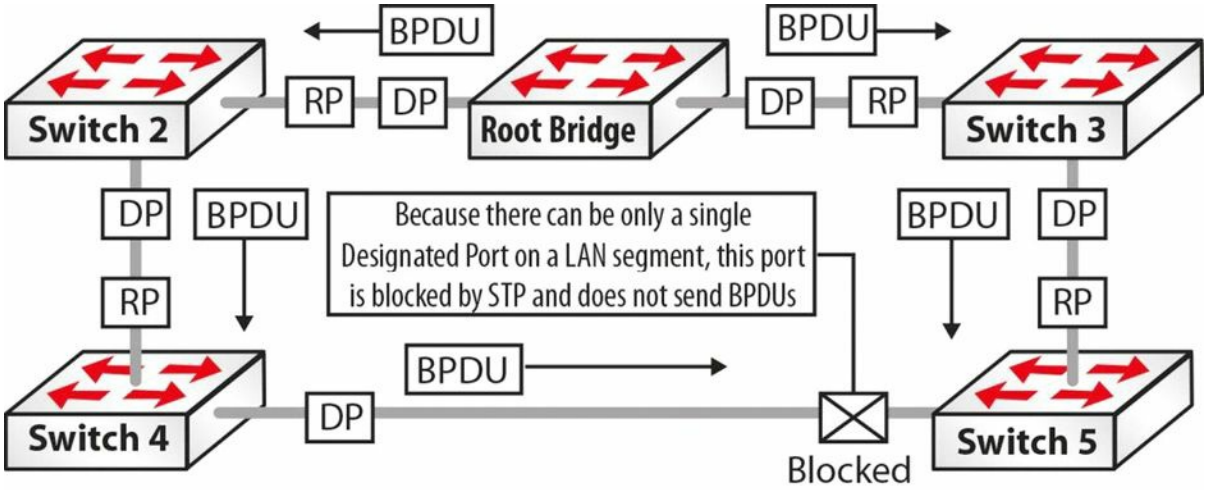


Figure 31.2 – A Configuration BPDU Flows throughout the STP Domain

1. Referencing Figure 31.2, the Configuration BPDU is originated by the Root Bridge and sent out via the Designated Ports on the Root Bridge towards the Non-Root Bridge switches, Switch 2 and Switch 3.
2. Non-Root Bridge Switch 2 and Switch 3 receive the Configuration BPDU on their Root Ports, which provide the best path to the Root Bridge.
3. Switch 2 and Switch 3 modify (update) the received Configuration BPDU and forward it out of their Designated Ports. Switch 2 is the Designated Switch on the LAN segment for itself and Switch 4, while Switch 3 is the Designated Switch on the LAN segment for itself and Switch 5. The Designated Port resides on the Designated Switch and is the port that has the lowest path cost when forwarding packets from that LAN segment to the Root Bridge.
4. On the LAN Segment between Switch 4 and Switch 5, Switch 4 is elected Designated Switch and the Designated Port resides on that switch. Because there can be only a single Designated Switch on a segment, the port on Switch 5 for that LAN segment is blocked. This port will not forward any BPDUs.

Spanning Tree Port States

The Spanning Tree Algorithm (STA) defines a number of states that a port under STP control will progress through before being in an active Forwarding state. 802.1D port states are as follows:

- Blocking – BPDUs received only (20 seconds)
- Listening – BPDUs sent and received (15 seconds)
- Learning – Bridging table is built (15 seconds)
- Forwarding – Sending/receiving data
- Disabled – Administratively down

A port moves through these states in the following manner:

1. From initialisation to Blocking

https://t.me/learningnets

2. From Blocking to either Listening or Disabled
3. From Listening to either Learning or Disabled
4. From Learning to either Forwarding or Disabled
5. From Forwarding to Disabled

STP timers are used in the process to control convergence:

- Hello – 2 seconds (time between each Configuration BPDU)
- Forward Delay – 15 seconds (controls durations of Listening/Learning states)
- Max Age – 20 seconds (controls the duration of the Blocking state)

Default convergence time is 30 to 50 seconds.

Spanning Tree Blocking State

A switch port that is in the Blocking state performs the following actions:

- Discards frames received on the port from the attached segment
- Discards frames switched from another port
- Does not incorporate station location into its address database
- Receives BPDUs and directs them to the system module
- Does not transmit BPDUs received from the system module
- Receives and responds to network management messages

Spanning Tree Listening State

The Listening state is the first transitional state that the port enters following the Blocking state. The port enters this state when STP determines that the port should participate in frame forwarding. A switch port that is in the Listening state performs the following actions:

- Discards frames received on the port from the attached segment
- Discards frames switched from another port
- Does not incorporate station location into its address database
- Receives BPDUs and directs them to the system module
- Receives, processes, and transmits BPDUs received from the system module
- Receives and responds to network management messages

Spanning Tree Learning State

The Learning state is the second transitional state the port enters. This state comes after the Listening state and before the port enters the Forwarding state. In this state, the port learns and installs MAC addresses into its forwarding table. A switch port that is in the Learning state performs the following actions:

https://t.me/learningnets

- ☐ Discards frames received from the attached segment
- ☐ Discards frames switched from another port
- ☐ Incorporates (installs) station location into its address database
- ☐ Receives BPDUs and directs them to the system module
- ☐ Receives, processes, and transmits BPDUs received from the system module
- ☐ Receives and responds to network management messages

Spanning Tree Forwarding State

The Forwarding state is the final transitional state the port enters after the Learning state. A port in the Forwarding state forwards frames. A switch port that is in the Forwarding state performs the following actions:

- ☐ Forwards frames received from the attached segment
- ☐ Forwards frames switched from another port
- ☐ Incorporates (installs) station location information into its address database
- ☐ Receives BPDUs and directs them to the system module
- ☐ Processes BPDUs received from the system module
- ☐ Receives and responds to network management messages

Spanning Tree Disabled State

The Disabled state is not part of the normal STP progression for a port. Instead, a port that is administratively shut down by the network administrator, or by the system because of a fault condition, is considered to be in the Disabled state. A disabled port performs the following actions:

- ☐ Discards frames received from the attached segment
- ☐ Discards frames switched from another port
- ☐ Does not incorporate station location into its address database
- ☐ Receives BPDUs but does not direct them to the system module
- ☐ Does not receive BPDUs from the system module
- ☐ Receives and responds to network management messages

Spanning Tree Bridge ID

Switches in a Spanning Tree domain have a Bridge ID (BID), which is used to identify uniquely the switch within the STP domain. The BID is also used to assist in the election of an STP Root Bridge, which will be described later. The BID is an 8-byte field that is composed from a 6-byte MAC address and a 2-byte Bridge Priority. The BID is illustrated in Figure 31.3 below:

https://t.me/learningnets

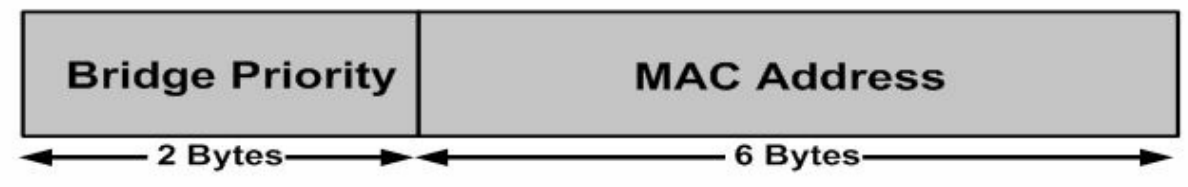


Figure 31.3 – Bridge ID Format

The Bridge Priority is the priority of the switch in relation to all other switches. The Bridge Priority values range from 0 to 65535. The default value for Cisco Catalyst switches is 32768.

```
Switch2#show spanning-tree vlan 2

VLAN0002
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0009.7c87.9081
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID  Priority    32770 (priority 32768 sys-id-ext 2)
             Address     0008.21a9.4f80
             Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time  300

Interface   Port ID              Designated                  Port ID
Name        Prio.Nbr  Cost  Sts Cost         Bridge ID      Prio.Nbr
----------  --------  ----  --- ------------ -------------- --------
Fa0/1       128.1     19    FWD 0 32768      0009.7c87.9081 128.13
Fa0/2       128.2     19    FWD 19 32770     0008.21a9.4f80 128.2
```

The MAC address in the output above is the hardware address derived from the switch backplane or supervisor engine. In the 802.1D standard, each VLAN requires a unique BID.

Most Cisco Catalyst switches have a pool of 1024 MAC addresses that can be used as BIDs for VLANs. These MAC addresses are allocated sequentially, with the first MAC address in the range assigned to VLAN 1, the second to VLAN 2, the third to VLAN 3, and so forth. This provides the capability to support the standard range of VLANs, but more MAC addresses would be needed to support the extended range of VLANs. This issue was resolved in the 802.1t (Technical and Editoral corrections for 802.1D) standard.

Spanning Tree Root Bridge Election

By default, following initialisation, all switches initially assume that they are the Root of the Spanning Tree, until they exchange BPDUs with other switches. When switches exchange BPDUs, an election is held and the switch with the lowest Bridge ID in the network is elected the STP Root Bridge. If two or more switches have the same priority, the switch with the lowest order MAC address is chosen. This concept is illustrated in Figure 31.4 below:

https://t.me/learningnets

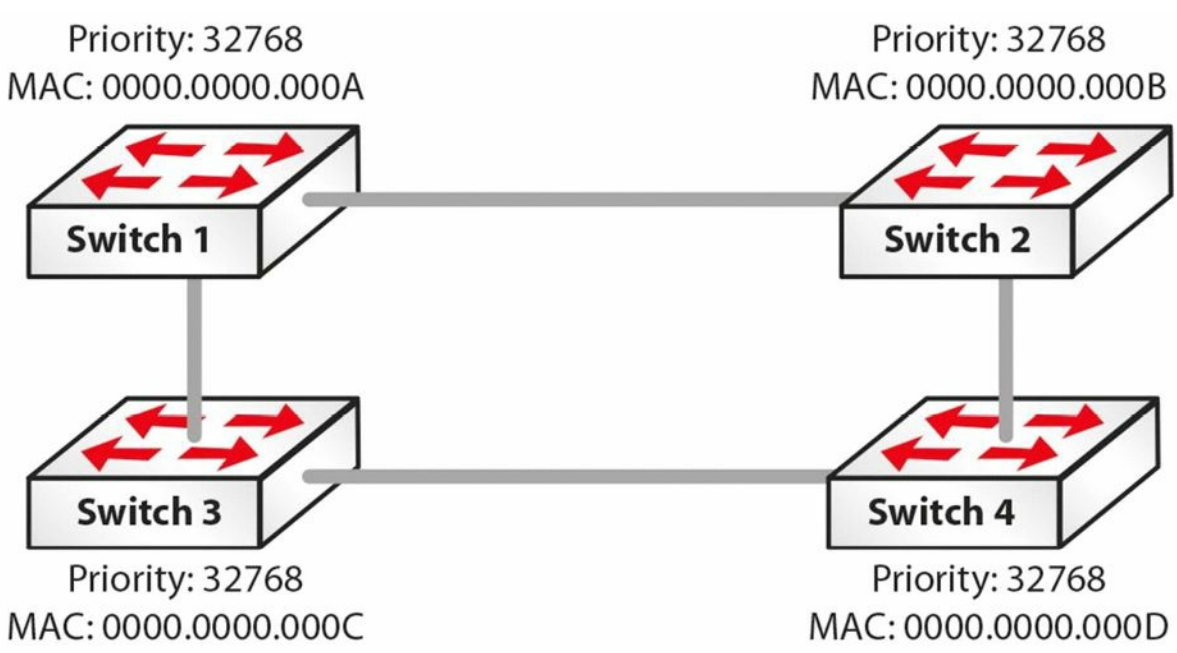


Figure 31.4 – Electing the STP Root Bridge

In Figure 31.4, four switches – Switch 1, Switch 2, Switch 3, and Switch 4 – are all part of the same STP domain. By default, all of the switches have a Bridge Priority of 32768. In order to determine which switch will become the Root Bridge, and thus break the tie, STP will select the switch based on the lowest-order MAC address. Based on this criterion, and referencing the information shown in Figure 31.4, Switch 1 will be elected the Root Bridge.

Once elected, the Root Bridge becomes the logical centre of the Spanning Tree network. This is not to say that the Root Bridge is physically at the centre of the network. Ensure that you do not make that false assumption.

NOTE: It is important to remember that during STP Root Bridge election, no traffic is forwarded over any switch in the same STP domain.

Cisco IOS software allows administrators to influence the election of the Root Bridge. In addition, administrators can also configure a backup Root Bridge. The backup Root Bridge is a switch that administrators would prefer to become the Root Bridge in the event that the current Root Bridge failed or was removed from the network.

It is always good practice to configure a backup Root Bridge for the Spanning Tree domain. This allows the network to be deterministic in the event that the Root Bridge fails. The most common practice is to configure the highest priority (i.e., the lowest numerical value) on the Root Bridge and then the second-highest priority on the switch that should assume Root Bridge functionality in the event that the current Root Bridge fails. This is illustrated in Figure 31.5 below:

https://t.me/learningnets

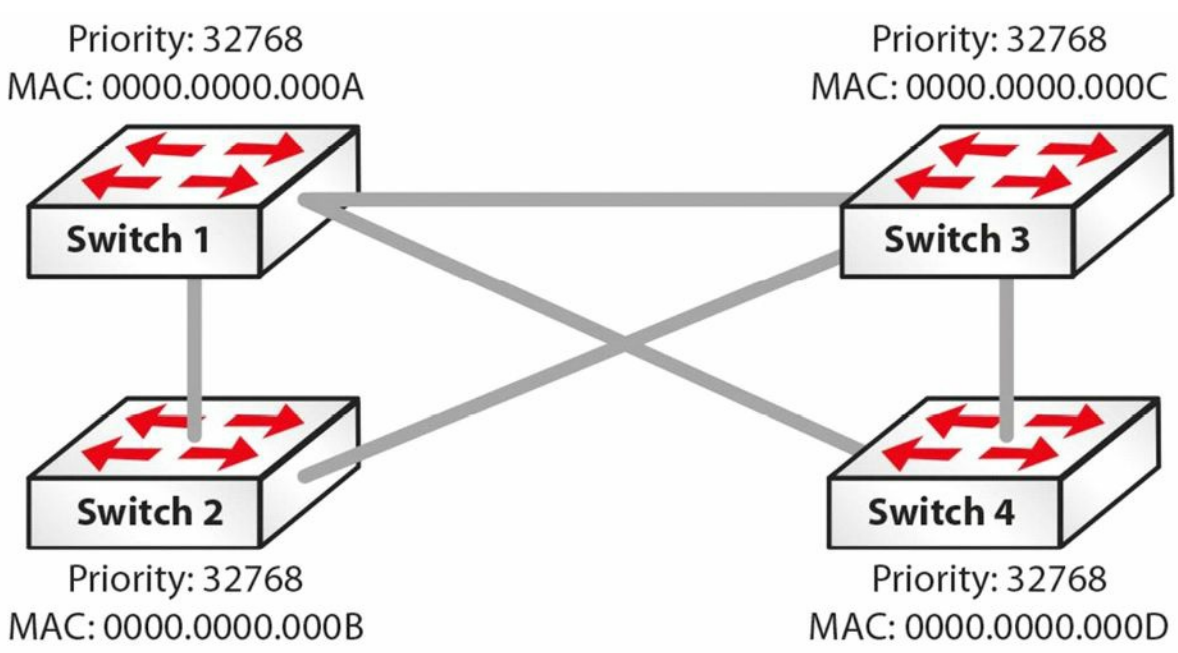


Figure 31.5 – Electing the STP Root Bridge (Continued)

Based on the configuration in Figure 31.5, the most likely switch to be elected as the Root Bridge in this network is Switch 1. This is because, although all priority values are the same, this switch has the lowest-order MAC address. In the event that Switch 1 failed, STP would elect Switch 2 as the Root Bridge, because it has the second-lowest MAC address. However, this would result in a suboptimal network topology.

To address this, administrators can manually configure the priority on Switch 1 to the lowest possible value (0) and that of Switch 2 to the second-lowest possible value (4096). This will ensure that in the event that the Root Bridge (Switch 1) fails, Switch 2 will be elected the Root Bridge. Because administrators are aware of the topology and know which switch would assume Root Bridge functionality, they created a deterministic network that is easier to troubleshoot. The Root ID is carried in BPDUs and includes the Bridge Priority and MAC address of the Root Bridge.

EXAM TIP: If you want to force a switch to become the Root Bridge, you can perform the following (see also Figure 31.6 below):

- You can manually set the priority

```
Switch(config)#spanning-tree vlan 2 priority ?
  <0-61440>  bridge priority in increments of 4096
```

- Or set it as the Root Bridge using macro the commands `primary` or `secondary`

```
Switch(config)#spanning-tree vlan 2 root ?
  primary    Configure this switch as primary root for this spanning tree
  secondary  Configure switch as secondary root
```

https://t.me/learningnets

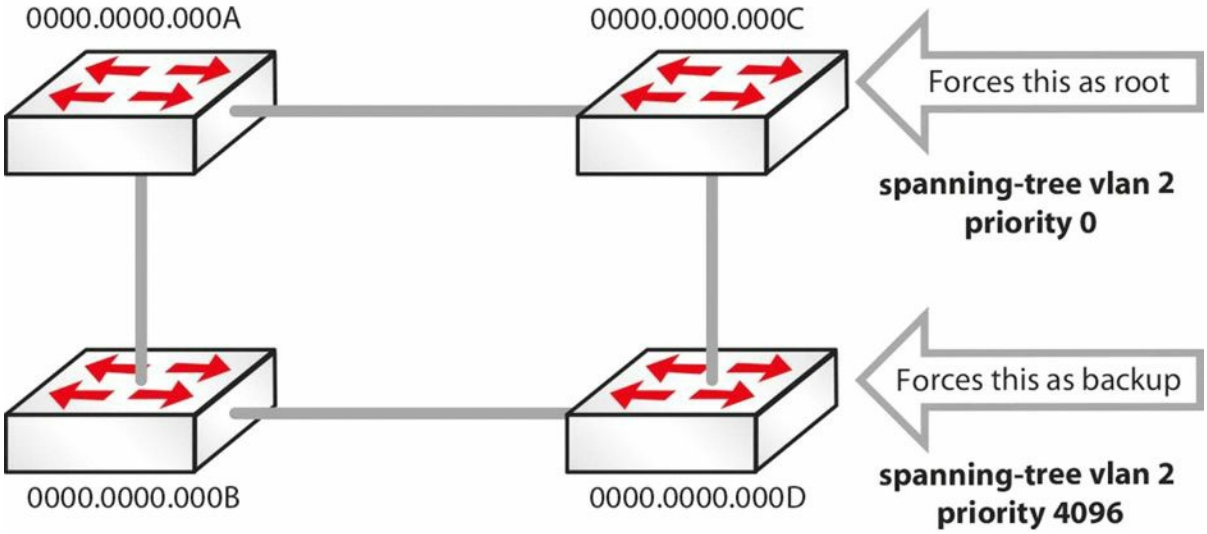


Figure 31.6 – Forcing a Switch to Become the Root Bridge

```
SwitchC#show spanning-tree vlan 5
VLAN0005
Spanning tree enabled protocol ieee
Root ID    Priority  0
Address  0000.0000.000c
This bridge is the root
Bridge ID   Priority  0 (priority 0 sys-id-ext 5)
SwitchD#show spanning-tree vlan 5
VLAN0005
Spanning tree enabled protocol ieee
Root ID    Priority  4096
Address  0000.0000.000d
Bridge ID   Priority  4096 (priority 8192 sys-id-ext 5)
SwitchD#show spanning-tree vlan 5
VLAN0005
Spanning tree enabled protocol ieee
Root ID    Priority  4096
Address  0000.0000.000d
Bridge ID   Priority  4096 (priority 8192 sys-id-ext 5)
```

Note that the VLAN number is often added to the priority number, as shown in the output below:

```
SwitchA#show spanning-tree vlan 5
Bridge ID   Priority 32773 (priority 32768 sys-id-ext 5)
Address 0013.c3e8.2500
Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface  Role  Sts   Cost   Prio.Nbr  Type
__https://t.me/learningnets__  --------  ----
```

```
Fa0/15   Desg   FWD  19   128.15   P2p
Fa0/18   Desg   FWD   19   128.18  P2
```

Spanning Tree Cost and Priority

STP uses cost and priority values to determine the best path to the Root Bridge. These values are then used in the election of the Root Port, which will be described in the following section. It is important to understand the calculation of the cost and priority values in order to understand how Spanning Tree selects one port over another, for example.

One of the key functions of the STA is to attempt to provide the shortest path to each switch in the network from the Root Bridge. Once selected, this path is then used to forward data, whilst redundant links are placed into a Blocking state. STA uses two values to determine which port will be placed into a Forwarding state (i.e., is the best path to the Root Bridge) and which port(s) will be placed into a Blocking state. These values are the port cost and the port priority. Both are described in the sections that follow.

Spanning Tree Port Cost

The 802.1D specification assigns 16-bit (short) default port cost values to each port that is based on the port's bandwidth. Because administrators also have the capability to assign port cost values manually (between 1 and 65535), the 16-bit values are used only for ports that have not been specifically configured for port cost. Table 31.1 below lists the default values for each type of port when using the short method to calculate the port cost:

Table 31.1 – Default STP Port Cost Values

Bandwidth	Default Port Cost
4Mbps	250
10Mbps	100
16Mbps	62
100Mbps	19
1Gbps	4
10Gbps	2

In Cisco IOS Catalyst switches, default port cost values can be verified by issuing the `show spanning-tree interface [name]` command, as illustrated in the following output, which shows the default short port cost for a FastEthernet interface:

```
VTP-Server#show spanning-tree interface FastEthernet0/2

Vlan             Role   Sts   Cost    Prio.Nbr Type
--------         ----   ---   ----    ------------
VLAN0050         Desg   FWD   19      128.2    P2p
```

The following output shows the same for long port cost assignment:

```
VTP-Server#show spanning-tree interface FastEthernet0/2
```

https://t.me/learningnets

```
Vlan             Role Sts Cost    Prio.Nbr Type
--------         ---- --- ------    -------- ----
VLAN0050         Desg FWD 200000   128.2    P2p
```

It is important to remember that ports with lower (numerical) costs are more preferred; the lower the port cost, the higher the probability of that particular port being elected the Root Port. The port cost value is globally significant and affects the entire Spanning Tree network. This value is configured on all Non-Root Switches in the Spanning Tree domain.

Spanning Tree Root and Designated Ports

STP elects two types of ports that are used to forward BPDUs: the Root Port, which points towards the Root Bridge, and the Designated Port, which points away from the Root Bridge. It is important to understand the functionality of these two port types and how they are elected by STP.

Spanning Tree Root Port Election

STA defines three types of ports: the Root Port, the Designated Port, and the Non-Designated Port. These port types are elected by the STA and placed into the appropriate state (e.g., Forwarding or Blocking). During the Spanning Tree election process, in the event of a tie, the following values will be used (in the order listed) as tiebreakers:

1. Lowest Root Bridge ID
2. Lowest Root path cost to Root Bridge
3. Lowest sender Bridge ID
4. Lowest sender Port ID

NOTE: It is important to remember these tiebreaking criteria in order to understand how Spanning Tree elects and designates different port types in any given situation. Not only is this something that you will most likely be tested on, but also it is very important to have a solid understanding of this in order to design, implement, and support internetworks in the real world.

The Spanning Tree Root Port is the port that provides the best path, or lowest cost, when the device forwards packets to the Root Bridge. In other words, the Root Port is the port that receives the best BPDU for the switch, which indicates that it is the shortest path to the Root Bridge in terms of path cost. The Root Port is elected based on the Root Bridge path cost.

The Root Bridge path cost is calculated based on the cumulative cost (path cost) of all the links leading up to the Root Bridge. The path cost is the value that each port contributes to the Root Bridge path cost. Because this concept is often quite confusing, it is illustrated in Figure 31.7 below:

NOTE: All but one of the links illustrated in Figure 31.7 are GigabitEthernet links. It should be assumed that the traditional 802.1D method is used for port cost calculation. Therefore, the default port cost of GigabitEthernet is 4, whilst that of FastEthernet is 19.

https://t.me/learningnets

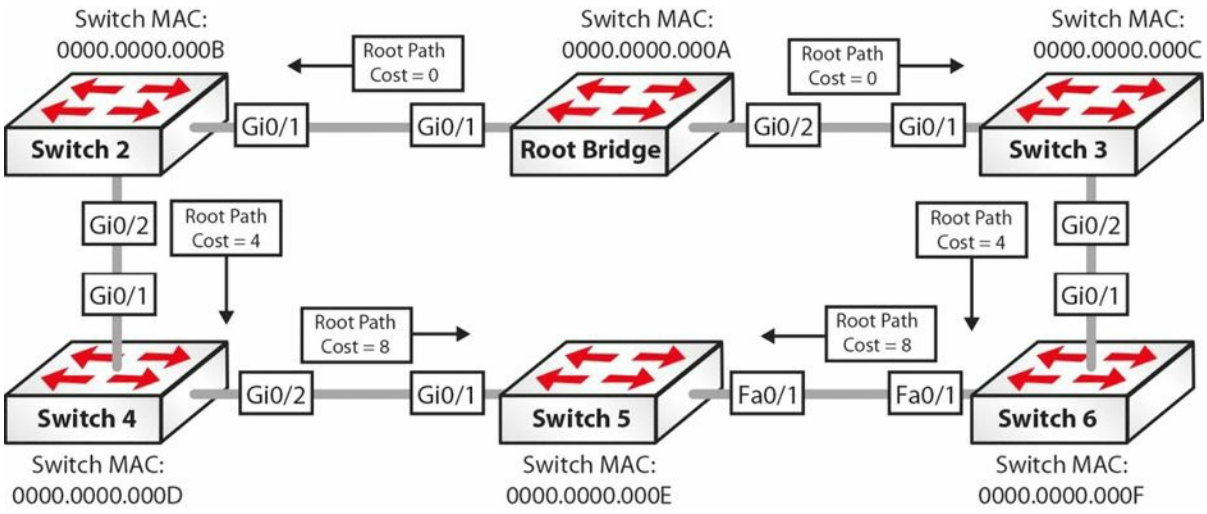


Figure 31.7 – Spanning Tree Root Port Election

NOTE: The following explanation illustrates the flow of BPDUs between the switches in the network. Along with other information, these BPDUs contain the Root Bridge path cost information, which is incremented by the ingress port on the receiving switch.

1. The Root Bridge sends out a BPDU with a Root Bridge path cost value of 0 because its ports reside directly on the Root Bridge. This BPDU is sent to Switch 2 and Switch 3.
2. When Switch 2 and Switch 3 receive the BPDU from the Root Bridge, they add their own path cost based on the ingress interface. Because Switch 2 and Switch 3 are both connected to the Root Bridge via GigabitEthernet connections, they add the path cost value received from the Root Bridge (0) to their GigabitEthernet path cost values (4). The Root Bridge path cost from Switch 2 and Switch 3 via GigabitEthernet0/1 to the Root Bridge is 0 + 4 = 4.
3. Switch 2 and Switch 3 send out new BPDUs to their respective neighbours, which are Switch 4 and Switch 6, respectively. These BPDUs contain the new cumulative value (4) as the Root Bridge path cost.
4. When Switch 4 and Switch 6 receive the BPDUs from Switch 2 and Switch 3, they increment the received Root Bridge path cost value based on the ingress interface. Since GigabitEthernet connections are being used, the value received from Switch 2 and Switch 3 is incremented by 4. The Root Bridge path cost to the Root Bridge on Switch 4 and Switch 6 via their respective GigabitEthernet0/1 interfaces is therefore 0 + 4 + 4 = 8.
5. Switch 5 receives two BPDUs: one from Switch 4 and the other from Switch 6. The BPDU received from Switch 4 has a Root Bridge path cost of 0 + 4 + 4 + 4 = 12. The BPDU received from Switch 6 has a Root Bridge path cost of 0 + 4 + 4 + 19 = 27. Because the Root Bridge path cost value contained in the BPDU received from Switch 4 is better than that received from Switch 6, Switch 5 elects GigabitEthernet0/1 as the Root Port.

NOTE: Switches 2, 3, 4, and 6 will all elect their GigabitEthernet0/1 ports as Root Ports.



https://t.me/learningnets

Further Explanation

To explain further and to help you understand the election of the Root Port, let's assume that all ports in the diagram in Figure 31.7 above are GigabitEthernet ports. This would mean that in Step 5 above, Switch 5 would receive two BPDUs with the same Root Bridge ID, both with a Root path cost value of 0 + 4 + 4 + 4 = 12. In order for the Root Port to be elected, STP will progress to the next option in the tiebreaker criteria listed below (the first two options, which have already been used, have been removed):

1. Lowest sender Bridge ID
2. Lowest sender Port ID

Based on the third selection criteria, Switch 5 will prefer the BPDU received from Switch 4 because its BID (0000.0000.000D) is lower than that of Switch 6 (0000.0000.000F). Switch 5 elects port GigabitEthernet0/1 as the Root Port.

Spanning Tree Designated Port Election

Unlike the Root Port, the Designated Port is a port that points away from the STP Root. This port is the one in which the designated device is attached to the LAN. It is also the port that has the lowest path cost when forwarding packets from that LAN to the Root Bridge.

NOTE: Some people refer to the Designated Port as the Designated Switch. The terms are interchangeable and refer to the same thing; that is, this is the switch, or port, that is used to forward frames from a particular LAN segment to the Root Bridge.

The primary purpose of the Designated Port is to prevent loops. When more than one switch is connected to the same LAN segment, all switches will attempt to forward a frame received on that segment. This default behaviour can result in multiple copies of the same frame being forwarded by multiple switches – resulting in a network loop. To avoid this default behaviour, a Designated Port is elected on all LAN segments. By default, all ports on the Root Bridge are Designated Ports. This is because the Root Bridge path cost will always be 0. The STA election of the Designated Port is illustrated in Figure 31.8 below:

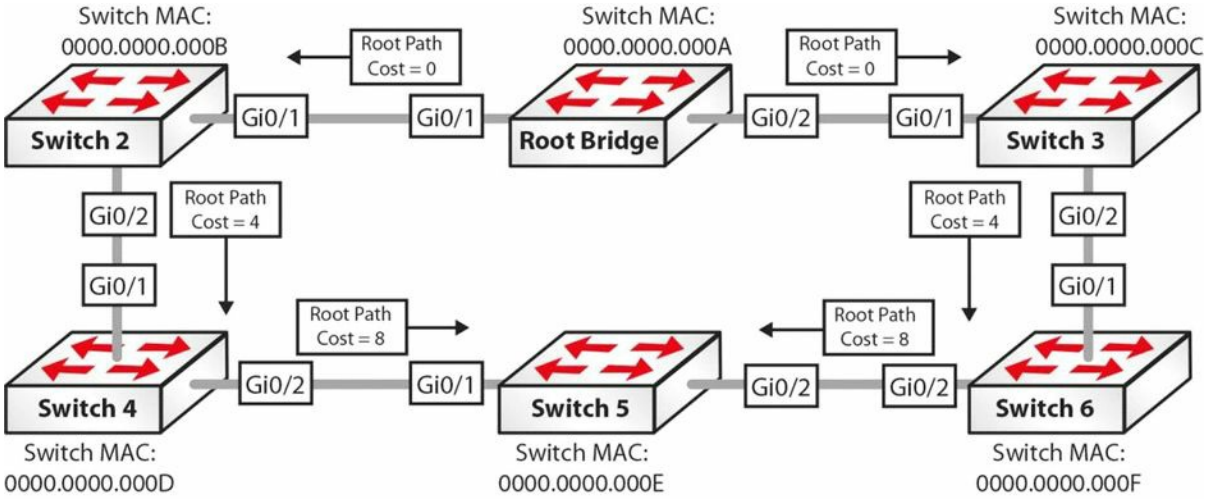


Figure 31.8 – Spanning Tree Designated Port Election

1. On the segment between the Root Bridge and Switch 2, the Root Bridge GigabitEthernet0/1 is elected as the Designated Port because it has the lower Root Bridge

https://t.me/learningnets

path cost, which is 0.

2. On the segment between the Root Bridge and Switch 3, the Root Bridge GigabitEthernet0/2 is elected as the Designated Port because it has the lower Root Bridge path cost, which is 0.
3. On the segment between Switch 2 and Switch 4, the GigabitEthernet0/2 port on Switch 2 is elected as the Designated Port because Switch 2 has the lowest Root Bridge path cost, which is 4.
4. On the segment between Switch 3 and Switch 6, the GigabitEthernet0/2 port on Switch 3 is elected as the Designated Port because Switch 3 has the lowest Root Bridge path cost, which is 4.
5. On the segment between Switch 4 and Switch 5, the GigabitEthernet0/2 port on Switch 4 is elected as the Designated Port because Switch 4 has the lowest Root Bridge path cost, which is 8.
6. On the segment between Switch 5 and Switch 6, the GigabitEthernet0/2 port on Switch 6 is elected as the Designated Port because Switch 6 has the lowest Root Bridge path cost, which is 8.

The Non-Designated Port is not really a Spanning Tree Port type. Instead, it is a term that simply means a port that is not the Designated Port on a LAN segment. This port will always be placed into a Blocking state by STP. Based on the calculation of Root and Designated Ports, the resultant Spanning Tree topology for the switched network that was used in the Root Port and Designated Port election examples is shown in Figure 31.9 below:

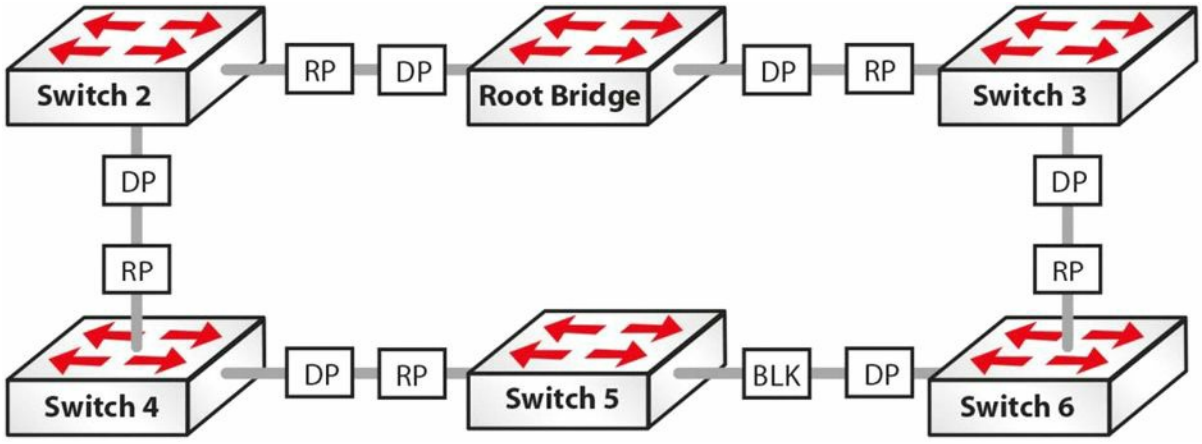


FIG 31.9 – Converged Spanning Tree Network

Cisco Spanning Tree Enhancements

As stated earlier, STP makes two assumptions about the environment in which it has been enabled, as follows:

- All links are bidirectional and can both send and receive Bridge Protocol Data Units
- All switches can regularly receive, process, and send Bridge Protocol Data Units

https://t.me/learningnets

In real-world networks, these two assumptions are not always correct. In situations where that

is the case, STP may not be able to prevent loops from being formed within the network. Because of this possibility, and to improve the performance of the basic IEEE 802.1D STA, Cisco has introduced a number of enhancements to the IEEE 802.1D standard, which are described below.

Port Fast

Port Fast is a feature that is typically enabled only for a port or interface that connects to a host. When the link comes up on this port, the switch skips the first stages of the STA and directly transitions to the Forwarding state. Contrary to popular belief, the Port Fast feature does not disable Spanning Tree on the selected port. This is because even with the Port Fast feature, the port can still send and receive BPDUs.

This is not a problem when the port is connected to a network device that does not send or respond to BPDUs, such as the NIC on a workstation, for example. However, this may result in a switching loop if the port is connected to a device that does send BPDUs, such as another switch. This is because the port skips the Listening and Learning states and proceeds immediately to the Forwarding state. Port Fast simply allows the port to begin forwarding frames much sooner than a port going through all normal STA steps.

BPDU Guard

The BPDU Guard feature is used to protect the Spanning Tree domain from external influence. BPDU Guard is disabled by default but is recommended for all ports on which the Port Fast feature has been enabled. When a port that is configured with the BPDU Guard feature receives a BPDU, it immediately transitions to the errdisable state.

This prevents false information from being injected into the Spanning Tree domain on ports that have Spanning Tree disabled. The operation of BPDU Guard, in conjunction with Port Fast, is illustrated in Figures 31.10, 31.11, and 31.12, below and following:

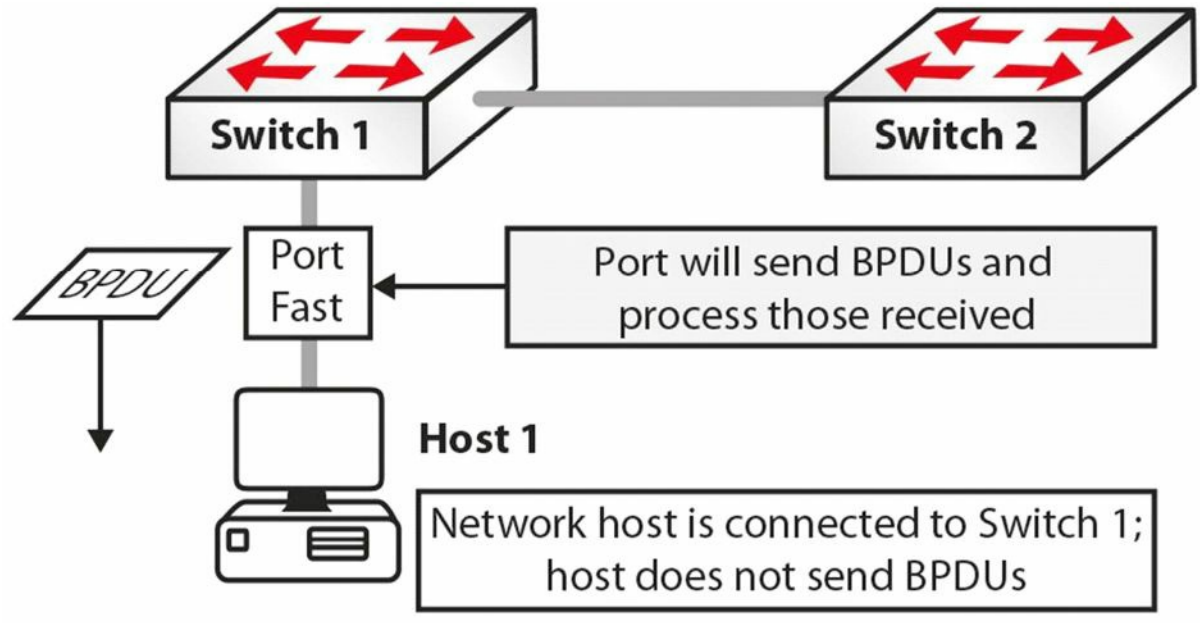


Figure 31.10 – Understanding BPDU Guard

In Figure 31.10, Port Fast is enabled on Switch 1 on its connection to Host 1. Following initialisation, the port transitions to a Forwarding state, which eliminates 30 seconds of delay

https://t.me/learningnets

that would have been encountered if STA was not bypassed and the port went through the Listening and Learning states. Because the network host is a workstation, it sends no BPDUs on that port.

Either by accident or due to some other malicious intent, Host 1 is disconnected from Switch 1. Using the same port, Switch 3 is connected to Switch 1. Switch 3 is also connected to Switch 2. Because Port Fast is enabled on the port connecting Switch 1 to Switch 3, this port moves from initialisation to the Forwarding state, bypassing normal STP initialisation. This port will also receive and process any BPDUs that are sent by Switch 3, as illustrated in Figure 31.11 below:

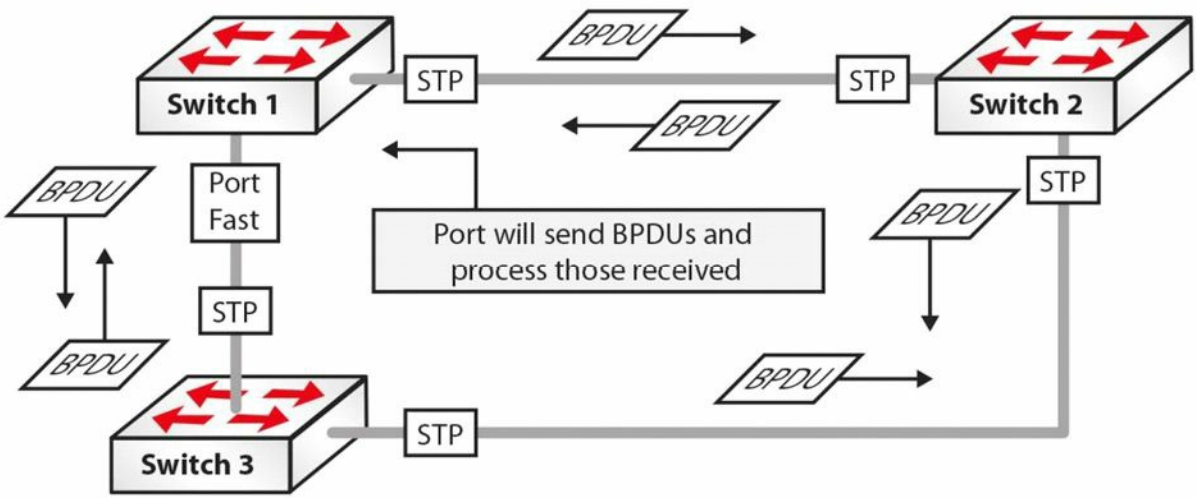


Figure 31.11 – Understanding BPDU Guard (Continued)

Based on the port states illustrated above, you can quickly see how a loop would be created in this network. To prevent this from occurring, BPDU Guard should be enabled on all ports with Port Fast enabled. This is illustrated in Figure 31.12 below:

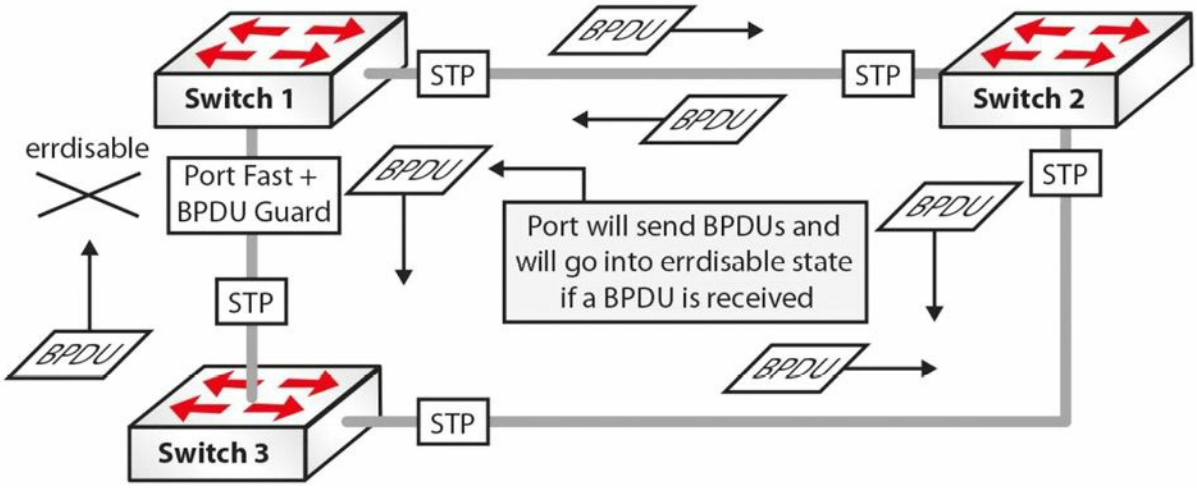


Figure 31.12 – Understanding BPDU Guard (Continued)

With BPDU Guard enabled on the Port Fast port, when Switch 1 receives a BPDU from Switch 3, it immediately transitions the port into the errdisable state. The result is that the STP calculation is not affected by this redundant link and the network will not have any loops.

BPDU Filter

The BPDU Guard and the BPDU Filter features are often confused or even thought to be the same. They are, however, different, and it is important to understand the differences between

https://t.me/learningnets

them. When Port Fast is enabled on a port, the port will send out BPDUs and will accept and process received BPDUs. The BPDU Guard feature prevents the port from receiving any BPDUs but does not prevent it from sending them. If any BPDUs are received, the port will be errdisabled.

The BPDU Filter feature has dual functionality. When configured at interface level it effectively disables STP on the selected ports by preventing them from sending or receiving any BPDUs. When configured globally and used in conjunction with global Port Fast, it will revert out of Port Fast any port that receives BPDUs. This is illustrated in Figure 31.13 below:

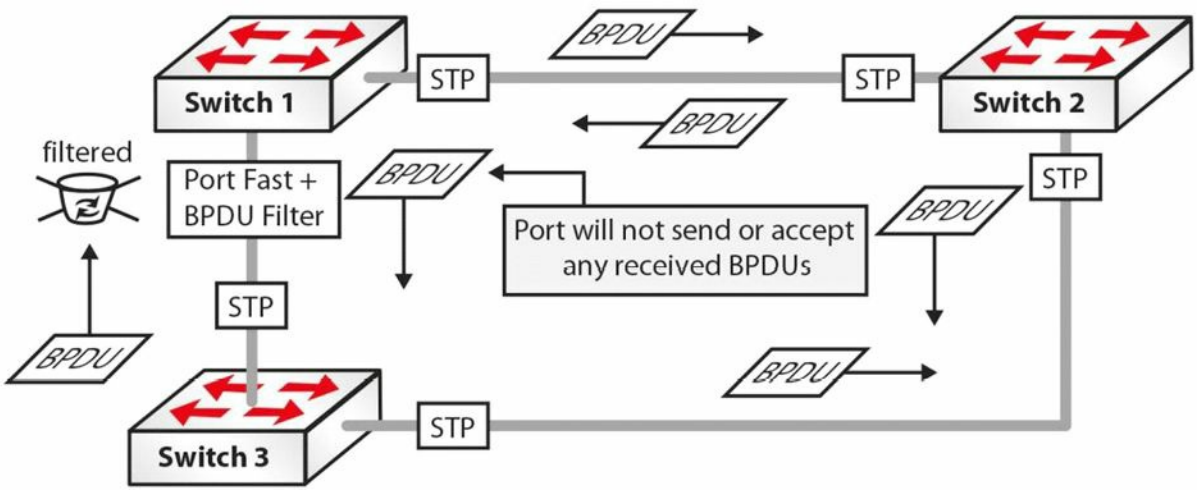
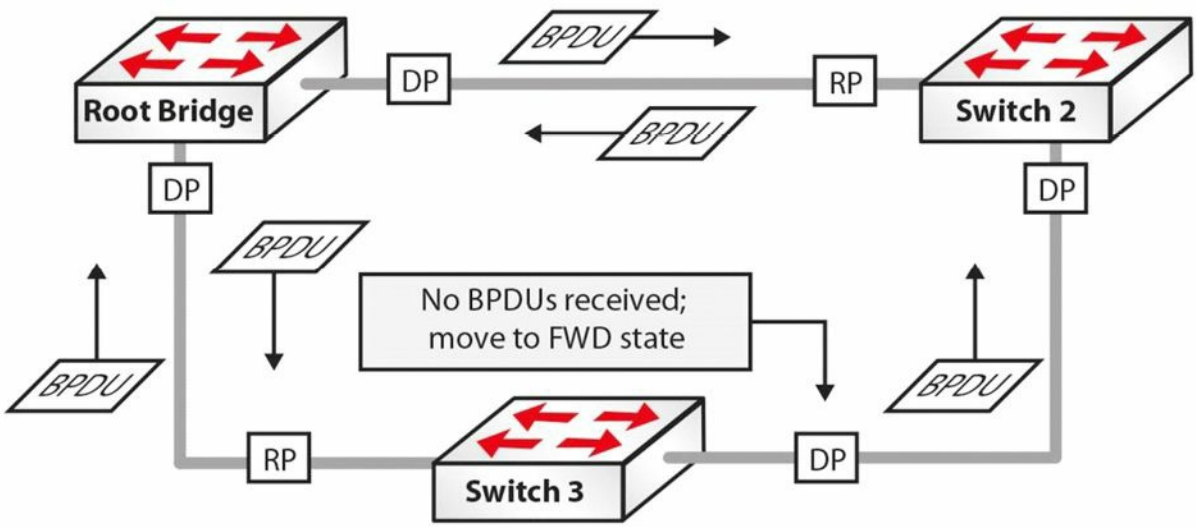


Figure 31.13 – Understanding BPDU Filter

Loop Guard

The Loop Guard feature is used to prevent the formation of loops within the Spanning Tree network. Loop Guard detects Root Ports and blocked ports and ensures that they continue to receive BPDUs. When switches receive BPDUs on blocked ports, the information is ignored because the best BPDU is still being received from the Root Bridge via the Root Port.

If the switch link is up and no BPDUs are received (due to a unidirectional link), the switch assumes that it is safe to bring this link up, and the port transitions to the Forwarding state and begins relaying received BPUDs. If a switch is connected to the other end of the link, this effectively creates a Spanning Tree loop. This concept is illustrated in Figure 31.14 below:



https://t.me/learningnets **Figure 31.14 – Understanding Loop Guard**

In Figure 31.14, the Spanning Tree network has converged and all ports are in a Blocking or Forwarding state. However, the Blocking port on Switch 3 stops receiving BPDUs from the Designated Port on Switch 2 due to a unidirectional link. Switch 3 assumes that the port can be transitioned into a Forwarding state and so begins this move. The switch then relays received BPDUs out of that port, resulting in a network loop.

When Loop Guard is enabled, the switch keeps track of all Non-Designated Ports. As long as the port continues to receive BPDUs, it is fine; however, if the port stops receiving BPDUs, it is moved into a loop-inconsistent state. In other words, when Loop Guard is enabled, the STP port state machine is modified to prevent the port from transitioning from the Non-Designated Port role to the Designated Port role in the absence of BPDUs. When implementing Loop Guard, you should be aware of the following implementation guidelines:

- Loop Guard cannot be enabled on a switch that also has Root Guard enabled
- Loop Guard does not affect Uplink Fast or Backbone Fast operation
- Loop Guard must be enabled on Point-to-Point links only
- Loop Guard operation is not affected by the Spanning Tree timers
- Loop Guard cannot actually detect a unidirectional link
- Loop Guard cannot be enabled on Port Fast or Dynamic VLAN ports

Root Guard

The Root Guard feature prevents a Designated Port from becoming a Root Port. If a port on which the Root Guard feature is enabled receives a superior BPDU, it moves the port into a root-inconsistent state, thus maintaining the current Root Bridge status quo. This concept is illustrated in Figure 31.15 below:

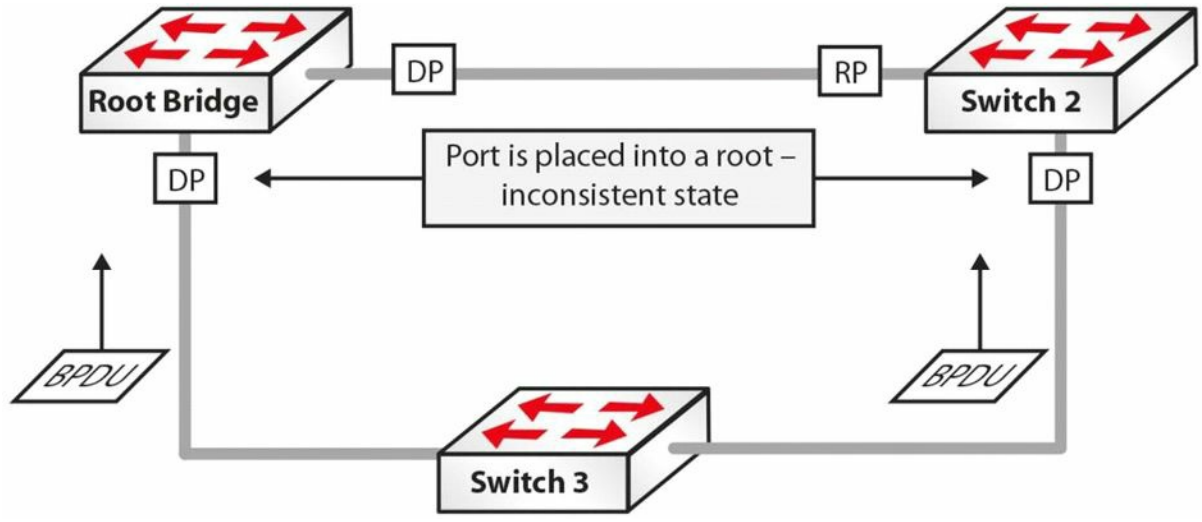


Figure 31.15 – Understanding Root Guard

In Figure 31.15, Switch 3 is added to the current STP network and sends out BPDUs that are superior to those of the current Root Bridge. Under ordinary circumstances, STP would recalculate the entire topology and Switch 3 would be elected the Root Bridge. However, because the Root Guard feature is enabled on the Designated Ports on the current Root Bridge,

https://t.me/learningnets

as well as on Switch 2, both switches will place these ports into a root-inconsistent state when they receive the superior BPDUs from Switch 3. This preserves the Spanning Tree topology.

The Root Guard feature prevents a port from becoming a Root Port, thus ensuring that the port is always a Designated Port. Unlike other STP enhancements, which can also be enabled on a global basis, Root Guard must be manually enabled on all ports where the Root Bridge should not appear. Because of this, it is important to ensure a deterministic topology when designing and implementing STP in the LAN. Root Guard enables an administrator to enforce the Root Bridge placement in the network, ensuring that no customer device inadvertently or otherwise becomes the Root of the Spanning Tree, so it is usually used on the network edge of the ISP towards the customer's equipment.

Uplink Fast

The Uplink Fast feature provides faster failover to a redundant link when the primary link fails (i.e., direct failure of the Root Port). The primary purpose of this feature is to improve the convergence time of STP in the event of a failure of an uplink. This feature is of most use on Access Layer switches with redundant uplinks to the Distribution Layer; hence, the name.

When Access Layer switches are dual-homed to the Distribution Layer, one of the links is placed into a Blocking state by STP to prevent loops. When the primary link to the Distribution Layer fails, the port in the Blocking state must transition through the Listening and Learning states before it begins forwarding traffic. This results in a 30-second delay before the switch is able to forward frames destined to other network segments. Uplink Fast operation is illustrated in Figure 31.16 below:

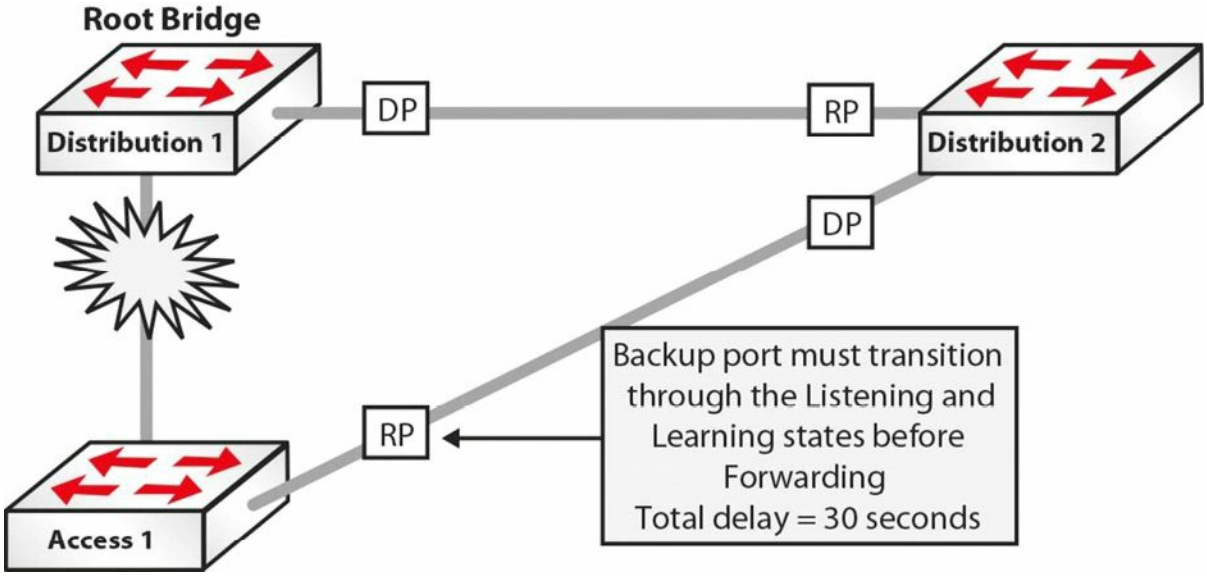


Figure 31.16 – Understanding Uplink Fast

In Figure 31.16, a failure on the link between Access 1 and Distribution 1, which is also the STP Root Bridge, would mean that STP would move the link between Access 1 and Distribution 1 into a Forwarding state (i.e., Blocking > Listening > Learning > Forwarding). The Listening and Learning states take 15 seconds each, so the port would begin to forward frames only after a total of 30 seconds had elapsed. When the Uplink Fast feature is enabled, the backup port to the Distribution Layer is immediately placed into a Forwarding state, resulting in no network downtime. This concept is illustrated in Figure 31.17 below:

https://t.me/learningnets

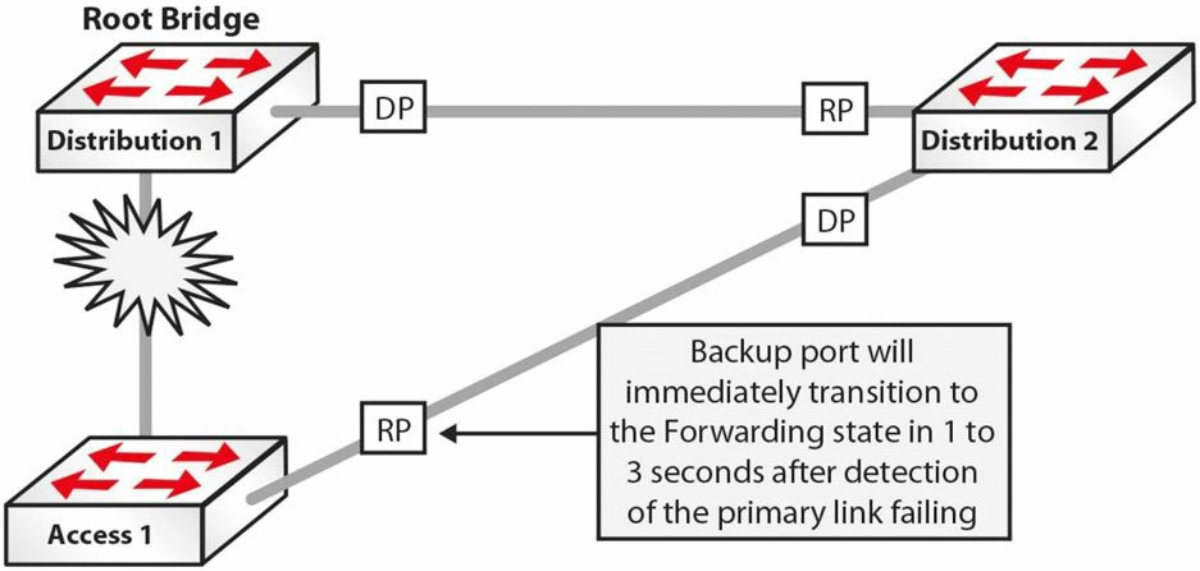


Figure 31.17 – Understanding Uplink Fast (Continued)

Backbone Fast

The Backbone Fast feature provides fast failover when an indirect link failure occurs in the STP domain. Failover occurs when the switch receives an inferior BPDU from its designated bridge (on it's Root Port). An inferior BPDU indicates that the designated bridge has lost its connection to the Root Bridge, so the switch knows there was an upstream failure and without waiting for timers to expire changes the Root Port. This is illustrated in Figure 31.18 below:

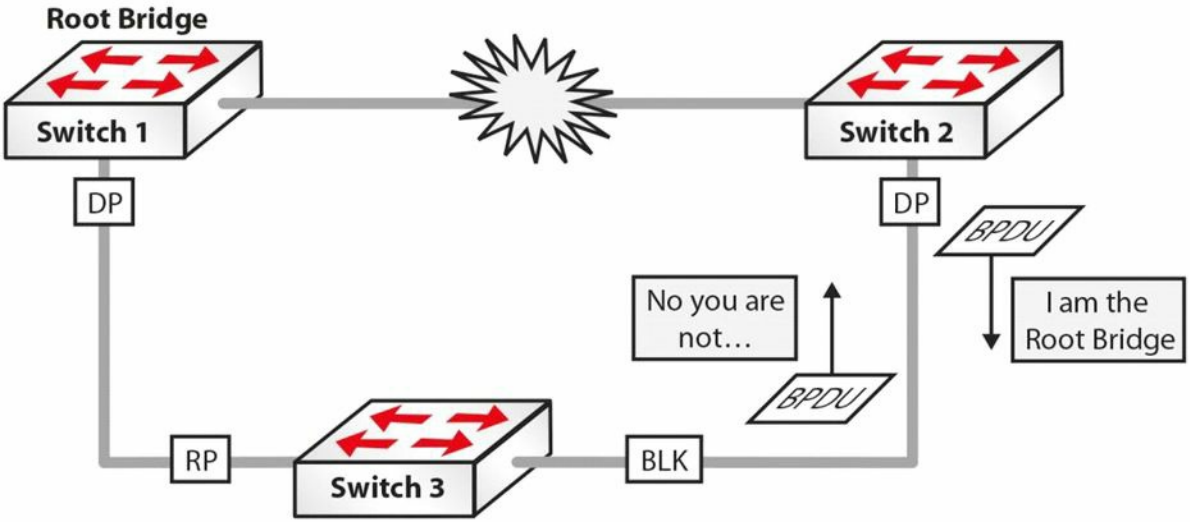


Figure 31.18 – Understanding Backbone Fast

In Figure 31.18, the link between Switch 1 and Switch 2 fails. Switch 2 detects this and sends out BPDUs indicating that it is the Root Bridge. The inferior BPDUs are received on Switch 3, which still has the BPDU information received from Switch 1 saved.

Switch 3 will ignore the inferior BPDUs until the Max Age value expires. During this time, Switch 2 continues to send BPDUs to Switch 3. When the Max Age expires, Switch 3 will age out the stored BPDU information from the Root Bridge and transition into a Listening state, and will then send out the received BPDU from the Root Bridge out to Switch 2.

Because this BPDU is better than its own, Switch 2 stops sending BPDUs, and the port between Switch 2 and Switch 3 transitions through the Listening and Learning states, and, finally, into

https://t.me/learningnets

the Forwarding state. This default method of operation by the STP process will mean that Switch 2 will be unable to forward frames for at least 50 seconds.

The Backbone Fast feature includes a mechanism that allows an immediate check to see whether the BPDU information stored on a port is still valid if an inferior BPDU is received. This is implemented with a new PDU and the Root Link Query (RLQ), which is referred to as the RLQ PDU.

Upon receipt of an inferior BPDU, the switch will send out an RLQ PDU on all Non-Designated Ports, except for the port on which the inferior BPDU was received. If the switch is the Root Bridge or it has lost its connection to the Root Bridge, it will respond to the RLQ. Otherwise, the RLQ will be propagated upstream. If the switch receives an RLQ response on its Root Port, connectivity to the Root Bridge is still intact. If the response is received on a Non-Root Port, it means that connectivity to the Root Bridge is lost, and the local switch Spanning Tree must be recalculated on the switch and the Max Age timer expired so that a new Root Port can be found. This concept is illustrated in Figure 31.19 below:

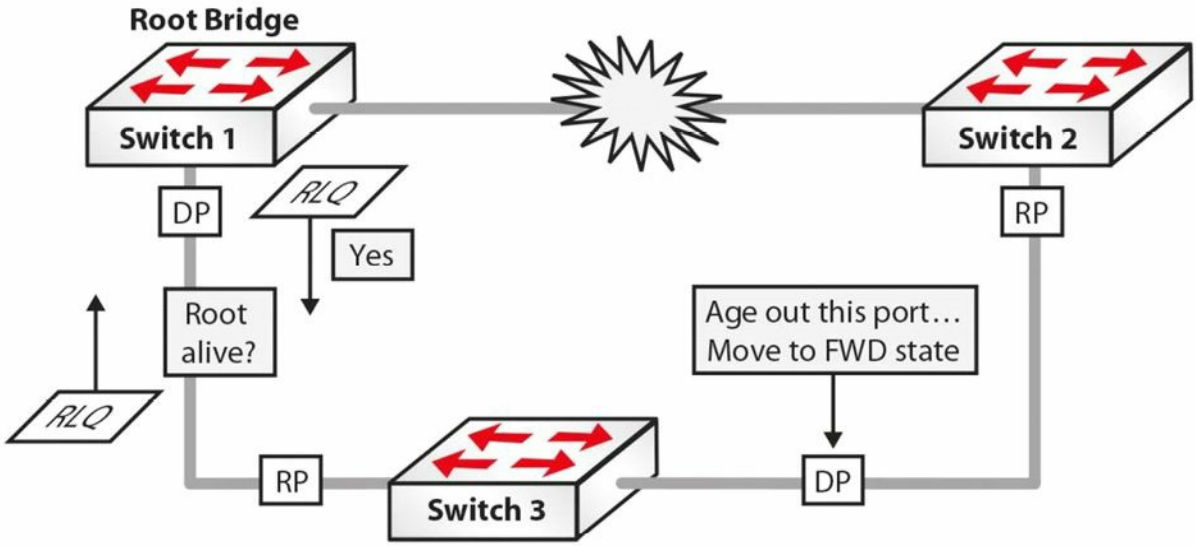


Figure 31.19 – Understanding Backbone Fast (Continued)

Referencing Figure 31.19, upon receipt of the inferior BPDU, Switch 3 sends out an RLQ request on all Non-Designated Ports, except for the port on which the BPDU was received. The Root Bridge responds via an RLQ response sent out of its Designated Port. Because the response is received on the Root Port of Switch 3, it is considered a positive response. However, if the response was received on a Non-Root Port, the response would be considered negative and the switch would need to go through the whole Spanning Tree calculation again.

Based on the positive response received on Switch 3, it can age out the port connected to Switch 2 without waiting for the Max Age timer to expire. The port, however, must still go through the Listening and Learning states. By immediately aging out the Max Age timer, Backbone Fast reduces the convergence time from 50 seconds (20 seconds Max Age + 30 seconds Listening and Learning) to 30 seconds (the time for the Listening and Learning states).

There are two types of RLQs: RLQ requests and RLQ responses. RLQ requests are typically sent out on the Root Port to check for connectivity to the Root Bridge. All RLQ responses are sent out on Designated Ports. Because the RLQ request contains the BID of the Root Bridge that sent

https://t.me/learningnets

it, if another switch in the path to the Root Bridge can still reach the Root Bridge specified in the RLQ response, it will respond back to the sending switch. If this is not the case, the switch simply forwards the query towards the Root Bridge through its Root Port.

NOTE: The RLQ PDU has the same packet format as a normal BPDU, with the only difference being that the RLQ PDU contains two Cisco SNAP addresses that are used for requests and replies.

Troubleshooting STP

Most Layer 2 issues are related to some kind of loop within the domain and this has multiple problems associated with it, including network downtime. When you are working with switch configuration and are plugging/unplugging a device, you should make sure that you aren't creating a loop in the process. To mitigate against such problems, you should usually configure Spanning Tree Protocol on switches in order to avoid situations that might occur if you happen to accidently create a loop somewhere in the network.

Every switch in a network is communicating using MAC addresses. As packets come in, the MAC address is analysed and the switch determines where that packet goes based on the destination MAC address in the Layer 2 header. Every device in the network has its own MAC address, so all the packets are very specific as to where they are going. Unfortunately, things like Broadcasts and Multicasts go to every port on the switch. If a Broadcast frame arrives at a switch port, it copies that Broadcast to every other device that might be connected to that switch. This process can often be a problem when you have loops in the network.

You should also keep in mind that the MAC address packets have no mechanism inside them to time out. In the case of TCP/IP, the IP protocol has within its header a function called TTL (Time to Live), which refers to the number of hops through a router, not actually to a specific unit of time. So if IP packets happen to be in a loop and are going through multiple routers, they will eventually time out and be removed from the network. On the other hand, switches do not offer that kind of mechanism. Layer 2 frames can theoretically loop forever, as there is no mechanism to time them out, meaning that if you create a loop, it is going to be there until you manually remove it from the network.

If you are plugging in one workstation to the network and a Broadcast reaches it, it will terminate at that point and will not be a problem for the network. On the other hand, if you misconfigure a port configuration on the switch side or you plug both ends into a switch without enabling STP, this might lead to a Broadcast storm within the Layer 2 domain. This happens because Broadcast packets are forwarded to all other ports, so the Broadcast packet keeps exiting and entering the switch on the same cable, causing a Layer 2 loop. This can lead to high resource usage and even network downtime.

If you enable STP on such a misconfigured network, the switch will recognise that a loop has occurred and it would block certain ports to avoid Broadcast storms. Every other port in the switch continues to operate normally, so the network is not affected. If STP is not configured, the only option would be to unplug the network cable that is causing the problem or administratively disable it if you can still operate the switch at that moment.

STP issues usually fall within the following three categories:

https://t.me/Harfiliyeti

- Incorrect Root Bridge
- Incorrect Root Port
- Incorrect Designated Port

Incorrect Root Bridge

Priority and base MAC addresses decide whether the Root Bridge is incorrect. You can issue the `show spanning-tree vlan <vlan#>` command to see the MAC address and switch priority. You can fix this problem with the `spanning-tree vlan <vlan#> priority <priority>` command.

Incorrect Root Port

The Root Port provides the fastest path from the switch to the Root Bridge, and the cost is cumulative across the entire path. If you suspect an incorrect Root Port, you can issue the `show spanning-tree vlan <vlan#>` command. If the Root Port is incorrect, you can issue the `spanning-tree cost <cost>` command to fix it.

Incorrect Designated Port

The Designated Port is the lowest cost port connecting a network segment to the rest of the network. If you suspect a problem with the Designated Port, you can issue the `show spanning-tree vlan <vlan#>` and `spanning-tree cost <cost>` commands.

A useful STP troubleshooting command that can debug related events is `Switch#debug spanning-tree events`.

https://t.me/learningnets

Day 31 Questions

1. How often do switches send Bridge Protocol Data Units (BPDUs)?
2. Name the STP port states in the correct order.
3. What is the default Cisco Bridge ID?
4. Which command will show you the Root Bridge and priority for a VLAN?
5. What is the STP port cost for a 100Mbps link?
6. When a port that is configured with the _____ _____ feature receives a BPDU, it immediately transitions to the errdisable state.
7. The _____ _____ feature effectively disables STP on the selected ports by preventing them from sending or receiving any BPDUs.
8. Which two commands will force the switch to become the Root Bridge for a VLAN?
9. Contrary to popular belief, the Port Fast feature does not disable Spanning Tree on the selected port. This is because even with the Port Fast feature, the port can still send and receive BPDUs. True or false?
10. The Backbone Fast feature provides fast failover when a direct link failure occurs. True or false?

https://t.me/learningnets

Day 31 Answers

1. Every two seconds.
2. Blocking, Listening, Learning, Forwarding, and Disabled.
3. 32768.
4. The `show spanning-tree vlan x` command.
5. 19.
6. BPDU Guard.
7. BPDU Filter.
8. The `spanning-tree vlan [number] priority [number]` and `spanning-tree vlan [number] root [primary|secondary]` commands.
9. True.
10. False.

https://t.me/learningnets

Day 31 Lab

Spanning Tree Root Selection Lab

Topology



Purpose

Learn how to influence which switch becomes the Spanning Tree Root Bridge.

Walkthrough

1. Set the hostname of each switch and connect them with a crossover cable. You can then check whether the interface between them is set to “trunk.”

```
SwitchA#show interface trunk
```

2. You may not see the trunk link become active until you set one side as a trunk link.

```
SwitchB#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchB(config)#int FastEthernet0/1
SwitchB(config-if)#switchport mode trunk
SwitchB(config-if)#^Z
SwitchB#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/1       1-1005
Port        Vlans allowed and active in management domain
Fa0/1       1
```

3. You will see that the other switch is left on auto mode.

```
SwitchA#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1
Port        Vlans allowed on trunk
Fa0/1       1-1005
Port        Vlans allowed and active in management domain
Fa0/1       1
```

4. Create two VLANs on each switch.

```
SwitchA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan 2
```

https://t.me/learningnets

```
SwitchA(config-vlan)#vlan 3
SwitchA(config-vlan)#^Z
SwitchA#
%SYS-5-CONFIG_I: Configured from console by console
SwitchA#show vlan brief
VLAN Name                             Status    Ports
---- -------------------              -------   --------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4,
                                                Fa0/5, Fa0/6, Fa0/7,
                                                Fa0/8, Fa0/9, Fa0/10,
                                                Fa0/11, Fa0/12, Fa0/13,
                                                Fa0/14, Fa0/15, Fa0/16,
                                                Fa0/17, Fa0/18, Fa0/19,
                                                Fa0/20, Fa0/21, Fa0/22,
                                                Fa0/23, Fa0/24
2    VLAN0002                           active
3    VLAN0003                           active
1002 fddi-default                       active
1003 token-ring-default                 active
```

Create the VLANs on Switch B as well (copy the commands above).

5. Determine which switch is the Root Bridge for VLANs 2 and 3.

```
SwitchB#show spanning-tree vlan 2
VLAN0002
  Spanning tree enabled protocol ieee
  Root ID     Priority    32770
              Address     0001.972A.7A23
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32770  (priority 32768 sys-id-ext 2)
              Address     0001.972A.7A23
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
Interface        Role  Sts  Cost      Prio.Nbr Type
---------        ----  ---  ----      -------- ----
Fa0/1            Desg  FWD  19        128.1    P2p
```

You can see that Switch B is the Root. Do the same command on Switch A and check for VLAN 3. The priority is 32768 plus the VLAN number, which is 2 in this case. The lowest MAC address will then determine the Root Bridge.

```
SwitchB#show spanning-tree vlan 3
```

https://t.me/learningnets

```
VLAN0003
  Spanning tree enabled protocol ieee
  Root ID    Priority    32771
             Address     0001.972A.7A23
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32771  (priority 32768 sys-id-ext 3)
             Address     0001.972A.7A23
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role  Sts  Cost      Prio.Nbr Type
---------        ----  ---  ----      -------- ----
Fa0/1            Desg  FWD  19        128.1    P2p
```

The MAC address I have for Switch A is higher, which is why it didn't become the Root Bridge：

```
0010.1123.D245
```

6. Set the other switch to be the Root Bridge for VLANs 2 and 3. Use the `spanning-tree vlan 2 priority 4096` command for VLAN 2 and the `spanning-tree Vlan 3 root primary` for VLAN 3.

```
SwitchA(config)#spanning-tree vlan 2 priority 4096
SwitchA(config)#spanning-tree vlan 3 root primary
SwitchA#show spanning-tree vlan 2
VLAN0002
  Spanning tree enabled protocol ieee
  Root ID    Priority    4098
             Address     0010.1123.D245
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4098  (priority 4096 sys-id-ext 2)
             Address     0010.1123.D245
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role  Sts  Cost      Prio.Nbr Type
---------        ----  ---  ----      -------- ----
Fa0/1            Desg  FWD  19        128.1    P2p
SwitchA#show spanning-tree vlan 3
VLAN0003
  Spanning tree enabled protocol ieee
  Root ID    Priority    24579
             Address     0010.1123.D245
```

https://t.me/learningnets

```
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    24579  (priority 24576 sys-id-ext 3)
             Address     0010.1123.D245
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
Interface        Role  Sts  Cost      Prio.Nbr Type
---------        ----  ---  ----      -------- ----
Fa0/1            Desg  FWD  19        128.1    P2p
SwitchA#
```

NOTE: Despite Switch B having the lower Bridge ID, Switch A was forced to be the Root Bridge.

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 32 – Rapid Spanning Tree Protocol

Day 32 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's lab
- Read the ICND2 cram guide
- Spend 15 minutes on the subnetting.org website

The IEEE 802.1D standard was designed at a time when the recovery of connectivity after an outage was within a minute or so, which was considered adequate performance. With the IEEE 802.1D STP, recovery takes around 50 seconds, which includes 20 seconds for the Max Age timer to expire and then an additional 30 seconds for the port to transition from the Blocking state to the Forwarding state.

As computer technology evolved, and networks became more critical, it became apparent that more rapid network convergence was required. Cisco addressed this requirement by developing some proprietary enhancements to STP that include Backbone Fast and Uplink Fast.

Today you will learn about the following:

- The need for RSTP
- RSTP configuration

This lesson maps to the following CCNA syllabus requirements:

- Identify enhanced switching technologies
  - RSTP
  - PVSTP

The Need for RSTP

With the continued evolution of technology, and the amalgamation of routing and switching capabilities on the same physical platform, it soon became apparent that switched network convergence lagged behind that of routing protocols such as OSPF and EIGRP, which are able to provide an alternate path in less time. The 802.1W standard was designed to address this.

The IEEE 802.1W standard, or Rapid Spanning Tree Protocol (RSTP), significantly reduces the time taken for STP to converge when a link failure occurs. With RSTP, network failover to an alternate path or link can occur in a subsecond timeframe. RSTP is an extension of 802.1D that performs functions similar to Uplink Fast and Backbone Fast. RSTP performs better than traditional STP, with no additional configuration. Additionally, RSTP is backward compatible with the original IEEE 802.1D STP standard. It does this by using a modified BPDU, as shown in the screenshot below:

https://t.me/learningnets

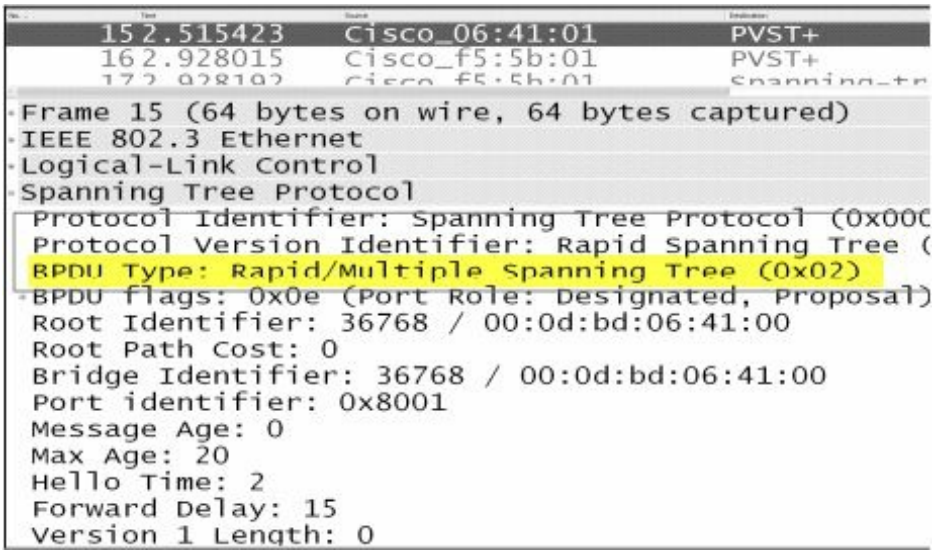


Figure 32.1 – Modified BPDU

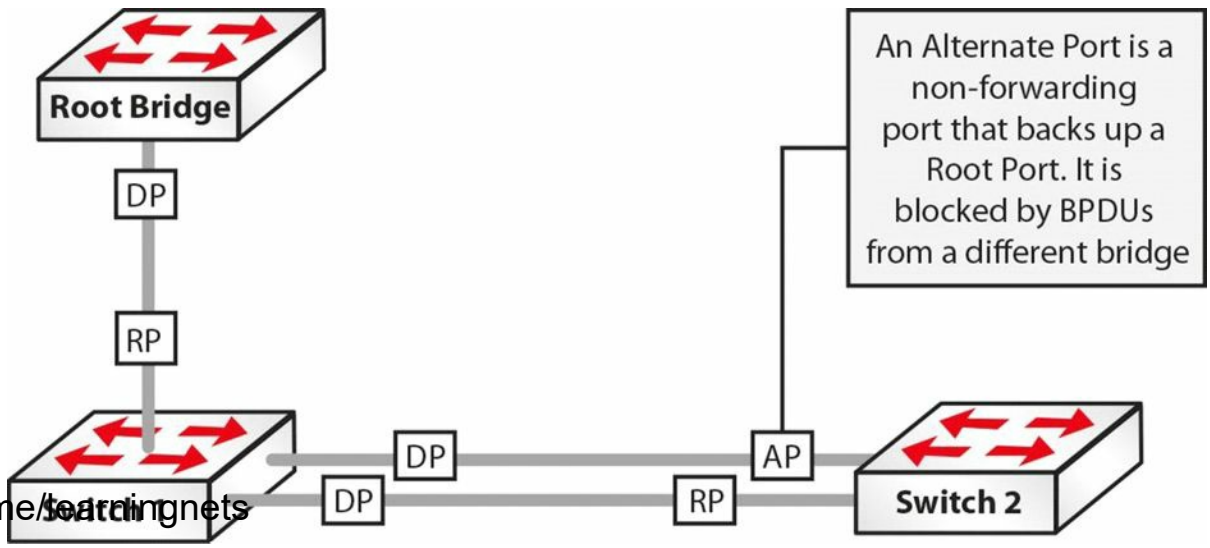
RSTP port states can be mapped against STP port states as follows:

- Disabled – Discarding
- Blocking – Discarding
- Listening – Discarding
- Learning – Learning
- Forwarding – Forwarding

RSTP port roles include the following:

- Root (Forwarding state)
- Designated (Forwarding state)
- Alternate (Blocking state)
- Backup (Blocking state)

For the exam it's very important that you understand the bullet points above, especially which port states forward traffic (once the network is converged). Figures 32.2 and 32.3 illustrate an RSTP Alternate Port and an RSTP Backup Port, respectively:



https://t.me/learningnets

Figure 32.2 – RSTP Alternate Port

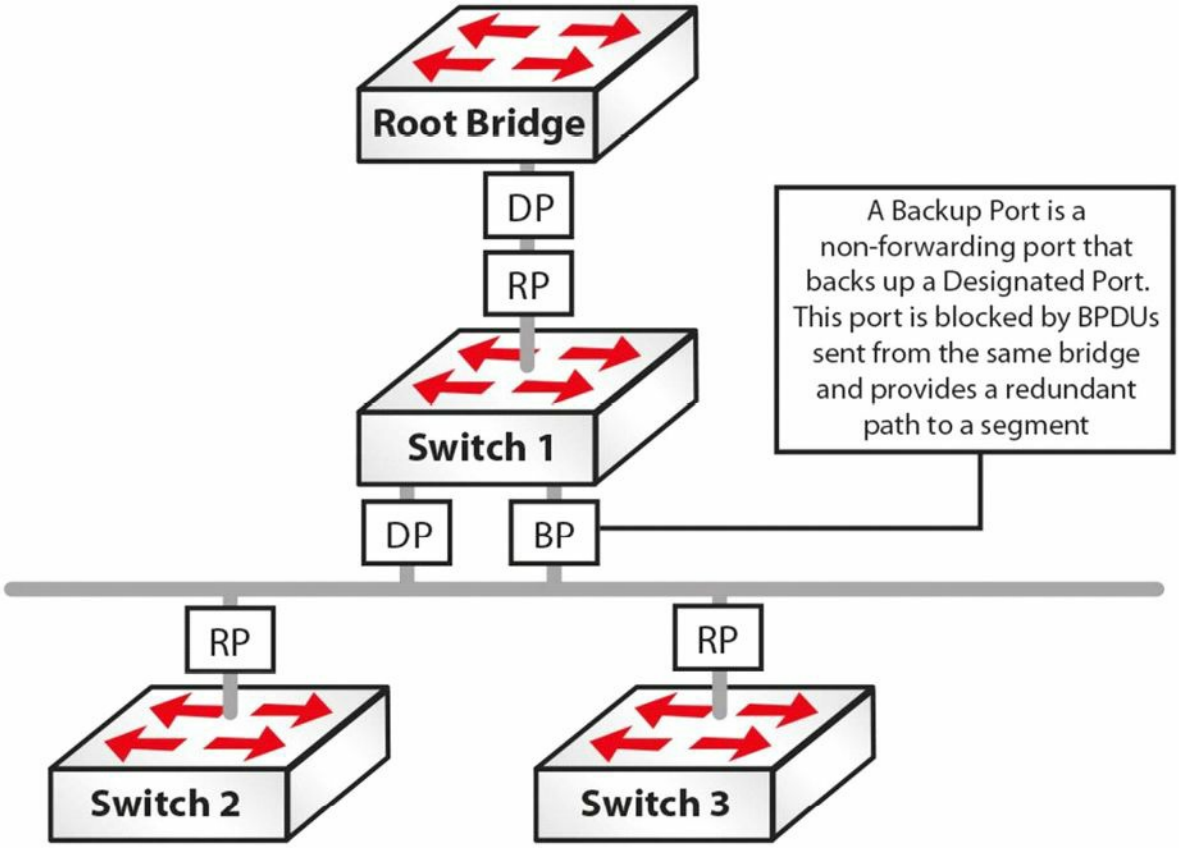


Figure 32.3 – RSTP Backup Port

RSTP with PVST+

Per VLAN Spanning Tree Plus (PVST+) allows for an individual STP instance per VLAN. Traditional or Normal PVST+ mode relies on the use of the older 802.1D STP for switched network convergence in the event of a link failure.

RPVST+

Rapid Per VLAN Spanning Tree Plus (R-PVST+) allows for the use of 802.1W with PVST+. This allows for an individual RSTP instance per VLAN, whilst providing much faster convergence than would be attained with the traditional 802.1D STP. By default, when RSTP is enabled on a Cisco switch, R-PVST+ is enabled on the switch.

Here is a little memory trick you can use to remember the letter designation of the various IEEE STP specification:

- 802.1D (“Classic” Spanning Tree) – It’s dog-gone slow
- 802.1W (Rapid Spanning Tree) – Imagine Elmer Fudd saying “rapid” as “wapid”
- 802.1S (Multiple Spanning Tree) – You add the letter “s” to nouns to make them plural (multiple) but this is a CCNP SWITCH subject

Configuring RSTP

This can be achieved with one command!

```
Switch(config)#spanning-tree mode rapid-pvst
```

https://t.me/learningnets

```
Switch#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0050, VLAN0060, VLAN0070
```

Day 32 Questions

1. RSTP is not backward compatible with the original IEEE 802.1D STP standard. True or false?
2. What are the RSTP port states?
3. What are the four RSTP port roles?
4. Which command enables RSTP?
5. By default, when RSTP is enabled on a Cisco switch, R-PVST+ is enabled on the switch. True or false?

https://t.me/learningnets

Day 32 Answers

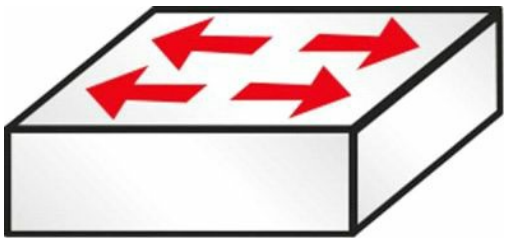
1. False.
2. Discarding, Learning, and Forwarding.
3. Root, Designated, Alernate, and Backup.
4. The `spanning-tree mode rapid-pvst` command.
5. True.

Because todays lesson is so short, please do review yesterdays notes again in detail.

Day 32 Lab

RSTP Lab

Topology



Purpose

Learn the configuration command for RSTP.

Walkthrough

1. Check the Spanning Tree mode on your switch.

```
SwitchA#show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0002 VLAN0003
```

2. Change the mode to RSTP and check again.

```
SwitchA(config)#spanning-tree mode rapid-pvst
SwitchA#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0002 VLAN0003
```

3. Repeat Day 31 (STP) lab using RSTP mode instead.
4. Can you predict which ports will be Root/Designated/Blocking beforehand?

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 33 – EtherChannels and Link Aggregation Protocols

Day 33 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's lab
- Read the ICND2 cram guide
- Spend 15 minutes on the subnetting.org website

Cisco IOS software allows administrators to combine multiple physical links in the chassis into a single logical link. This provides an ideal solution for load sharing, as well as link redundancy, and can be used by both Layer 2 and Layer 3 subsystems.

Today you will learn about the following:

- Understanding EtherChannels
- Port Aggregation Protocol (PAgP) overview
- PAgP port modes
- PAgP EtherChannel Protocol packet forwarding
- Link Aggregation Control Protocol (LACP) overview
- LACP port modes
- EtherChannel load-distribution methods
- EtherChannel configuration guidelines
- Configuring and verifying Layer 2 EtherChannels

This lesson maps to the following ICND2 syllabus requirement:

- EtherChannels

Understanding EtherChannels

An EtherChannel is comprised of physical, individual FastEthernet, GigabitEthernet, or Ten-GigabitEthernet (10Gbps) links that are bundled together into a single logical link, as illustrated in Figure 33.1 below. An EtherChannel comprised of FastEthernet links is referred to as a FastEtherChannel (FEC); an EtherChannel comprised of GigabitEthernet links is referred to as a GigabitEtherChannel (GEC); and, finally, an EtherChannel comprised of Ten-GigabitEthernet links is referred to as a Ten-GigabitEtherChannel (10GEC):

https://t.me/learningnets

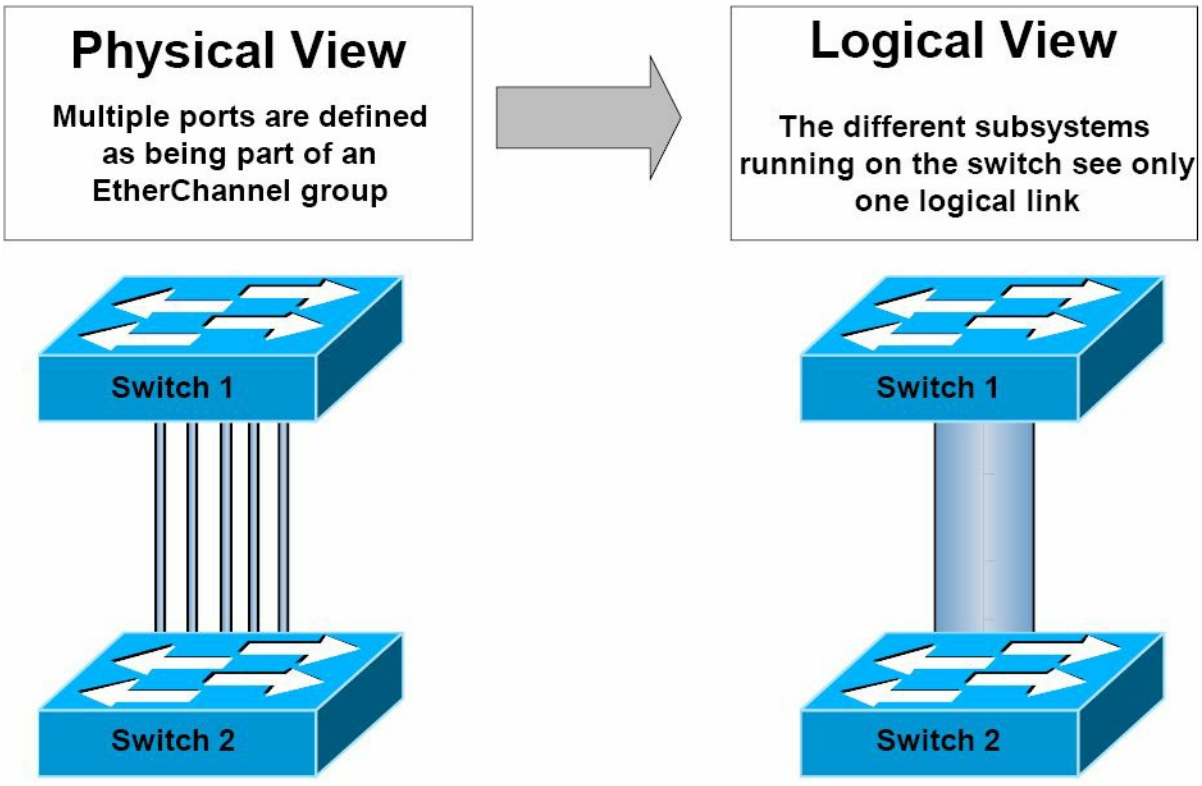


Figure 33.1 – EtherChannel Physical and Logical Views

Each EtherChannel can consist of up to eight ports. Physical links in an EtherChannel must share similar characteristics, such as be defined in the same VLAN or have the same speed and duplex settings, for example. When configuring EtherChannels on Cisco Catalyst switches, it is important to remember that the number of supported EtherChannels will vary between the different Catalyst switch models.

For example, on the Catalyst 3750 series switches, the range is 1 to 48; on the Catalyst 4500 series switches, the range is 1 to 64; and on the flagship Catalyst 6500 series switches, the number of valid values for EtherChannel configuration depends on the software release. For releases prior to Release 12.1(3a)E3, valid values are from 1 to 256; for Releases 12.1(3a)E3, 12.1(3a)E4, and 12.1(4)E1, valid values are from 1 to 64. Release 12.1(5c)EX and later support a maximum of 64 values, ranging from 1 to 256.

NOTE: You are not expected to known the values supported in each different IOS version.

There are two link aggregation protocol options that can be used to automate the creation of an EtherChannel group: Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP). PAgP is a Cisco proprietary protocol, while LACP is part of the IEEE 802.3ad specification for creating a logical link from multiple physical links. These two protocols will be described in detail throughout this module.

Port Aggregation Protocol Overview

Port Aggregation Protocol (PAgP) is a Cisco proprietary link aggregation protocol that enables the automatic creation of EtherChannels. By default, PAgP packets are sent between EtherChannel-capable ports in order to negotiate the forming of an EtherChannel. These packets are sent to the destination Multicast MAC address 01-00-0C-CC-CC-CC, which is also the same Multicast address that is used by CDP, UDLD, VTP, and DTP. Figure 33.2 below shows the

https://t.me/learningnets

fields contained within a PAgP frame as seen on the wire:

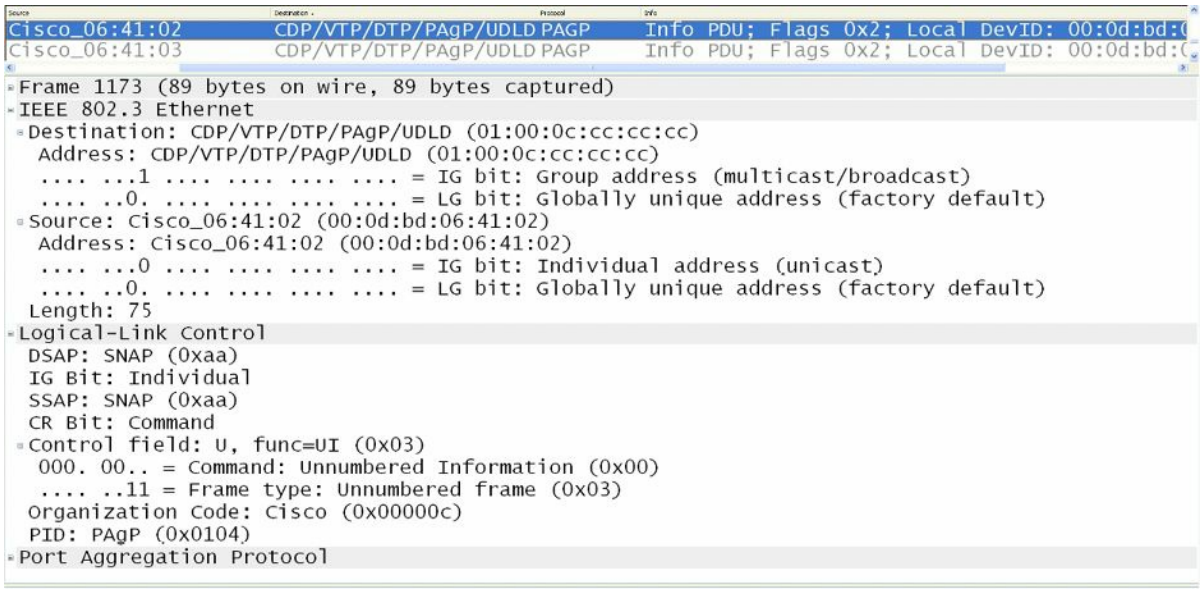


Figure 33.2 – PAgP Ethernet Header

Although going into detail on the PAgP packet format is beyond the scope of the CCNA exam requirements, Figure 33.3 below shows the fields contained in a typical PAgP packet. Some of the fields contained within the PAgP packet are of relevance to the CCNA exam and will be described in detail as we progress through this module:

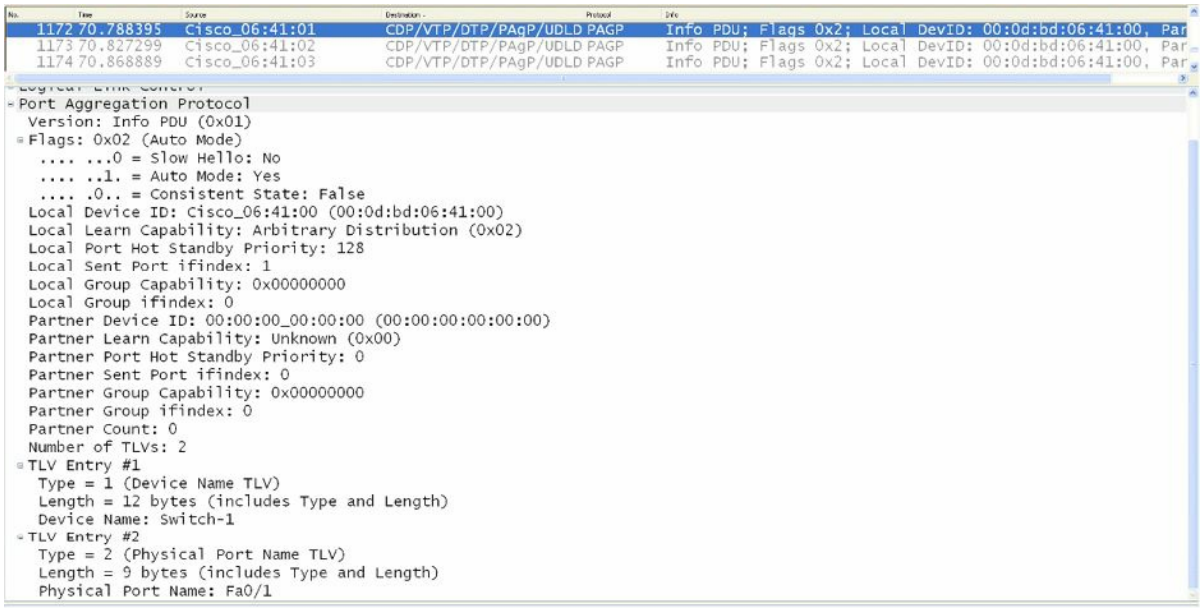


Figure 33.3 – The Port Aggregation Protocol Frame

PAgP Port Modes

PAgP supports different port modes that determine whether an EtherChannel will be formed between two PAgP-capable switches. Before we delve into the two PAgP port modes, one particular mode deserves special attention. This mode (the “on” mode) is sometimes incorrectly referenced as a PAgP mode. The truth, however, is that it is not a PAgP port mode.

The on mode forces a port to be placed into a channel unconditionally. The channel will only be created if another switch port is connected and is configured in the on mode. When this mode is enabled, there is no negotiation of the channel performed by the local EtherChannel

https://t.me/learningnets

protocol. In other words, this effectively disables EtherChannel negotiation and forces the port to the channel. The operation of this mode is similar to the operation of the `switchport nonegotiate` command on trunk links. It is important to remember that switch interfaces that are configured in the on mode do not exchange PAgP packets.

Switch EtherChannels using PAgP may be configured to operate in one of two modes: auto or desirable. These two PAgP modes of operation are described in the following sections.

Auto Mode

Auto mode is a PAgP mode that will negotiate with another PAgP port only if the port receives a PAgP packet. When this mode is enabled, the port(s) will never initiate PAgP communications but will instead listen passively for any received PAgP packets before creating an EtherChannel with the neighbouring switch.

Desirable Mode

Desirable mode is a PAgP mode that causes the port to initiate PAgP negotiation for a channel with another PAgP port. In other words, in this mode, the port actively attempts to establish an EtherChannel with another switch running PAgP.

In summation, it is important to remember that switch interfaces configured in the on mode do not exchange PAgP packets, but they do exchange PAgP packets with partner interfaces configured in the auto or desirable modes. Table 33.1 shows the different PAgP combinations and the result of their use in establishing an EtherChannel:

Table 33.1 – EtherChannel Formation Using Different PAgP Modes

Switch 1 PAgP Mode	Switch 2 PAgP Mode	EtherChannel Result
Auto	Auto	No EtherChannel Formed
Auto	Desirable	EtherChannel Formed
Desirable	Auto	EtherChannel Formed
Desirable	Desirable	EtherChannel Formed

PAgP EtherChannel Protocol Packet Forwarding

While PAgP allows for all links within the EtherChannel to be used to forward and receive user traffic, there are some restrictions that you should be familiar with regarding the forwarding of traffic from other protocols. DTP and CDP send and receive packets over all the physical interfaces in the EtherChannel. PAgP sends and receives PAgP Protocol Data Units only from interfaces that are up and have PAgP enabled for auto or desirable modes.

When an EtherChannel bundle is configured as a trunk port, the trunk sends and receives PAgP frames on the lowest numbered VLAN. Spanning Tree Protocol (STP) always chooses the first operational port in an EtherChannel bundle. The `show pagp [channel number] neighbor` command, which can also be used to validate the port that will be used by STP to send and receive packets, determines the port STP will use in an EtherChannel bundle, as shown in the following output:

https://t.me/learningnets

```
Switch-1#show pagp neighbor
Flags:  S - Device is sending Slow hello. C - Device is in Consistent state.
        A - Device is in Auto mode.       P - Device learns on physical port.
Channel group 1 neighbors
          Partner     Partner          Partner         Partner Group
Port      Name        Device ID        Port       Age  Flags   Cap.
Fa0/1     Switch-2    0014.a9e5.d640   Fa0/1      2s   SC      10001
Fa0/2     Switch-2    0014.a9e5.d640   Fa0/2      1s   SC      10001
Fa0/3     Switch-2    0014.a9e5.d640   Fa0/3      15s  SC      10001
```

Referencing the above output, STP will send packets only out of port FastEthernet0/1 because it is the first operational interface. If that port fails, STP will send packets out of FastEthernet0/2. The default port used by PAgP can be viewed with the `show EtherChannel summary` command, as illustrated in the following output:

```
Switch-1#show EtherChannel summary
Flags:  D - down
        I - stand-alone
        H - Hot-standby (LACP only)
        R - Layer3
        u - unsuitable for bundling
        U - in use
        d - default port
        P - in port-channel
        s - suspended
        S - Layer2
        f - failed to allocate aggregator
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+--------------------------------
1      Po1(SU)        PAgP        Fa0/1(Pd)   Fa0/2(P)    Fa0/3(P)
```

When configuring additional STP features such as Loop Guard on an EtherChannel, it is very important to remember that if Loop Guard blocks the first port, no BPDUs will be sent over the channel, even if other ports in the channel bundle are operational. This is because PAgP will enforce uniform Loop Guard configuration on all of the ports that are part of the EtherChannel group.

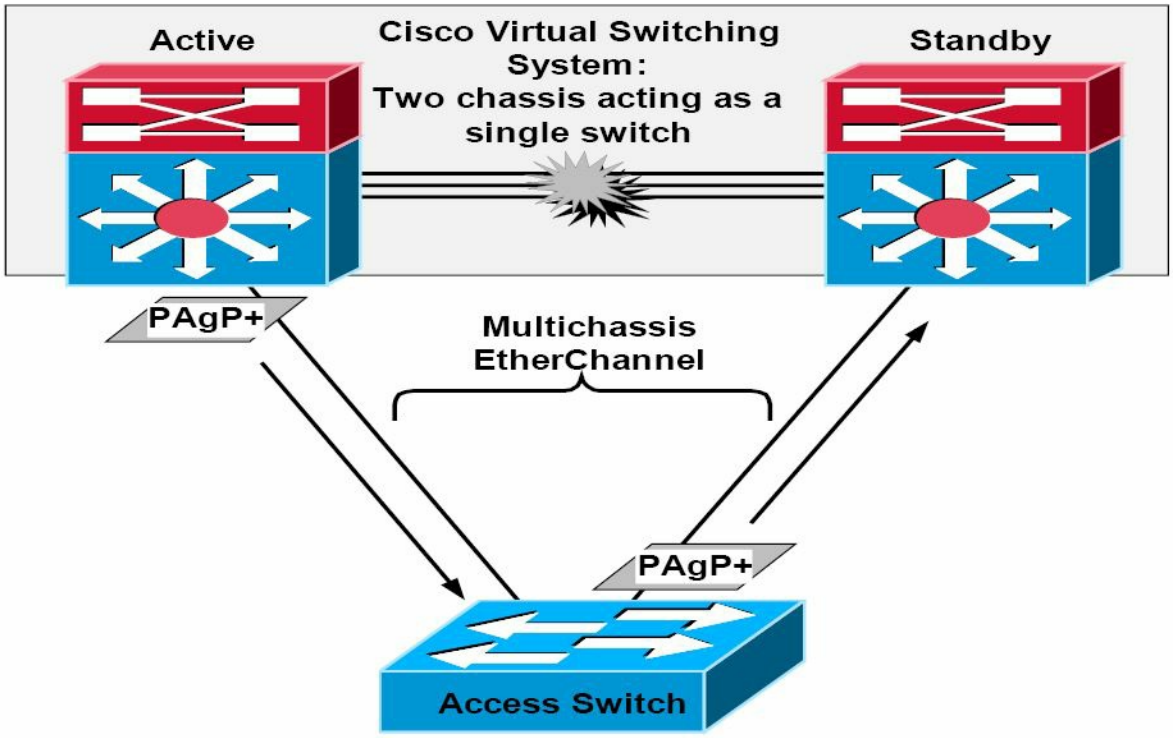


Real-World Implementation

https://t.me/learningnets

In production networks, you may run across the Cisco Virtual Switching System (VSS), which is comprised of two physical Catalyst 6500 series switches acting as a single logical switch. In the VSS, one switch is selected as the active switch, while the other is selected as the standby switch. The two switches are connected together via an EtherChannel, which allows for the sending and receiving of control packets between them.

Access switches are connected to the VSS using Multichassis EtherChannel (MEC). An MEC is simply an EtherChannel that spans the two physical Catalyst 6500 switches but terminates to the single logical VSS. Enhanced PAgP (PAgP+) can be used to allow the Catalyst 6500 switches to communicate via the MEC in the event that the EtherChannel between them fails, which would result in both switches assuming the active role (dual active), effectively affecting forwarding of traffic within the switched network. This is illustrated in the diagram below:



While VSS is beyond the scope of the CCNA exam requirements, it is beneficial to know that only PAgP can be used to relay VSS control packets. Therefore, if implementing EtherChannels in a VSS environment, or an environment in which VSS may eventually be implemented, you may want to consider running PAgP instead of LACP, which is an open standard that does not support the proprietary VSS frames. VSS will not be described any further in this guide.

Link Aggregation Control Protocol Overview

Link Aggregation Control Protocol (LACP) is part of the IEEE 802.3ad specification for creating a logical link from multiple physical links. Because LACP and PAgP are incompatible, both ends of the link need to run LACP in order to automate the formation of EtherChannel groups.

As is the case with PAgP, when configuring LACP EtherChannels, all LAN ports must be the same speed and must all be configured as either Layer 2 or Layer 3 LAN ports. If a link within a port channel fails, traffic previously carried over the failed link is switched over to the remaining links within the port channel. Additionally, when you change the number of active bundled ports in a port channel, traffic patterns will reflect the rebalanced state of the port channel.

https://t.me/learningnets

LACP supports the automatic creation of port channels by exchanging LACP packets between ports. It learns the capabilities of port groups dynamically and informs the other ports. Once LACP identifies correctly matched Ethernet links, it facilitates grouping the links into a GigabitEthernet port channel. Unlike PAgP, where ports are required to have the same speed and duplex settings, LACP mandates that ports be only full-duplex, as half-duplex is not supported. Half-duplex ports in an LACP EtherChannel are placed into the suspended state.

By default, all inbound Broadcast and Multicast packets on one link in a port channel are blocked from returning on any other link of the port channel. LACP packets are sent to the IEEE 802.3 Slow Protocols Multicast group address 01-80-C2-00-00-02. LACP frames are encoded with the EtherType value 0x8809. Figure 33.4 below illustrates these fields in an Ethernet frame:

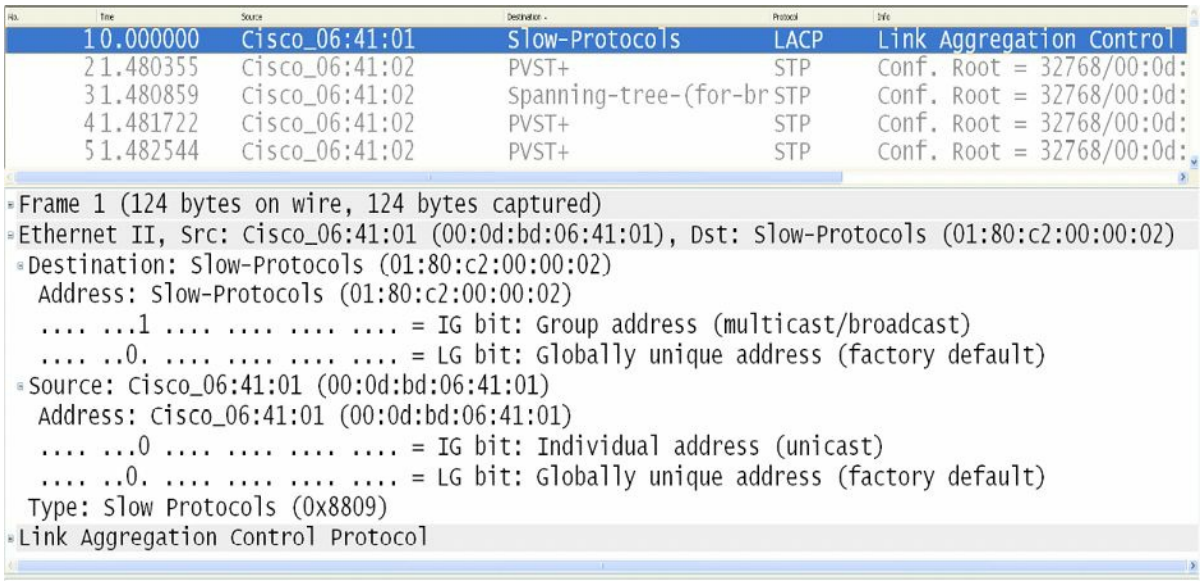


Figure 33.4 – IEEE 802.3 LACP Frame

LACP Port Modes

LACP supports the automatic creation of port channels by exchanging LACP packets between ports. LACP does this by learning the capabilities of port groups dynamically and informing the other ports. Once LACP identifies correctly matched Ethernet links, it facilitates grouping the links into a port channel. Once an LACP mode has been configured, it can only be changed if a single interface has been assigned to the specified channel group. LACP supports two modes: active and passive. These two modes of operation are described in the following sections.

LACP Active Mode

LACP active mode places a switch port into an active negotiating state in which the switch port initiates negotiations with remote ports by sending LACP packets. Active mode is the LACP equivalent of PAgP desirable mode. In other words, in this mode, the switch port actively attempts to establish an EtherChannel with another switch that is also running LACP.

LACP Passive Mode

When a switch port is configured in passive mode, it will negotiate with an LACP channel only if it receives another LACP packet. In passive mode, the port responds to LACP packets that the interface receives but does not start LACP packet negotiation. This setting minimises the

https://t.me/learningnets

transmission of LACP packets. In this mode, the port channel group attaches the interface to the EtherChannel bundle. This mode is similar to the auto mode that is used with PAgP.

It is important to remember that the active and passive modes are valid on non-PAgP interfaces only. However, if you have a PAgP EtherChannel and want to convert it to LACP, then Cisco IOS software allows you to change the protocol at any time. The only caveat is that this change causes all existing EtherChannels to reset to the default channel mode for the new protocol. Table 33.2 below shows the different LACP combinations and the result of their use in establishing an EtherChannel between two switches:

Table 33.2 – EtherChannel Formation Using Different LACP Modes

Switch 1 LACP Mode	Switch 2 LACP Mode	EtherChannel Result
Passive	Passive	No EtherChannel Formed
Passive	Active	EtherChannel Formed
Active	Active	EtherChannel Formed
Active	Passive	EtherChannel Formed

EtherChannel Load-Distribution Methods

For both PAgP and LACP EtherChannels, Catalyst switches use a polymorphic algorithm that utilises key fields from the header of the packet to generate a hash, which is then matched to a physical link in the EtherChannel group. In other words, the switch distributes the traffic load across the links in an EtherChannel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the EtherChannel.

This operation can be performed on MAC addresses or IP addresses and can be based solely on source or destination addresses, or even both source and destination addresses. While delving into detail on the actual computation of the hash used in EtherChannel load distribution is beyond the scope of the CCNA exam requirements, it is important to know that the administrator can define which fields in the header can be used as input to the algorithm used to determine the physical link transport to the packet.

The load-distribution method is configured via the `port-channel load-balance [method]` global configuration command. Only a single method can be used at any given time. Table 33.3 below lists and describes the different methods available in Cisco IOS Catalyst switches when configuring EtherChannel load distribution:

Table33.3 – EtherChannel Load-Distribution (Load-Balancing) Options

Method	Description
dst-ip	Performs load distribution based on the destination IP address
dst-mac	Performs load distribution based on the destination MAC address
dst-port	Performs load distribution based on the destination Layer 4 port
src-dst-ip	Performs load distribution based on the source and destination IP address
src-dst-mac	Performs load distribution based on the source and destination MAC address

https://t.me/learningnets

src-dst-port	Performs load distribution based on the source and destination Layer 4 port
src-ip	Performs load distribution based on the source IP address
src-mac	Performs load distribution based on the source MAC address
src-port	Performs load distribution based on the source Layer 4 port

EtherChannel Configuration Guidelines

The following section lists and describes the steps that are required to configure Layer 2 PAgP EtherChannels. However, before we delve into these configuration steps, it is important that you are familiar with the following caveats when configuring Layer 2 EtherChannels:

- Each EtherChannel can have up to eight compatibly configured Ethernet interfaces. LACP allows you to have more than eight ports in an EtherChannel group. These additional ports are hot-standby ports.
- All interfaces in the EtherChannel must operate at the same speed and duplex modes. Keep in mind, however, that unlike PAgP, LACP does not support half-duplex ports.
- Ensure that all interfaces in the EtherChannel are enabled. In some cases, if the interfaces are not enabled, the logical port channel interface will not be created automatically.
- When first configuring an EtherChannel group, it is important to remember that ports follow the parameters set for the first group port added.
- If Switch Port Analyzer (SPAN) is configured for a member port in an EtherChannel, then the port will be removed from the EtherChannel group.
- It is important to assign all interfaces in the EtherChannel to the same VLAN or configure them as trunk links. If these parameters are different, the channel will not form.
- Keep in mind that similar interfaces with different STP path costs (manipulated by an administrator) can still be used to form an EtherChannel.
- It is recommended to shut down all member interfaces prior to beginning channelling configuration.

Configuring and Verifying Layer 2 EtherChannels

This section describes the configuration of Layer 2 EtherChannels by unconditionally forcing the selected interfaces to establish an EtherChannel.

1. The first configuration step is to enter Interface Configuration mode for the desired EtherChannel interface(s) via the `interface [name]` or `interface range [range]` global configuration command.
2. The second configuration step is to configure the interfaces as Layer 2 switch ports via the `switchport` interface configuration command.
3. The third configuration step is to configure the switch ports as either trunk or access links via the `switchport mode [access|trunk]` interface configuration command.

https://thelearningnets

4. Optionally, if the interface or interfaces have been configured as access ports, assign them to the same VLAN using the `switchport access vlan [number]` command. If the interface or interfaces have been configured as a trunk port, select the VLANs allowed to traverse the trunk by issuing the `switchport trunk allowed vlan [range]` interface configuration command; if VLAN 1 will not be used as the native VLAN (for 802.1Q), enter the native VLAN by issuing the `switchport trunk native vlan [number]` interface configuration command. This configuration must be the same on all of the port channel member interfaces.
5. The next configuration step is to configure the interfaces to unconditionally trunk via the `channel-group [number] mode on` interface configuration command.

The configuration of unconditional EtherChannels using the steps described above will be based on the network topology illustrated in Figure 33.5 below:

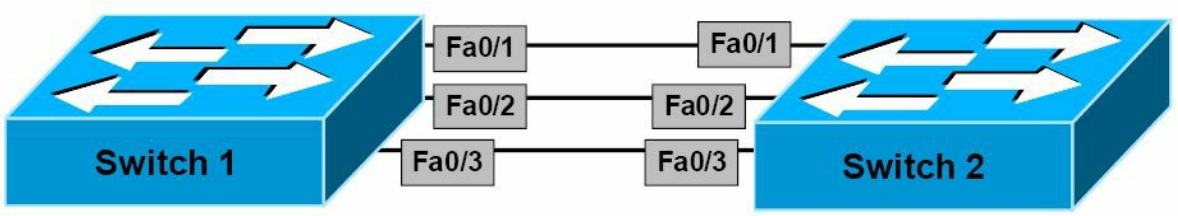


Figure 33.5 – Network Topology for EtherChannel Configuration Output Examples

The following output illustrates how to configure unconditional channelling on Switch 1 and Switch 2 based on the network topology depicted in Figure 33.5. The EtherChannel will be configured as a Layer 2 802.1Q trunk using default parameters:

```
Switch-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch-1(config)#interface range fa0/1 - 3
Switch-1(config-if-range)#no shutdown
Switch-1(config-if-range)#switchport
Switch-1(config-if-range)#switchport trunk encapsulation dot1q
Switch-1(config-if-range)#switchport mode trunk
Switch-1(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1
Switch-1(config-if-range)#exit
Switch-1(config)#exit
```

NOTE: Notice that the switch automatically creates `interface port-channel 1` by default (refer to the output below). No explicit user configuration is required to configure this interface.

```
Switch-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch-2(config)#interface range fa0/1 - 3
Switch-2(config-if-range)#switchport
Switch-2(config-if-range)#switchport trunk encapsulation dot1q
Switch-2(config-if-range)#switchport mode trunk
```

https://t.me/learningnets

```
Switch-2(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1
Switch-2(config-if-range)#exit
Switch-2(config)#exit
```

The `show EtherChannel [options]` command can then be used to verify the configuration of the EtherChannel. The available options (which may vary depending upon platform) are printed in the following output:

```
Switch-2#show EtherChannel ?
  <1-6>          Channel group number
  detail         Detail information
  load-balance  Load-balance/frame-distribution scheme among ports in port-channel
  port           Port information
  port-channel   Port-channel information
  protocol       protocol enabled
  summary        One-line summary per channel-group
  |              Output modifiers
  <cr>
```

The following output illustrates the `show EtherChannel summary` command:

```
Switch-2#show EtherChannel summary
Flags:  D - down
        I - stand-alone
        H - Hot-standby (LACP only)
        R - Layer3
        u - unsuitable for bundling
        U - in use
        d - default port
        P - in port-channel
        s - suspended
        S - Layer2
        f - failed to allocate aggregator
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+--------------------------------
1      Po1(SU)          -        Fa0/1(Pd)   Fa0/2(P)    Fa0/3(P)
```

In the output above, you can see that there are three links in Channel Group 1. Interface FastEthernet0/1 is the default port; this port will be used to send STP packets, for example. If this port fails, FastEthernet0/2 will be designated as the default port, and so forth. You can also see that this is an active Layer 2 EtherChannel by looking at the SU flag next to Po1. The following output shows the information printed by the `show EtherChannel detail` command:

https://t.me/learningnets

```
Switch-2#show EtherChannel detail
               Channel-group listing:
               ----------------------
Group: 1
----------
Group state = L2
Ports: 3   Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol:    -
               Ports in the group:
               -------------------
Port: Fa0/1
------------
Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = On/FEC           Gcchange = -
Port-channel  = Po1         GC   = -     Pseudo port-channel = Po1
Port index    = 0           Load = 0x00             Protocol = -
Age of the port in the current state: 0d:00h:20m:20s
Port: Fa0/2
------------
Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = On/FEC          Gcchange = -
Port-channel  = Po1         GC   = -    Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol = -
Age of the port in the current state: 0d:00h:21m:20s
Port: Fa0/3
------------
Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = On/FEC          Gcchange = -
Port-channel  = Po1         GC   = -    Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol = -
Age of the port in the current state: 0d:00h:21m:20s
               Port-channels in the group:
               ---------------------------
Port-channel: Po1
------------
Age of the Port-channel   = 0d:00h:26m:23s
Logical slot/port   = 1/0             Number of ports = 3
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
```

https://t.me/learningnets

```
Protocol            = -
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
0       00     Fa0/1    On/FEC          0
0       00     Fa0/2    On/FEC          0
0       00     Fa0/3    On/FEC          0
Time since last port bundled:    0d:00h:21m:20s    Fa0/3
```

In the output above, you can see that this is a Layer 2 EtherChannel with three out of a maximum of eight possible ports in the channel group. You can also see that the EtherChannel mode is on, based on the protocol being denoted by a dash (-). In addition, you can also see that this is a FastEtherChannel (FEC).

Finally, you can also verify the Layer 2 operational status of the logical port-channel interface by issuing the `show interfaces port-channel [number] switchport` command. This is illustrated in the following output:

```
Switch-2#show interfaces port-channel 1 switchport
Name: Po1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Protected: false
Appliance trust: none
```

Configuring and Verifying PAgP EtherChannels

This section describes the configuration of PAgP Layer 2 EtherChannels. The following steps

https://t.me/learninghets

need to be executed in order to configure and establish a PAgP EtherChannel.

1. The first configuration step is to enter Interface Configuration mode for the desired EtherChannel interface(s) via the `interface [name]` or `interface range [range]` global configuration command.
2. The second configuration step is to configure the interfaces as Layer 2 switch ports via the `switchport` interface configuration command.
3. The third configuration step is to configure the switch ports as either trunk or access links via the `switchport mode [access|trunk]` interface configuration command.
4. Optionally, if the interface or interfaces have been configured as access ports, assign them to the same VLAN using the `switchport access vlan [number]` command. If the interface or interfaces have been configured as a trunk port, select the VLANs allowed to traverse the trunk by issuing the `switchport trunk allowed vlan [range]` interface configuration command; if VLAN 1 will not be used as the native VLAN (for 802.1Q), enter the native VLAN by issuing the `switchport trunk native vlan [number]` interface configuration command. This configuration must be the same on all of the port channel member interfaces.
5. Optionally, configure PAgP as the EtherChannel protocol by issuing the `channel-protocol pagp` interface configuration command. Because EtherChannels default to PAgP, this command is considered optional and is not required. It is considered good practice to issue this command just to be absolutely sure of your configuration.
6. The next configuration step is to configure the interfaces to unconditionally trunk via the `channel-group [number] mode` interface configuration command.

The following output illustrates how to configure PAgP channelling on Switch 1 and Switch 2 based on the network topology depicted in Figure 33.5 above. The EtherChannel will be configured as a Layer 2 802.1Q trunk using default parameters:

```
Switch-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch-1(config)#interface range fa0/1 - 3
Switch-1(config-if-range)#switchport
Switch-1(config-if-range)#switchport trunk encap dot1q
Switch-1(config-if-range)#switchport mode trunk
Switch-1(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
Switch-1(config-if-range)#exit
```

NOTE: In the output above, the port channel desirable mode has been selected. An additional keyword, `[non-silent]`, may also be appended to the end of this command. This is because, by default, PAgP auto and desirable modes default to a silent mode. The silent mode is used when the switch is connected to a device that is not PAgP-capable and that seldom, if ever, transmits packets. An example of a silent partner is a file server or a packet analyser that is not generating traffic. It is also used if a device will not be sending PAgP packets (such as in auto mode).

In this case, running PAgP on a physical port connected to a silent partner prevents that switch

https://t.me/learningnets

port from ever becoming operational; however, the silent setting allows PAgP to operate, to attach the interface to a channel group, and to use the interface for transmission. In this example, because Switch 2 will be configured for auto mode (passive mode), it is preferred that the port uses the default silent mode operation. This is illustrated in the PAgP EtherChannel configuration output below:

```
Switch-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch-1(config)#interface range fa0/1 - 3
Switch-1(config-if-range)#switchport
Switch-1(config-if-range)#switchport trunk encap dot1q
Switch-1(config-if-range)#switchport mode trunk
Switch-1(config-if-range)#channel-group 1 mode desirable ?
  non-silent  Start negotiation only after data packets received
  <cr>
Switch-1(config-if-range)#channel-group 1 mode desirable non-silent
Creating a port-channel interface Port-channel 1
Switch-1(config-if-range)#exit
```

Proceeding with PAgP EtherChannel configuration, Switch 2 is configured as follows:

```
Switch-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch-2(config)#int range fa0/1 - 3
Switch-2(config-if-range)#switchport
Switch-2(config-if-range)#switchport trunk encapsulation dot1q
Switch-2(config-if-range)#switchport mode trunk
Switch-2(config-if-range)#channel-group 1 mode auto
Creating a port-channel interface Port-channel 1
Switch-2(config-if-range)#exit
```

The following output illustrates how to verify the PAgP EtherChannel configuration by using the `show EtherChannel summary` command on Switch 1 and Switch 2:

```
Switch-1#show EtherChannel summary
Flags:  D - down
        I - stand-alone
        H - Hot-standby (LACP only)
        R - Layer3
        u - unsuitable for bundling
        U - in use
        d - default port
        P - in port-channel
        s - suspended
        S - Layer2
```

https://t.me/learningnets

```
        f - failed to allocate aggregator
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------------
1      Po1(SU)         PAgP      Fa0/1(Pd)   Fa0/2(P)    Fa0/3(P)
```

PAgP EtherChannel configuration and statistics may also be viewed by issuing the `show pagp [options]` command. The options available with this command are illustrated in the following output:

```
Switch-1#show pagp ?
  <1-6>     Channel group number
  counters  Traffic information
  internal  Internal information
  neighbor  Neighbor information
```

NOTE: Entering the desired port channel number provides the same options as the last three options printed above. This is illustrated in the following output:

```
Switch-1#show pagp 1 ?
  counters  Traffic information
  internal  Internal information
  neighbor  Neighbor information
```

The `[counters]` keyword provides information on PAgP sent and received packets. The `[internal]` keyword provides information such as the port state, Hello interval, PAgP port priority, and the port learning method, for example. Using the `show pagp internal` command, this is illustrated in the following output:

```
Switch-1#show pagp 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        d - PAgP is down.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.
Channel group 1
                            Hello    Partner PAgP      Learning Group
Port    Flags State  Timers Interval Count Priority Method   Ifindex
Fa0/1   SC    U6/S7  H      30s      1     128      Any      29
Fa0/2   SC    U6/S7  H      30s      1     128      Any      29
Fa0/3   SC    U6/S7  H      30s      1     128      Any      29
```

The `[neighbor]` keyword prints out the neighbour name, ID of the PAgP neighbour, the neighbour device ID (MAC), and the neighbour port. The flags also indicate the mode the neighbour is operating in, as well as if it is a physical learner, for example. Using the `show pagp neighbor` command, this is illustrated in the following output:

https://t.me/learningnets

```
Switch-1#show pagp 1 neighbor
```

```
Flags:  S - Device is sending Slow hello. C - Device is in Consistent state.
        A - Device is in Auto mode.       P - Device learns on physical port.
Channel group 1 neighbors
          Partner     Partner          Partner        Partner Group
Port      Name        Device ID        Port      Age  Flags   Cap.
Fa0/1     Switch-2    0014.a9e5.d640   Fa0/1     19s  SAC     10001
Fa0/2     Switch-2    0014.a9e5.d640   Fa0/2     24s  SAC     10001
Fa0/3     Switch-2    0014.a9e5.d640   Fa0/3     18s  SAC     10001
```

Configuring and Verifying LACP EtherChannels

This section describes the configuration of LACP Layer 2 EtherChannels. The following steps need to be executed in order to configure and establish an LACP EtherChannel.

1. The first configuration step is to enter Interface Configuration mode for the desired EtherChannel interface(s) via the `interface [name]` or `interface range [range]` global configuration command.
2. The second configuration step is to configure the interfaces as Layer 2 switch ports via the `switchport` interface configuration command.
3. The third configuration step is to configure the switch ports as either trunk or access links via the `switchport mode [access|trunk]` interface configuration command.
4. Optionally, if the interface or interfaces have been configured as access ports, assign them to the same VLAN using the `switchport access vlan [number]` command. If the interface or interfaces have been configured as a trunk port, select the VLANs allowed to traverse the trunk by issuing the `switchport trunk allowed vlan [range]` interface configuration command; if VLAN 1 will not be used as the native VLAN (for 802.1Q), enter the native VLAN by issuing the `switchport trunk native vlan [number]` interface configuration command. This configuration must be the same on all of the port channel member interfaces.
5. Configure LACP as the EtherChannel protocol by issuing the `channel-protocol lacp` interface configuration command. Because EtherChannels default to PAgP, this command is considered mandatory for LACP and is required.
6. The next configuration step is to configure the interfaces to unconditionally trunk via the `channel-group [number] mode` interface configuration command.

In the above output illustrating how to configure LACP channelling on Switch 1 and Switch 2 based on the network topology depicted in Figure 33.5, the EtherChannel will be configured as a Layer 2 802.1Q trunk using default parameters, as shown in the following outputs:

```
Switch-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch-1(config)#int range FastEthernet0/1 - 3
Switch-1(config-if-range)#switchport
Switch-1(config-if-range)#switchport trunk encapsulation dot1q
```

https://t.me/learningnets

```
Switch-1(config-if-range)#switchport mode trunk
Switch-1(config-if-range)#channel-protocol lacp
Switch-1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
Switch-1(config-if-range)#exit
Switch-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch-2(config)#interface range FastEthernet0/1 - 3
Switch-2(config-if-range)#switchport
Switch-2(config-if-range)#switchport trunk encapsulation dot1q
Switch-2(config-if-range)#switchport mode trunk
Switch-2(config-if-range)#channel-protocol lacp
Switch-2(config-if-range)#channel-group 1 mode passive
Creating a port-channel interface Port-channel 1
Switch-2(config-if-range)#exit
```

The following output illustrates how to verify the LACP EtherChannel configuration by using the `show EtherChannel summary` command on Switch 1 and Switch 2:

```
Switch-1#show EtherChannel summary
Flags:  D - down
        I - stand-alone
        H - Hot-standby (LACP only)
        R - Layer3
        u - unsuitable for bundling
        U - in use
        d - default port
        P - in port-channel
        s - suspended
        S - Layer2
        f - failed to allocate aggregator
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+--------------------------------
1      Po1(SU)       LACP        Fa0/1(Pd)   Fa0/2(P)    Fa0/3(P)
```

By default, LACP allows up to 16 ports to be entered into a port channel group. The first eight operational interfaces will be used by LACP, while the remaining eight interfaces will be placed into the hot-standby state. The `show EtherChannel detail` command shows the maximum number of supported links in an LACP EtherChannel, as illustrated in the following output:

```
Switch-1#show EtherChannel 1 detail
Group state = L2
```

https://t.me/learningnets

Ports: 3   Maxports = 16

Port-channels: 1 Max Port-channels = 16

```
Protocol:   LACP
               Ports in the group:
               -------------------

Port: Fa0/1
------------
Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Active      Gcchange = -
Port-channel  = Po1         GC   = -       Pseudo port-channel = Po1
Port index    = 0           Load = 0x00        Protocol = LACP
Flags:  S - Device is sending Slow LACPDUs.  F - Device is sending fast
                                                LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                    LACP port     Admin     Oper    Port     Port
Port   Flags  State  Priority      Key       Key     Number   State
Fa0/1  SA     bndl   32768         0x1       0x1     0x0      0x3D
Partner's information:
          Partner               Partner                   Partner
Port      System ID             Port Number     Age       Flags
Fa0/1     00001,0014.a9e5.d640  0x1             4s        SP
          LACP Partner         Partner         Partner
          Port Priority        Oper Key        Port State
          32768                0x1             0x3C
Age of the port in the current state: 00d:00h:00m:35s
Port: Fa0/2
------------
Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Active      Gcchange = -
Port-channel  = Po1         GC   = -       Pseudo port-channel = Po1
Port index    = 0           Load = 0x00        Protocol = LACP
Flags:  S - Device is sending Slow LACPDUs.  F - Device is sending fast
                                                LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                    LACP port   Admin     Oper    Port     Port
Port    Flags  State  Priority    Key       Key     Number   State
Fa0/2   SA     bndl   32768       0x1       0x1     0x1      0x3D
Partner's information:
```

https://t.me/learningnets

```
          Partner               Partner                    Partner
Port      System ID             Port Number     Age        Flags
Fa0/2     00001,0014.a9e5.d640  0x2             28s        SP
          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          32768                 0x1             0x3C
Age of the port in the current state: 00d:00h:00m:33s
Port: Fa0/3
------------
Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Active      Gcchange = -
Port-channel  = Po1         GC   = -       Pseudo port-channel = Po1
Port index    = 0           Load = 0x00        Protocol = LACP
Flags:  S - Device is sending Slow LACPDUs.  F - Device is sending fast
                                               LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                    LACP port     Admin     Oper    Port     Port
Port   Flags  State  Priority      Key       Key     Number   State
Fa0/3  SA     bndl   32768         0x1       0x1     0x2      0x3D
Partner's information:
          Partner               Partner                    Partner
Port      System ID             Port Number     Age        Flags
Fa0/3     00001,0014.a9e5.d640  0x3             5s         SP
          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          32768                 0x1             0x3C
Age of the port in the current state: 00d:00h:00m:29s
               Port-channels in the group:
               ----------------------
Port-channel: Po1    (Primary Aggregator)
------------
Age of the Port-channel = 00d:00h:13m:50s
Logical slot/port   = 1/0          Number of ports = 3
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            = LACP
Ports in the Port-channel:
Index   Load   Port    EC state
```

---https://t.me/learningnets--------

```
0       00     Fa0/1   Active
0       00     Fa0/2   Active
0       00     Fa0/3   Active
Time since last port bundled:    00d:00h:00m:32s    Fa0/3
Time since last port Un-bundled: 00d:00h:00m:49s    Fa0/1
```

LACP configuration and statistics may also be viewed by issuing the `show lacp [options]` command. The options available with this command are illustrated in the following output:

```
Switch-1#show lacp ?
  <1-6>     Channel group number
  counters  Traffic information
  internal  Internal information
  neighbor  Neighbor information
  sys-id    LACP System ID
```

The `[counters]` keyword provides information on LACP sent and received packets. The output printed by this command is illustrated below:

```
Switch-1#show lacp counters
             LACPDUs         Marker      Marker Response    LACPDUs
Port        Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 1
Fa0/1       14     12       0      0        0      0         0
Fa0/2       21     18       0      0        0      0         0
Fa0/3       21     18       0      0        0      0         0
```

The `[internal]` keyword provides information such as the port state, administrative key, LACP port priority, and the port number, for example. This is illustrated in the following output:

```
Switch-1#show lacp internal
Flags:  S - Device is sending Slow LACPDUs. F - Device is sending Fast
                                              LACPDUs.
        A - Device is in Active mode.       P - Device is in Passive mode.
Channel group 1
                            LACP port    Admin    Oper   Port    Port
Port      Flags  State      Priority     Key      Key    Number  State
Fa0/1     SA     bndl       32768        0x1      0x1    0x0     0x3D
Fa0/2     SA     bndl       32768        0x1      0x1    0x1     0x3D
Fa0/3     SA     bndl       32768        0x1      0x1    0x2     0x3D
```

The `[neighbor]` keyword prints out the neighbour name, ID of the LACP neighbour, the neighbour device ID (MAC), and the neighbour port. The flags also indicate the mode the neighbour is operating in, as well as whether it is a physical learner, for example. This is illustrated in the following output:

https://t.me/learningnets

```
Switch-1#show lacp neighbor
Flags:  S - Device is sending Slow LACPDUs. F - Device is sending Fast
                                              LACPDUs.
        A - Device is in Active mode.       P - Device is in Passive mode.
Channel group 1 neighbors
Partner's information:
          Partner               Partner                   Partner
Port      System ID             Port Number     Age       Flags
Fa0/1     00001,0014.a9e5.d640  0x1             11s       SP
          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          32768                 0x1             0x3C
Partner's information:
          Partner               Partner                   Partner
Port      System ID             Port Number     Age       Flags
Fa0/2     00001,0014.a9e5.d640  0x2             19s       SP
          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          32768                 0x1             0x3C
Partner's information:
          Partner               Partner                   Partner
Port      System ID             Port Number     Age       Flags
Fa0/3     00001,0014.a9e5.d640  0x3             24s       SP
          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          32768                 0x1             0x3C
```

Finally, the `[sys-id]` keyword provides the system ID of the local switch. This is a combination of the switch MAC and LACP priority, as illustrated in the following output:

```
Switch-1#show lacp sys-id
1    ,000d.bd06.4100
```

https://t.me/learningnets

Day 33 Questions

1. What type of ports does a FastEtherChannel contain?
2. How many ports can a standard EtherChannel contain?
3. What are the two protocol options you have when configuring EtherChannels on a Cisco switch?
4. Which of the protocols mentioned above is Cisco proprietary?
5. PagP packets are sent to the destination Multicast MAC address 01-00-0C-CC-CC-CC. True or false?
6. What are the two port modes supported by PagP?
7. What are the two port modes supported by LACP?
8. If more than eight links are assigned to an EtherChannel bundle running LACP, the protocol uses the port priority to determine which ports are placed into a standby mode. True or false?
9. LACP automatically configures an administrative key value on each port configured to use LACP. The administrative key defines the ability of a port to aggregate with other ports. Only ports that have the same administrative key are allowed to be aggregated into the same port channel group. True or false?
10. What is the command used to assign a port to a channel group?

https://t.me/learningnets

Day 33 Answers

1. 100 Mbps ports.
2. Up to eight ports.
3. PagP and LACP.
4. PagP.
5. True.
6. Auto and desirable.
7. Active and passive.
8. True.
9. True.
10. The `channel-group [number] mode` command in Interface Configuration mode.

https://t.me/learningnets

Day 33 Lab

EtherChannel Lab

Test the configuration commands presented in this module on a simple topology that includes two directly connected switches (at least two links between them). Connect them via Fa1/1 and Fa2/2 (Fa1/1 to Fa1/1 and Fa2/2 to Fa2/2):

- ☐ Configure PagP on the two links in mode auto-desirable
- ☐ Configure the EtherChannel link as a trunk and allow a couple of VLANs through it
- ☐ Issue a `show etherchannel summary` command and verify that the port channel is up
- ☐ Issue a `show mac-address-table` command and see the learned MAC addresses on each switch
- ☐ Issue a `show papg neighbor` command and verify the results
- ☐ Repeat the steps above using LACP mode passive-active
- ☐ Verify the configuration using the `show EtherChannel detail` and `show lacp neighbor` commands
- ☐ Verify the configuration using the `show interface port-channel [number] switchport` command
- ☐ Issue some traffic (ping) across the port channel and verify the counters using the `show lacp counters` command
- ☐ Configure a different `lacp system-priority` output and verify it with the `show lacp sys-id` command
- ☐ Configure a different `lacp port-priority` output and verify it with the `show lacp internal` command
- ☐ Configure LACP load balancing using the `port-channel load-balance` command and verify this with the `show etherchannel load-balance` command

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 34 – First Hop Redundancy Protocols

Day 34 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's lab
- Read the ICND2 cram guide
- Spend 15 minutes on the subnetting.org website

High Availability (HA) is an integral component when designing and implementing switched networks. HA is technology delivered in Cisco IOS software that enables networkwide resilience to increase IP network availability. All network segments must be resilient to recover quickly enough for faults to be transparent to users and network applications. First Hop Redundancy Protocols (FHRPs) provide redundancy in switched LAN environments.

Today you will learn about the following:

- Hot Standby Router Protocol
- Virtual Router Redundancy Protocol
- Gateway Load Balancing Protocol

This lesson maps to the following ICND2 syllabus requirements:

- Recognise High Availability (FHRP)
  - HSRP
  - VRRP
  - GLBP

Hot Standby Router Protocol

Hot Standby Router Protocol (HSRP) is a Cisco-proprietary First Hop Redundancy Protocol (FHRP). HSRP allows two physical gateways that are configured as part of the same HSRP group to share the same virtual gateway address. Network hosts residing on the same subnet as the gateways are configured with the virtual gateway IP address as their default gateway.

While operational, the primary gateway forwards packets destined to the virtual gateway IP address of the HSRP group. In the event that the primary gateway fails, the secondary gateway assumes the role of primary gateway and forwards all packets sent to the virtual gateway IP address. Figure 34.1 below illustrates the operation of HSRP in a network:

https://t.me/learningnets

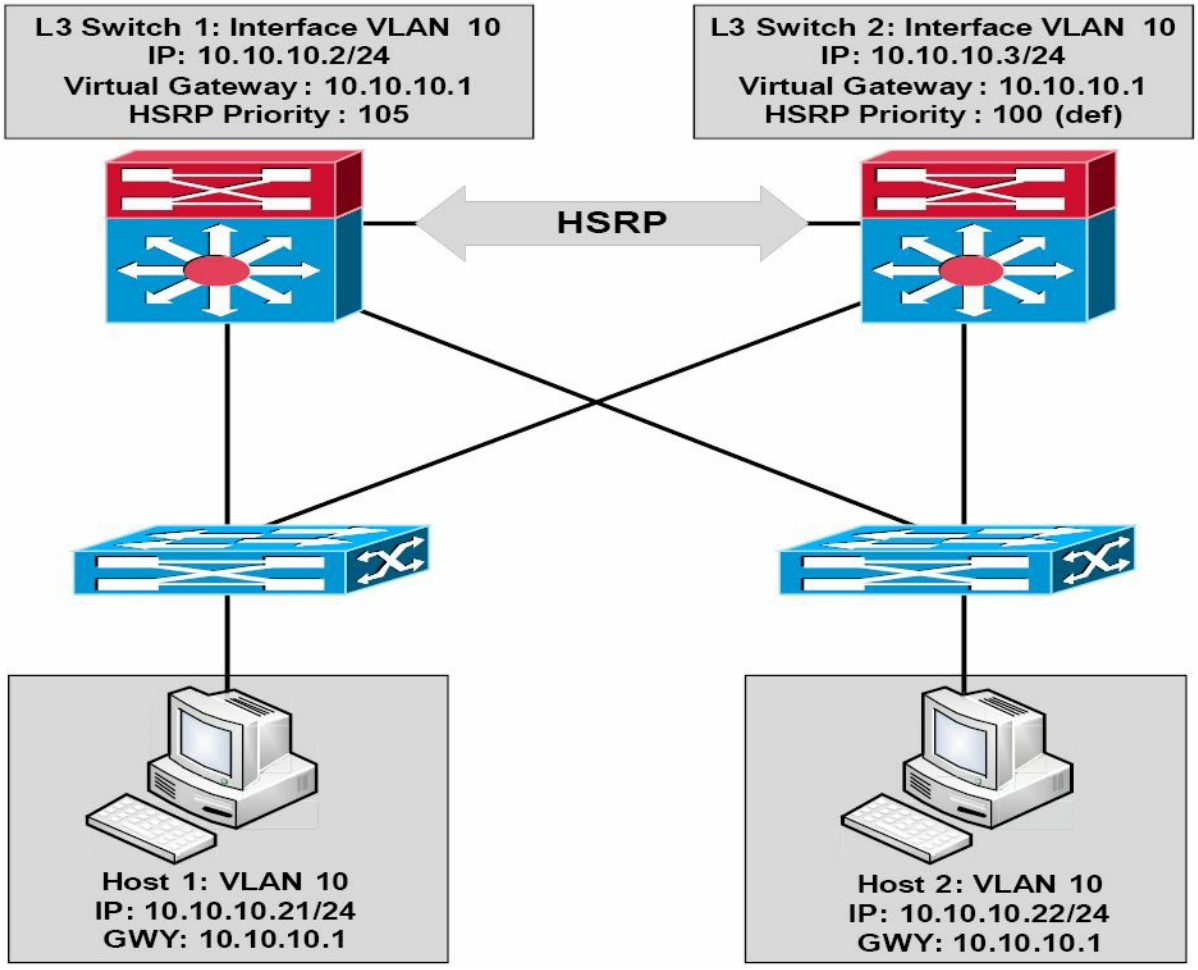


Figure 34.1 – Hot Standby Router Protocol (HSRP) Operation

Referencing Figure 34.1, HSRP is configured between the Layer 3 (Distribution Layer) switches, providing gateway redundancy for VLAN 10. The IP address assigned to the Switch Virtual Interface (SVI) on Layer 3 Switch 1 is 10.10.10.2/24, and the IP address assigned to the SVI on Layer 3 Switch 2 is 10.10.10.3/24. Both switches are configured as part of the same HSRP group and share the IP address of the virtual gateway, which is 10.10.10.1.

Switch 1 has been configured with a priority of 105, while Switch 2 is using the default priority of 100. Because of the higher priority, Layer 3 Switch 1 is elected as the primary switch and Layer 3 Switch 2 is elected as the secondary switch. All hosts on VLAN 10 are configured with a default gateway address of 10.10.10.1. Based on this solution, Switch 1 will forward all packets sent to the 10.10.10.1 address. However, in the event that Switch 1 fails, then Switch 2 will assume this responsibility. This process is entirely transparent to the network hosts.



Real-World Implementation

In production networks, when configuring FHRPs, it is considered good practice to ensure that the active (primary) gateway is also the Spanning Tree Root Bridge for the particular VLAN. Referencing the diagram in Figure 34.1, for example, Switch 1 would be configured as the Root Bridge for VLAN 10 in tandem with being the HSRP primary gateway for the same VLAN.

https://t.me/learningnets

This results in a deterministic network and avoids suboptimal forwarding at Layer 2 or Layer 3. For example, if Switch 2 was the Root Bridge for VLAN 10, while Switch 1 was the primary gateway for VLAN 10, packets from the network hosts to the default gateway IP address would be forwarded as shown in Figure 34.2 below:

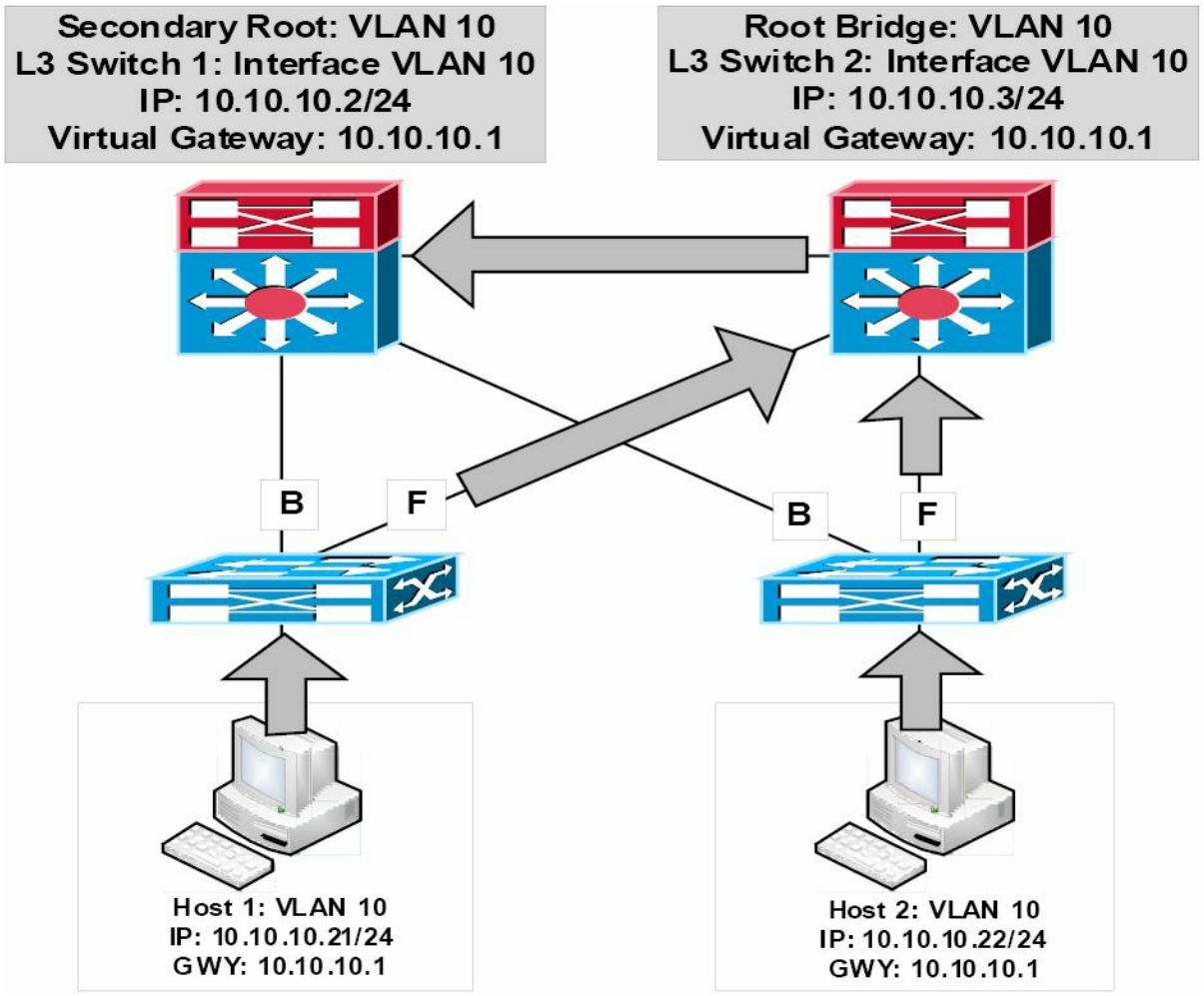


Figure 34.2 – Synchronising the STP Topology with HSRP

In the network above, packets from Host 1 to 10.10.10.1 are forwarded as follows:

1. The Access Layer switch receives a frame destined to the MAC address of the virtual gateway IP address from Host 1. This frame is received in VLAN 10 and the MAC address for the virtual gateway has been learned by the switch via its Root Port.
2. Because the Root Bridge for VLAN 10 is Switch 2, the uplink towards Switch 1 (the HSRP primary router) is placed into a Blocking state. The Access Layer switch forwards the frame via the uplink to Switch 2.
3. Switch 2 forwards the frame via the Designated Port connected to Switch 1. The same suboptimal forwarding path is used for frames received from Host 2.

Currently, two versions of HSRP are supported in Cisco IOS software: versions 1 and 2. The similarities and differences between the versions will be described in the sections that follow.

HSRP Version 1

By default, when Hot Standby Router Protocol is enabled in Cisco IOS software, version 1 is enabled. HSRP version 1 restricts the number of configurable HSRP groups to 255. HSRP version

https://t.me/learningnets

1 routers communicate by sending messages to Multicast group address 224.0.0.2 using UDP port 1985. This is shown in Figure 34.3 below:

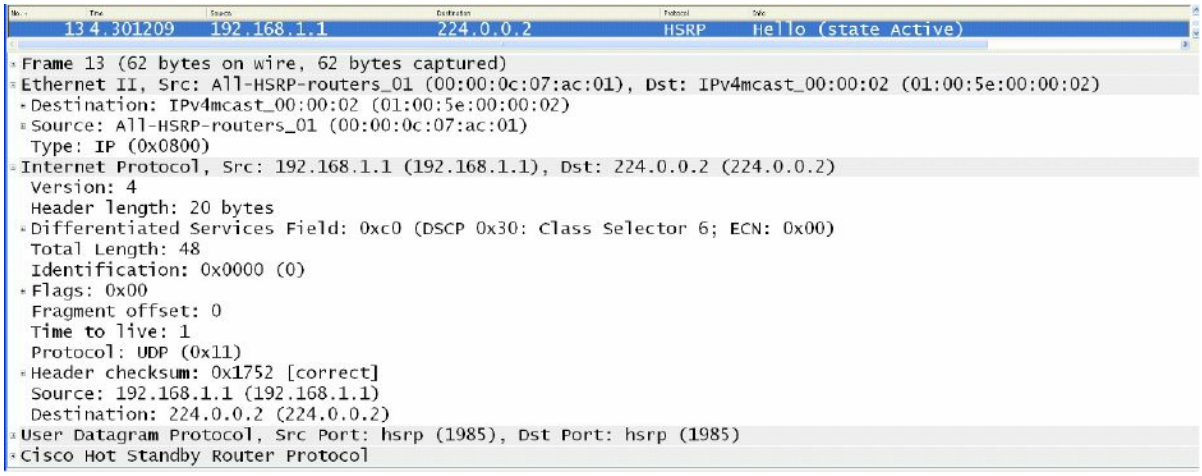


Figure 34.3 – HSRP Version 1 Multicast Group Address

While going into detail on the HSRP packet format is beyond the scope of the CCNA exam requirements, Figure 34.4 below illustrates the information contained in the HSRP version 1 packet:

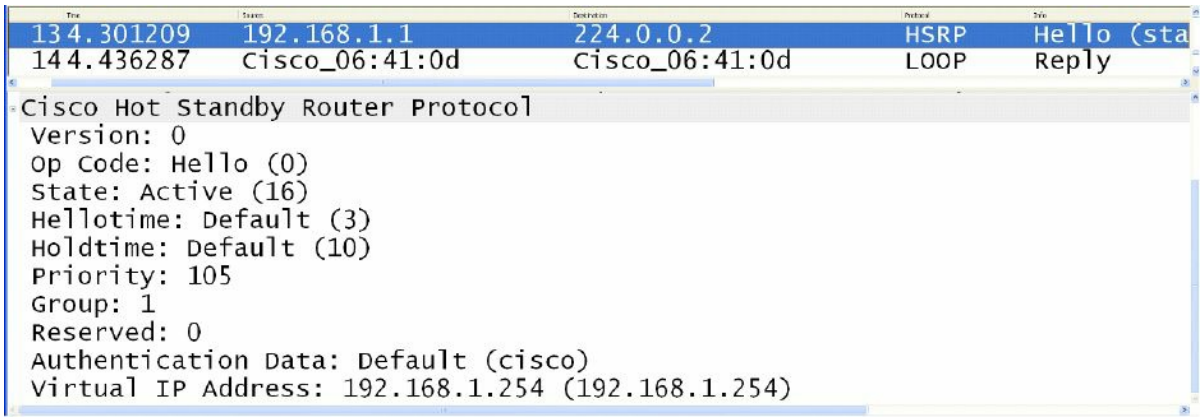


Figure 34.4 – The HSRP Version 1 Packet Fields

In Figure 34.4, notice that the Version field shows a value of 0. This is the default value for this field when version 1 is enabled; however, remember that this implies HSRP version 1.

HSRP Version 2

HSRP version 2 uses the new Multicast address 224.0.0.102 to send Hello packets instead of the Multicast address of 224.0.0.2, which is used by version 1. The UDP port number, however, remains the same. This new address is also encoded in both the IP packet and the Ethernet frame, as shown below in Figure 34.5:

https://t.me/learningnets

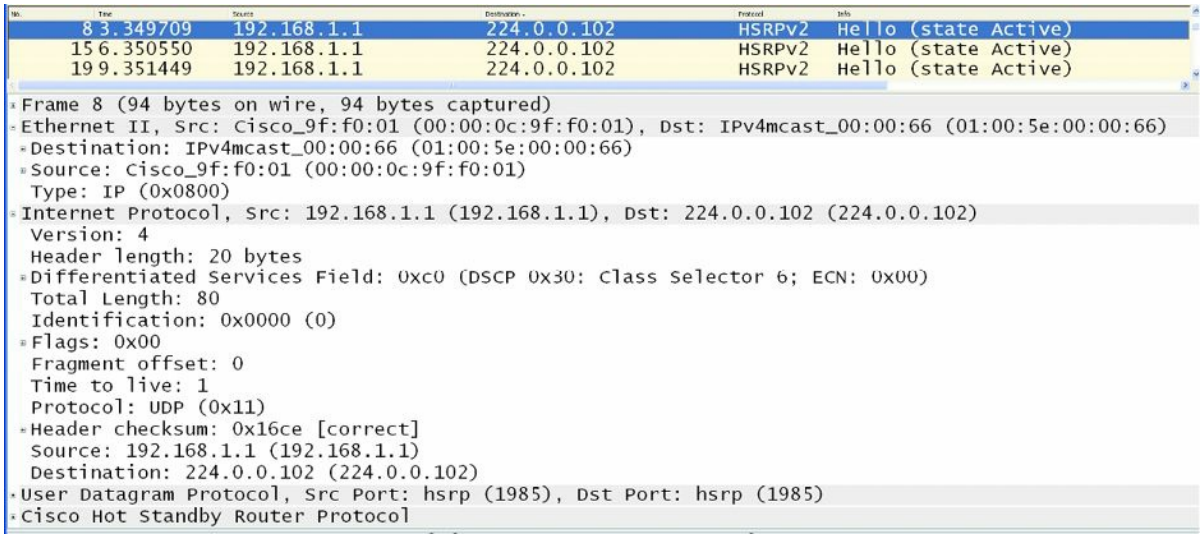


Figure 34.5 – HSRP Version 2 Multicast Group Address

While going into detail on the HSRP version 2 packet format is beyond the scope of the CCNA exam requirements, it is important to remember that HSRP version 2 does not use the same packet format as HSRP version 1.

The version 2 packet format uses a Type/Length/Value (TLV) format. HSRP version 2 packets received by an HSRP version 1 router will have the Type field mapped to the Version field by HSRP version 1 and will be subsequently ignored. Figure 34.6 illustrates the information contained in the HSRP version 2 packet:

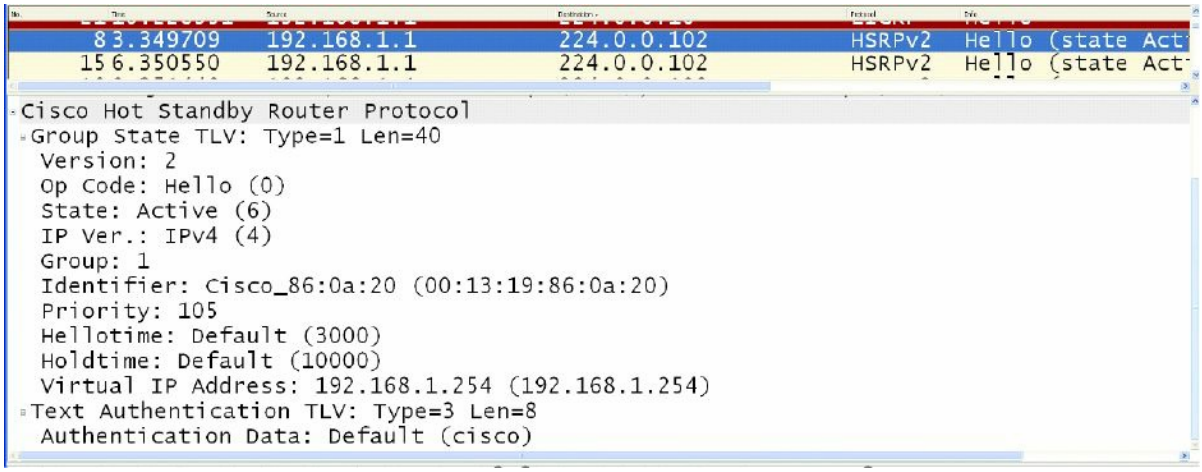


Figure 34.6 – The HSRP Version 2 Packet Fields

HSRP Version 1 and Version 2 Comparison

HSRP version 2 includes enhancements to HSRP version 1. The version 2 enhancements and differences from version 1 will be described in this section.

Although HSRP version 1 advertises timer values, these values are always to the whole second, as it is not capable of advertising or learning millisecond timer values. Version 2 is capable of both advertising and learning millisecond timer values. Figures 34.7 and 34.8 below highlight the differences between the Timer fields for both HSRP version 1 and HSRP version 2, respectively:

https://t.me/learningnets

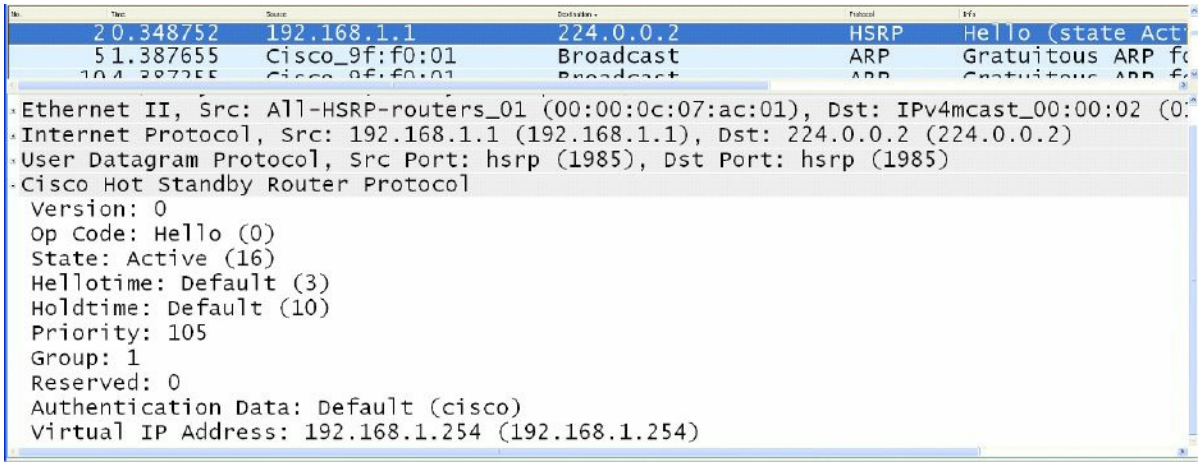


Figure 34.7 – HSRP Version 1 Timer Fields

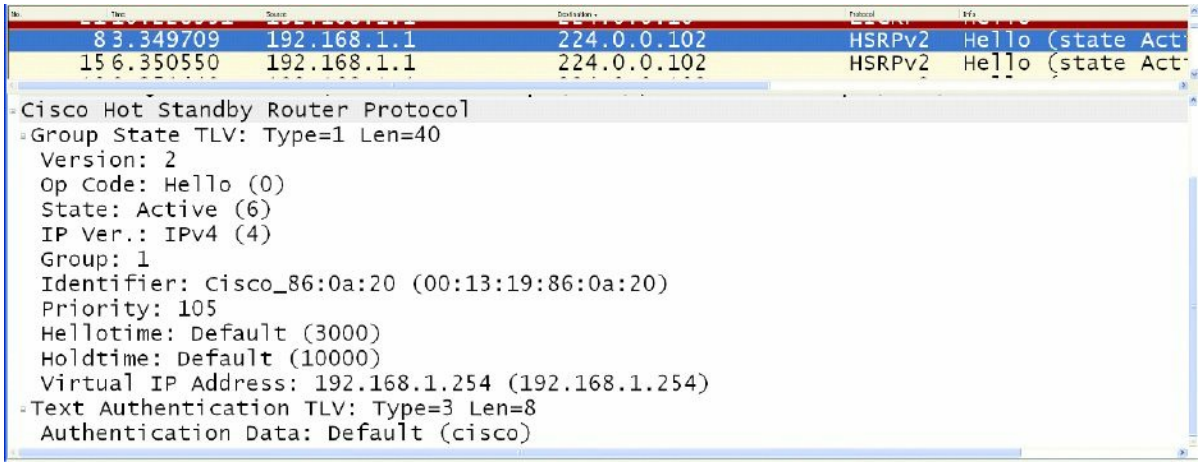
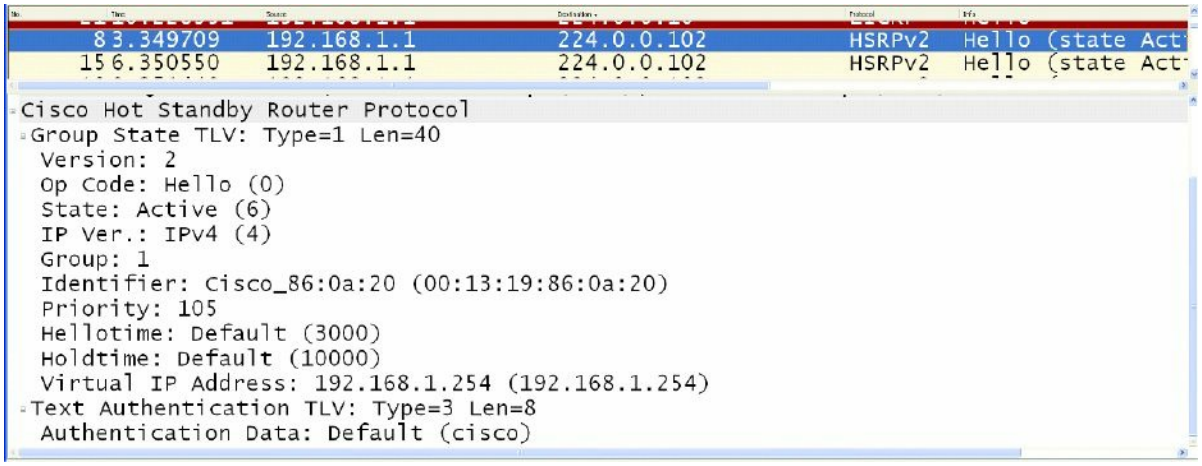


Figure 34.8 – HSRP Version 2 Timer Fields

HSRP version 1 group numbers are restricted to the range of 0 to 255, whereas the version 2 group numbers have been extended from 0 to 4095. This difference will be illustrated in the HSRP configuration examples that will be provided later in this module.

Version 2 provides improved management and troubleshooting by including a 6-byte Identifier field that is populated with the physical router interface MAC address and is used to uniquely identify the source of HSRP active Hello messages. In version 1, these messages contain the virtual MAC address as the source MAC, which means it is not possible to determine which HSRP router actually sent the HSRP Hello message. Figure 34.9 below shows the Identifier field that is present in the version 2 packet but not in the HSRP version 1 packet:



https://t.me/learningnets**Figure 34.9 – HSRP Version 2 Identifier Field**

In HSRP version 1, the Layer 2 address that is used by the virtual IP address will be a virtual MAC address composed of 0000.0C07.AC*xx*, where "*xx*" is the HSRP group number in hexadecimal value and is based on the respective interface. HSRP version 2, however, uses a new MAC address range of 0000.0C9F.F000 to 0000.0C9F.FFFF for the virtual gateway IP address. These differences are illustrated below in Figure 34.10, which shows the version 1 virtual MAC address for HSRP Group 1, as well as in Figure 34.11, which shows the version 2 virtual MAC address, also for HSRP Group 1:

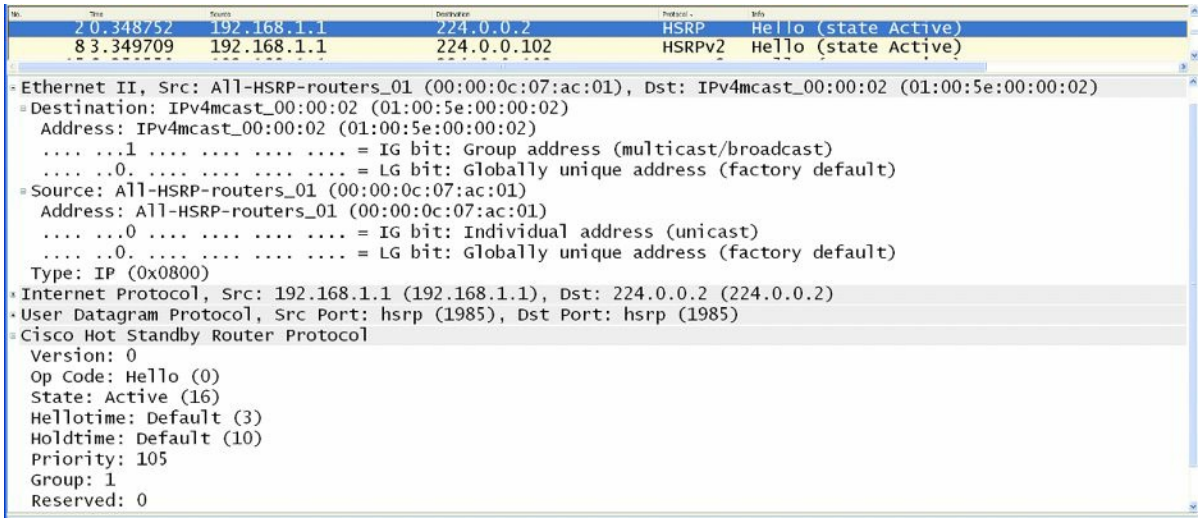


Figure 34.10 – HSRP Version 1 Virtual MAC Address Format

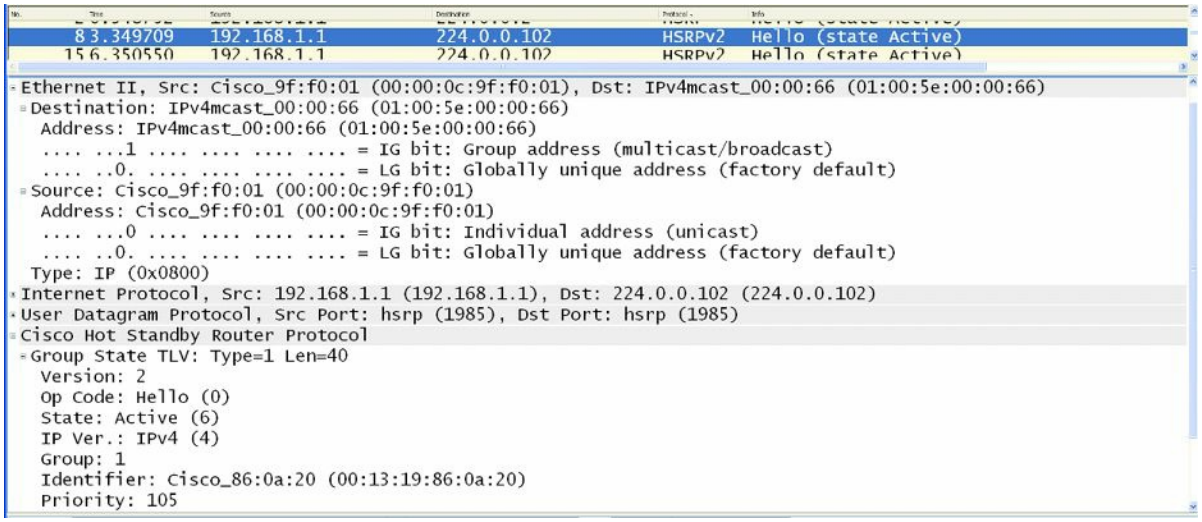


Figure 34.11 – HSRP Version 2 Virtual MAC Address Format

HSRP Primary Gateway Election

HSRP primary gateway election can be influenced by adjusting the default HSRP priority of 100 to any value between 1 and 255. The router with the highest priority will be elected as the primary gateway for the HSRP group.

If two gateways are using the default priority values, or if the priority values on two gateways are manually configured as equal, the router with the highest IP address will be elected as the primary gateway. The HSRP priority value is carried in the HSRP frame, as is the current state of the router (e.g., primary or standby). Figure 34.12 below illustrates the Priority and State fields of a gateway configured with a non-default priority value of 105, which resulted in it being elected as the active gateway for the HSRP group:

https://t.me/learningnets

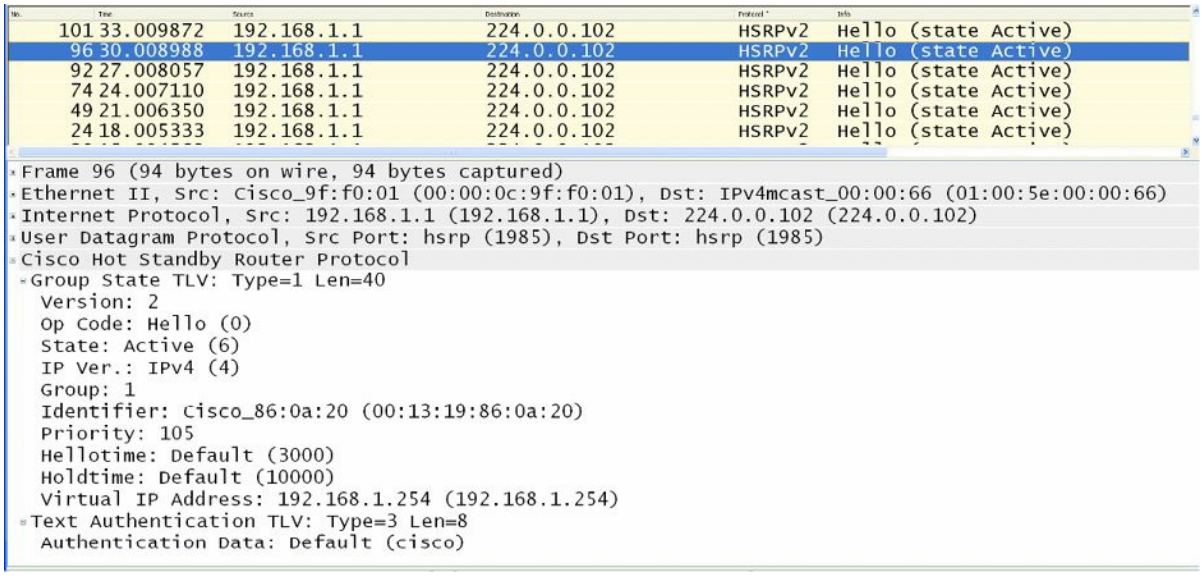


Figure 34.12 – HSRP Priority and State Fields

HSRP Messages

HSRP routers exchange the following three types of messages:

- Hello messages
- Coup messages
- Resign messages

Hello messages are exchanged via Multicast and they tell the other gateway the HSRP state and priority values of the local router. Hello messages also include the Group ID, HSRP timer values, version, and authentication information. All of the messages shown in the previous screenshots are HSRP Hello messages.

HSRP Coup messages are sent when the current standby router wants to assume the role of active gateway for the HSRP group. This is similar to a coup d'état in real life.

HSRP Resign messages are sent by the active router when it is about to shut down or when a gateway that has a higher priority sends a Hello or Coup message. In other words, this message is sent when the active gateway concedes its role as primary gateway.

HSRP Preemption

If a gateway has been elected as the active gateway and another gateway that is part of the HSRP group is reconfigured with a higher priority value, the current active gateway retains the primary forwarding role. This is the default behaviour of HSRP.

In order for a gateway with a higher priority to assume active gateway functionality when a primary gateway is already present for an HSRP group, the router must be configured for preemption. This allows the gateway to initiate a coup and assume the role of the active gateway for the HSRP group. HSRP preemption is illustrated in the configuration examples to follow.

NOTE: Preemption does not necessarily mean that the Spanning Tree topology changes also.

https://t.me/learningnets

HSRP States

In a manner similar to Open Shortest Path First (OSPF), when HSRP is enabled on an interface, the gateway interface goes through the following series of states:

1. Disabled
2. Init
3. Listen
4. Speak
5. Standby
6. Active

NOTE: There are no set time values for these interface transitions.

In either the Disabled or the Init states, the gateway is not yet ready or is unable to participate in HSRP, possibly because the associated interface is not up.

The Listen state is applicable to the standby gateway. Only the standby gateway monitors Hello messages from the active gateway. If the standby gateway does not receive Hellos within 10 seconds, it assumes that the active gateway is down and takes on this role itself. If other gateways exist on the same segment, they also listen to Hellos and will be elected as the group active gateway if they have the next highest priority value or IP address.

During the Speak phase, the standby gateway exchanges messages with the active gateway. Upon completion of this phase, the primary gateway transitions to the Active state and the backup gateway transitions to the Standby state. The Standby state indicates that the gateway is ready to assume the role of active gateway if the primary gateway fails, and the Active state indicates that the gateway is ready to actively forward packets.

The following output shows the state transitions displayed in the `debug standby` command on a gateway for which HSRP has just been enabled:

```
R2#debug standby
HSRP debugging is on
R2#
R2#conf t
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#logging con
R2(config)#int f0/0
R2(config-if)#stand 1 ip 192.168.1.254
R2(config-if)#
*Mar  1 01:21:55.471: HSRP: Fa0/0 API 192.168.1.254 is not an HSRP address
*Mar  1 01:21:55.471: HSRP: Fa0/0 Grp 1 Disabled -> Init
*Mar  1 01:21:55.471: HSRP: Fa0/0 Grp 1 Redundancy "hsrp-Fa0/0-1" state Disabled -> Init
```

https://t.me/learningnets

```
*Mar  1 01:22:05.475: HSRP: Fa0/0 Interface up
...
[Truncated Output]
...
*Mar  1 01:22:06.477: HSRP: Fa0/0 Interface min delay expired
*Mar  1 01:22:06.477: HSRP: Fa0/0 Grp 1 Init: a/HSRP enabled
*Mar  1 01:22:06.477: HSRP: Fa0/0 Grp 1 Init -> Listen
*Mar  1 01:22:06.477: HSRP: Fa0/0 Redirect adv out, Passive, active 0 passive 1
...
[Truncated Output]
...
*Mar  1 01:22:16.477: HSRP: Fa0/0 Grp 1 Listen: d/Standby timer expired (unknown)
*Mar  1 01:22:16.477: HSRP: Fa0/0 Grp 1 Listen -> Speak
...
[Truncated Output]
...
*Mar  1 01:22:26.478: HSRP: Fa0/0 Grp 1 Standby router is local
*Mar  1 01:22:26.478: HSRP: Fa0/0 Grp 1 Speak -> Standby
*Mar  1 01:22:26.478: %HSRP-5-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby
*Mar  1 01:22:26.478: HSRP: Fa0/0 Grp 1 Redundancy "hsrp-Fa0/0-1" state Speak -> Standby
```

HSRP Addressing

Earlier in this module, you learned that in HSRP version 1, the Layer 2 address that is used by the virtual IP address will be a virtual MAC address composed of 0000.0C07.AC*xx*, where "*xx*" is the HSRP group number in hexadecimal value and is based on the respective interface. HSRP version 2, however, uses a new MAC address range of 0000.0C9F.F000 to 0000.0C9F.FFFF for the virtual gateway IP address.

In some cases, it may not be desirable to use these default address ranges. An example would be a situation where several HSRP groups were configured on a router interface connected to a switch port that was configured for port security. In such a case, the router would use a different MAC address for each HSRP group, the result being multiple MAC addresses that would all need to be accommodated in the port security configuration. This configuration would have to be modified each time an HSRP group was added to the interface; otherwise, a port security violation would occur.

To address this issue, Cisco IOS software allows administrators to configure HSRP to use the actual MAC address of the physical interface on which it is configured. The result is that a single MAC address is used by all groups (i.e., the MAC address of the active gateway is used) and the port security configuration need not be modified each time an HSRP group is configured between the routers connected to the switches. This is performed via the `standby use-bia` interface configuration command. The following output illustrates the `show standby` command, which shows a gateway interface that is configured with two different HSRP groups:

https://t.me/learningnets

```
Gateway-1#show standby
FastEthernet0/0 - Group 1
  State is Active
    8 state changes, last state change 00:13:07
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.002 secs
  Preemption disabled
  Active router is local
  Standby router is 192.168.1.2, priority 100 (expires in 9.019 sec)
  Priority 105 (configured 105)
  IP redundancy name is "hsrp-Fa0/0-1" (default)
FastEthernet0/0 - Group 2
  State is Active
    2 state changes, last state change 00:09:45
  Virtual IP address is 172.16.1.254
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.423 secs
  Preemption disabled
  Active router is local
```

In the output above, based on the default HSRP version, the virtual MAC address for HSRP Group 1 is 0000.0c07.ac01, while that for HSRP Group 2 is 0000.0c07.ac02. This means that the switch port that this gateway is connected to learns three different addresses: the actual or burnt-in MAC address assigned to the actual physical FastEthernet0/0 interface, the virtual MAC address for HSRP Group 1, and the virtual MAC address for HSRP Group 2.

The following output illustrates how to configure HSRP to use the actual MAC address of the gateway interface as the virtual MAC address of the different HSRP groups:

```
Gateway-1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Gateway-1(config)#int f0/0
Gateway-1(config-if)#standby use-bia
Gateway-1(config-if)#exit
```

Based on the configuration in the output above, the `show standby` command reflects the new MAC address for the HSRP group, as illustrated in the following output:

https://t.me/learningnets

```
Gateway-1#show standby
FastEthernet0/0 - Group 1
  State is Active
    8 state changes, last state change 00:13:30
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0013.1986.0a20
    Local virtual MAC address is 0013.1986.0a20 (bia)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.756 secs
  Preemption disabled
  Active router is local
  Standby router is 192.168.1.2, priority 100 (expires in 9.796 sec)
  Priority 105 (configured 105)
  IP redundancy name is "hsrp-Fa0/0-1" (default)
FastEthernet0/0 - Group 2
  State is Active
    2 state changes, last state change 00:10:09
  Virtual IP address is 172.16.1.254
  Active virtual MAC address is 0013.1986.0a20
    Local virtual MAC address is 0013.1986.0a20 (bia)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.188 secs
  Preemption disabled
  Active router is local
  Standby router is unknown
  Priority 105 (configured 105)
  IP redundancy name is "hsrp-Fa0/0-2" (default)
```

The MAC address used by both groups, 0013.1986.0a20, is the MAC address assigned to the physical gateway interface. This is illustrated in the following output:

```
Gateway-1#show interface FastEthernet0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0013.1986.0a20 (bia 0013.1986.0a20)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
...
[Truncated Output]
```

NOTE: In addition to configuring HSRP to use the burnt-in address (BIA), administrators also have the option of statically specifying the MAC address that the virtual gateway should use via the `standby [number] mac-address [mac]` interface

https://t.me/learningnets

configuration command. This option is typically avoided, as it can result in duplicate MAC addresses in the switched network, which can cause severe network issues and possibly even an outage.

HSRP Plain Text Authentication

By default, HSRP messages are sent with the plain text key string “cisco” as a simple method to authenticate HSRP peers. If the key string in a message matches the key configured on an HSRP peer, the message is accepted. If not, HSRP ignores the unauthenticated message(s).

Plain text keys provide very little security because they can be “captured on the wire” using simple packet capture tools, such as Wireshark and Ethereal. Figure 34.13 below shows the default plain text authentication key used in HSRP messages:

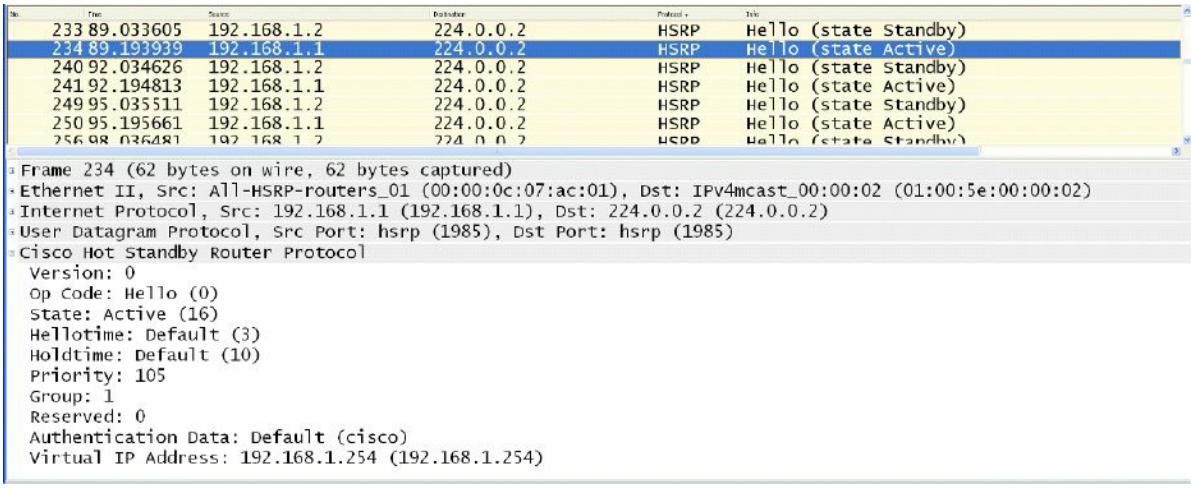


Figure 34.13 – Viewing the Default HSRP Plain Text Key

Because plain text authentication provides very little security, Message Digest 5 (MD5) authentication, which is described in the following section, is the recommended authentication method for HSRP.

HSRP MD5 Authentication

This isn’t a CCNA subject but it’s included here for completeness and for those of you who will be applying these lessons in your job on a live network.

Message Digest 5 authentication provides greater security for HSRP than that provided by plain text authentication by generating an MD5 digest for the HSRP portion of the Multicast HSRP protocol packet. Using MD5 authentication allows each HSRP group member to use a secret key to generate a keyed MD5 hash that is part of the outgoing packet. A keyed hash of the incoming HSRP packet is generated and if the hash within the incoming packet does not match the MD5-generated hash, the packet is simply ignored by the receiving router.

The key for the MD5 hash can be either given directly in the configuration using a key string or supplied indirectly through a key chain. Both configuration options will be described in detail later in this module. When using plain-text or MD5 authentication, the gateway will reject HSRP packets if any of the following is true:

- ☐ The authentication schemes differ on the router and in the incoming packets
- ☐ The MD5 digests differ on the router and in the incoming packets

https://t.me/learningnets

- The text authentication strings differ on the router and in the incoming packets

HSRP Interface Tracking

HSRP allows administrators to track the status of interfaces on the current active gateway so that when that interface fails, the gateway decrements its priority by a specified value, the default being 10, allowing another gateway to assume the role of active gateway for the HSRP group. This concept is illustrated below in Figure 34.14:

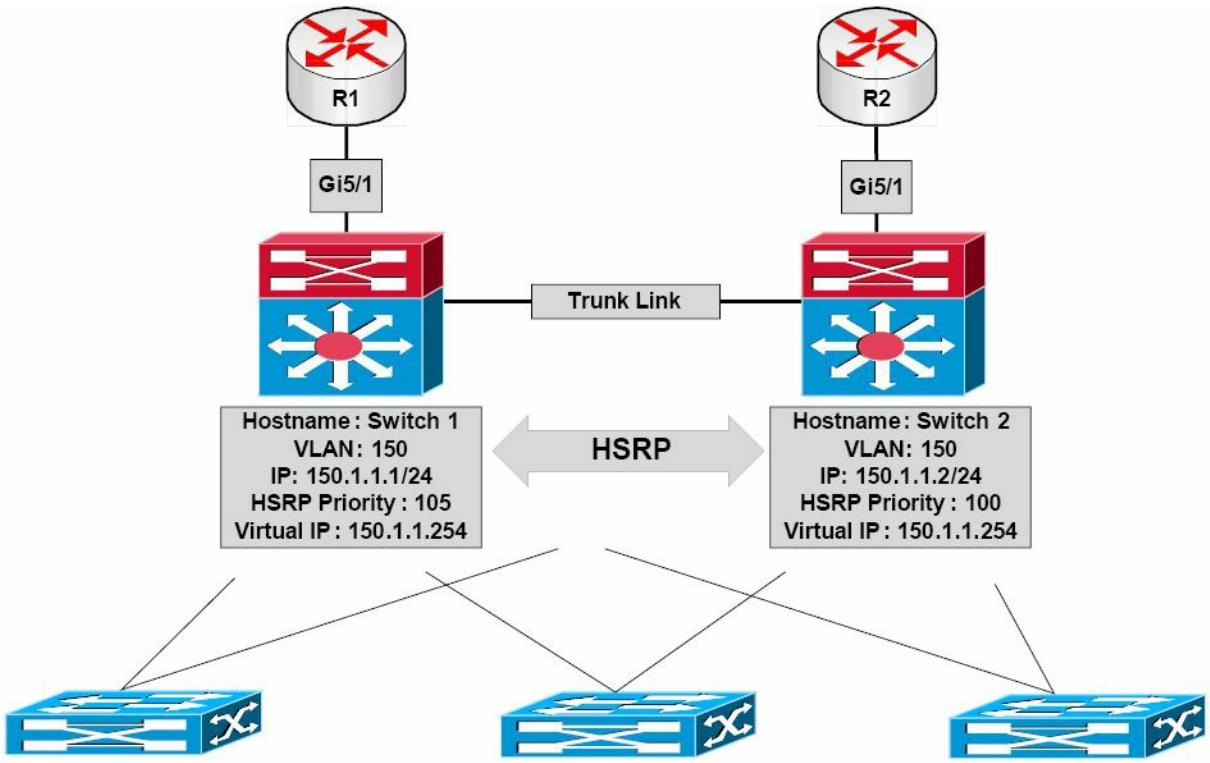


Figure 34.14 – HSRP Interface Tracking

Referencing Figure 34.14, HSRP has been enabled on Switch 1 and Switch 2 for VLAN 150. Based on the current priority configuration, Switch 1, with a priority value of 105, has been elected as the primary switch for this VLAN. Both Switch 1 and Switch 2 are connected to two routers via their GigabitEthernet5/1 interfaces. It is assumed that these two routers peer with other external networks, such as the Internet.

Without HSRP interface tracking, if the GigabitEthernet5/1 interface between Switch 1 and R1 failed, Switch 1 would retain its primary gateway status. It would then have to forward any received packets destined for the Internet, for example, over to Switch 2 using the connection between itself and Switch 2. The packets would be forwarded out via R2 towards their intended destination. This results in a suboptimal traffic path within the network.

HSRP interface tracking allows the administrators to configure HSRP to track the status of an interface and decrement the active gateway priority by either a default value of 10 or a value specified by the administrators. Referencing Figure 34.14, if HSRP interface tracking was configured using the default values on Switch 1, allowing it to track the status of interface GigabitEthernet5/1, and that interface failed, Switch 1 would decrement its priority for the HSRP group by 10, resulting in a priority of 95.

Assuming that Switch 2 was configured to preempt, which is mandatory in this situation, it

https://t.me/learningnets

would realise that it had the higher priority (100 versus 95) and perform a coup, assuming the role of active gateway for this HSRP group.



Real-World Implementation

In production networks, Cisco Catalyst switches also support Enhanced Object Tracking (EOT), which can be used with any FHRP (i.e., HSRP, VRRP, and GLBP). Enhanced Object Tracking allows administrators to configure the switch to track the following parameters:

- The IP routing state of an interface
- IP route reachability
- The threshold of IP route metrics
- IP SLA operations

FHRPs, such as HSRP, can be configured to track these enhanced objects, allowing for greater flexibility when implementing FHRP failover situations. For example, using EOT, the active HSRP router could be configured to decrement its priority value by a certain amount if a network or host route was not reachable (i.e., present in the routing table). EOT is beyond the scope of the CCNA exam requirements and will not be illustrated in the configuration examples.

HSRP Load Balancing

HSRP allows administrators to configure multiple HSRP groups on physical interfaces to allow for load balancing. By default, when HSRP is configured between two gateways, only one gateway actively forwards traffic for that group at any given time. This can result in wasted bandwidth for the standby gateway link. This is illustrated below in Figure 34.15:

https://t.me/learningnets

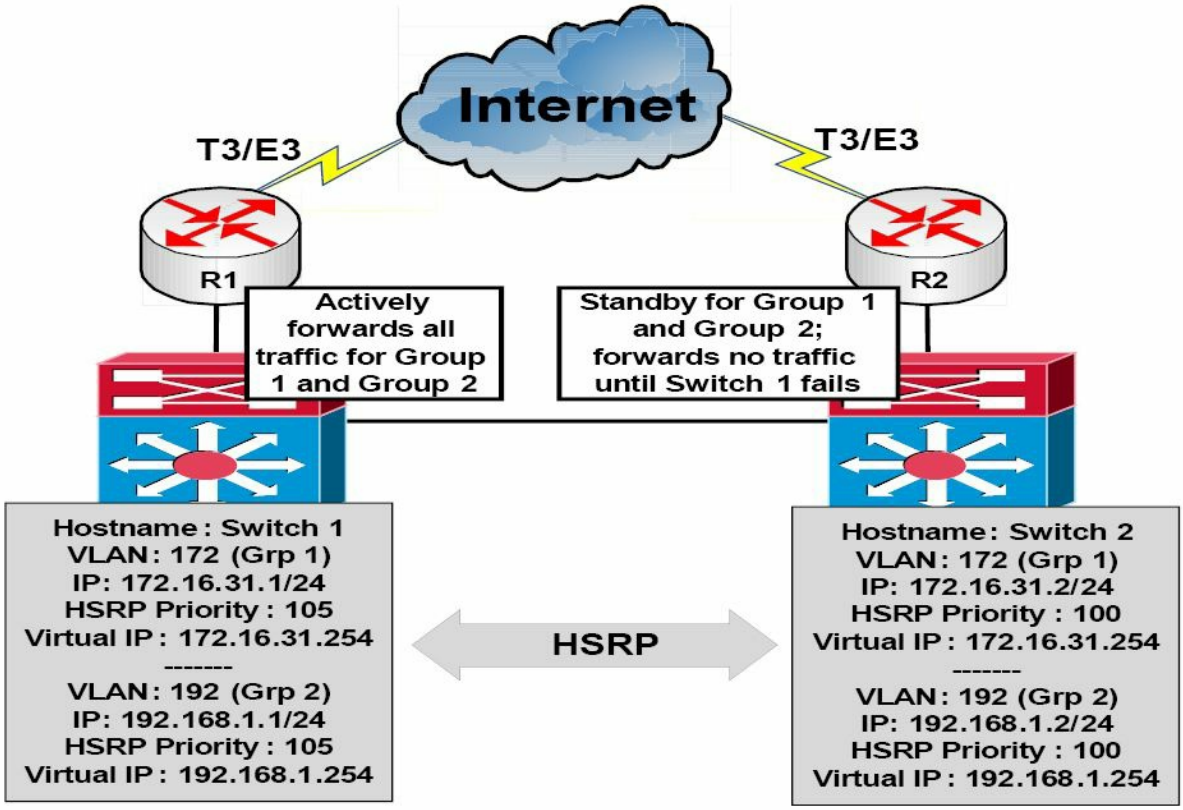


Figure 34.15 – A Network without HSRP Load Balancing

In Figure 34.15, two HSRP groups are configured between Switch 1 and Switch 2. Switch 1 has been configured as the active (primary) gateway for both groups – based on the higher priority value. Switch 1 and Switch 2 are connected to R1 and R2, respectively. These routers are both connected to the Internet via T3/E3 dedicated lines. Because Switch 1 is the active gateway for both groups, it will forward traffic for both groups until it fails and Switch 2 will then assume the role of active (primary) gateway.

While this does satisfy the redundancy needs of the network, it also results in the expensive T3/E3 link on R2 remaining idle until Switch 2 becomes the active gateway and begins to forward traffic through it. Naturally, this represents a wasted amount of bandwidth.

By configuring multiple HSRP groups, each using a different active gateway, administrators can effectively prevent the unnecessary waste of resources and load balance between Switch 1 and Switch 2. This is illustrated below in Figure 34.16:

https://t.me/learningnets

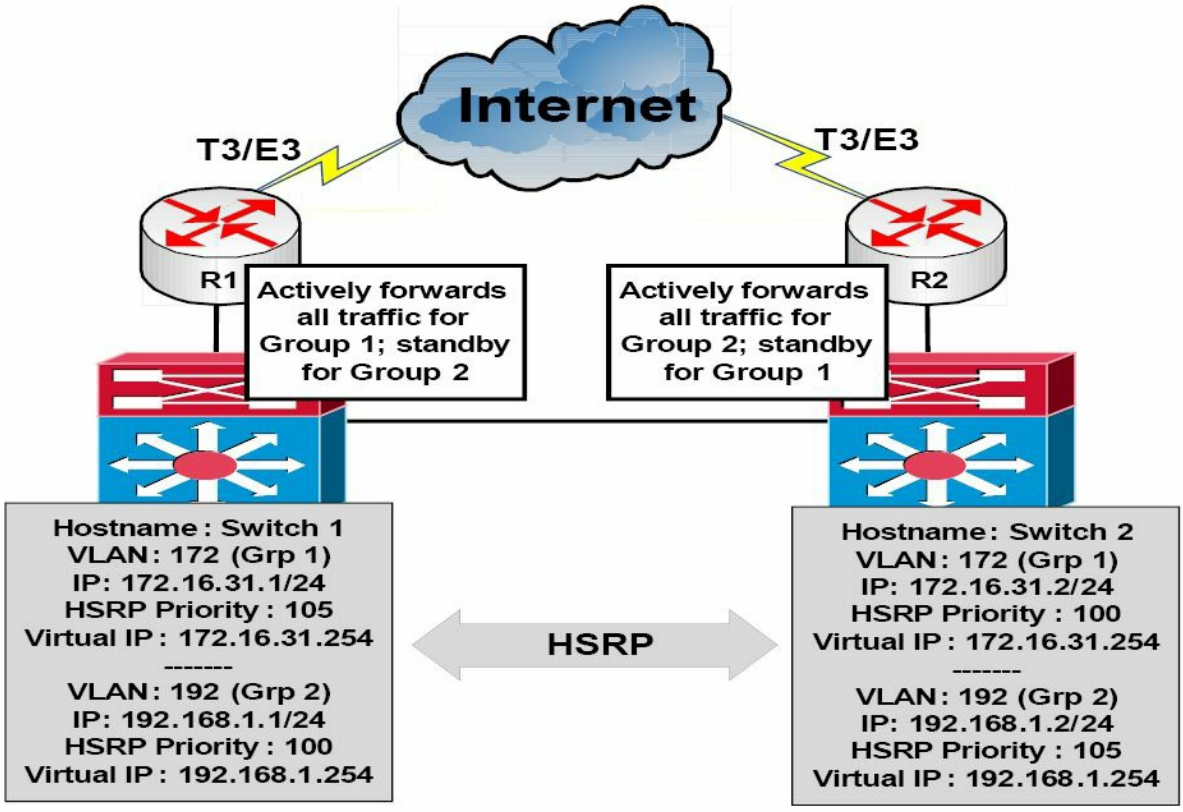


Figure 34.16 – A Network Using HSRP for Load Balancing

By configuring Switch 1 as the active gateway for HSRP Group 1 and Switch 2 as the active gateway for HSRP Group 2, administrators can allow traffic from these two groups to be load balanced between Switch 1 and Switch 2, and ultimately across the two dedicated T3/E3 WAN connections. Each switch then backs up the other's group. For example, Switch 1 will assume the role of active gateway for Group 2 if Switch 2 fails, and vice versa.



Real-World Implementation

In production networks, it is important to remember that creating multiple HSRP groups may result in increased gateway CPU utilisation, as well as increased network utilisation due to HSRP message exchanges. Cisco Catalyst switches, such as the Catalyst 4500 and 6500 series switches, support the implementation of HSRP client groups.

In the previous section, you learned that HSRP allows for the configuration of multiple groups on a single gateway interface. The primary issue with running many different HSRP groups on the gateway interface is that it increases CPU utilisation on the gateway and may potentially also increase the amount of network traffic, given the 3-second Hello interval used by HSRP.

To address this potential issue, HSRP also allows for the configuration of client or slave groups. These are simply HSRP groups that are configured to follow a master HSRP group and that do not participate in the HSRP election. These client or slave groups follow the operation and HSRP status of the master group and, therefore, do not need to exchange periodic Hello packets themselves. This reduces CPU and network utilisation when using multiple HSRP groups.

https://t.me/learningnets

However, it should be noted that client groups send periodic messages in order to refresh their virtual MAC addresses in switches. The refresh message may be sent at a much lower frequency compared with the protocol election messages sent by the master group. While the configuration of client groups is beyond the scope of the CCNA exam requirements, the following output illustrates the configuration of two client groups, which are configured to follow master group HSRP Group 1, also named the SWITCH-HSRP group:

```
Gateway-1(config)#interface vlan100
Gateway-1(config-if)#ip address 192.168.1.1 255.255.255.0
Gateway-1(config-if)#ip address 172.16.31.1 255.255.255.0 secondary
Gateway-1(config-if)#ip address 10.100.10.1 255.255.255.0 secondary
Gateway-1(config-if)#standby 1 ip 192.168.1.254
Gateway-1(config-if)#standby 1 name SWITCH-HSRP
Gateway-1(config-if)#standby 2 ip 172.16.31.254
Gateway-1(config-if)#standby 2 follow SWITCH-HSRP
Gateway-1(config-if)#standby 3 ip 10.100.10.254
Gateway-1(config-if)#standby 3 follow SWITCH-HSRP
Gateway-1(config-if)#exit
```

In the configuration in the output above, Group 1 is configured as the master HSRP group and Groups 2 and 3 are configured as client or slave HSRP groups.

Configuring HSRP on the Gateway

The following steps are required to configure HSRP on the gateway:

1. Configure the correct IP address and mask for the gateway interface using the `ip address [address] [mask] [secondary]` interface configuration command.
2. Create an HSRP group on the gateway interface and assign the group the virtual IP address via the `standby [number] ip [virtual address][secondary]` interface configuration command. The `[secondary]` keyword specifies the IP address as a secondary gateway IP address for the specified group.
3. Optionally, assign the HSRP group a name using the `standby [number] name [name]` interface configuration command.
4. Optionally, if you want to control the election of the active gateway, configure the group priority via the `standby [number] priority [value]` interface configuration command.

The following HSRP configuration outputs in this section will be based on the network below in Figure 34.17:

https://t.me/learningnets

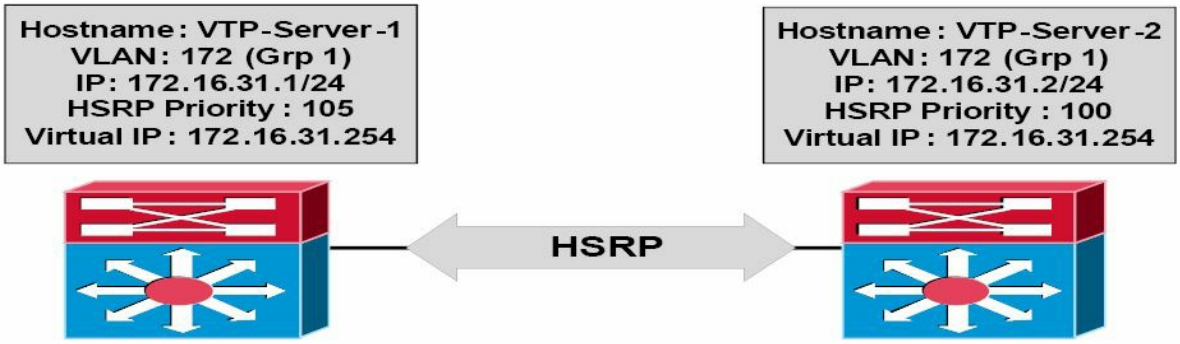


Figure 34.17 – HSRP Configuration Examples Topology

NOTE: It is assumed that the VLAN and trunking configuration between VTP-Server-1 and VTP-Server-2 is already in place and the switches are successfully able to ping each other across VLAN172. For brevity, this configuration output will be omitted from the configuration examples.

```
VTP-Server-1(config)#interface vlan172
VTP-Server-1(config-if)#ip address 172.16.31.1 255.255.255.0
VTP-Server-1(config-if)#standby 1 ip 172.16.31.254
VTP-Server-1(config-if)#standby 1 priority 105
VTP-Server-1(config-if)#exit
VTP-Server-2(config)#interface vlan172
VTP-Server-2(config-if)#ip address 172.16.31.2 255.255.255.0
VTP-Server-2(config-if)#standby 1 ip 172.16.31.254
VTP-Server-2(config-if)#exit
```

NOTE: No priority value is manually assigned for the HSRP configuration applied to VTP-Server-2. By default, HSRP will use a priority value of 100, allowing VTP-Server-1, with a priority value of 105, to win the election and to be elected the primary gateway for the HSRP group.

Once implemented, HSRP configuration may be validated using the `show standby [interface brief]` command. The `show standby brief` command is shown in the following outputs:

```
VTP-Server-1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active  Standby         Virtual IP
Vl172       1    105   Active  local   172.16.31.2     172.16.31.254
VTP-Server-2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active  Standby       Virtual IP
Vl172       1    100   Standby  local   172.16.31.1   172.16.31.254
```

Based on this configuration, VTP-Server-2 will become the active gateway for this group only if VTP-Server-1 fails. Additionally, because preemption is not configured, when VTP-Server-1 comes back online, it will not be able to assume forcefully the role of active gateway, even though it has a higher priority for the HSRP group than that being used on VTP-Server-2.

https://t.me/learningnets

Configuring HSRP Preemption

Preemption allows a gateway to assume forcefully the role of active gateway if it has a higher priority than the current active gateway. HSRP preemption is configured using the `standby [number] preempt` command. This configuration is illustrated on VTP-Server-1 in the following output:

```
VTP-Server-1(config)#interface vlan172
VTP-Server-1(config-if)#standby 1 preempt
```

The `show standby [interface [name]|brief]` command is also used to verify that preemption has been configured on a gateway. This is illustrated by the "`P`" shown in the output of the `show standby brief` command below:

```
VTP-Server-1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active  Standby         Virtual IP
Vl172       1    105 P Active  local   172.16.31.2     172.16.31.254
```

Based on this modification, if VTP-Server-1 did fail and VTP-Server-2 assumed the role of active gateway for VLAN 172, VTP-Server-1 could forcibly reassume that role once it reinitialises. When configuring preemption, Cisco IOS software allows you to specify the duration the switch must wait before it preempts and forcibly reassumes the role of active gateway.

By default, this happens immediately. However, it may be adjusted using the `standby [number] preempt delay [minimum|reload|sync]` interface configuration command. The `[minimum]` keyword is used to specify the minimum amount of time to wait (seconds) before preemption. The following output shows how to configure the gateway to wait 30 seconds before preemption:

```
VTP-Server-1(config)#interface vlan172
VTP-Server-1(config-if)#standby 1 preempt delay minimum 30
```

This configuration may be validated using the `show standby [interface]` command. This is illustrated in the following output:

```
VTP-Server-1#show standby vlan172
Vlan172 - Group 1
  State is Active
    5 state changes, last state change 00:00:32
  Virtual IP address is 172.16.31.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.636 secs
  Preemption enabled, delay min 30 secs
  Active router is local
  Standby router is 172.16.31.2, priority 100 (expires in 8.629 sec)
```

https://t.me/learningnets

```
  Priority 105 (configured 105)
  IP redundancy name is "hsrp-Vl172-1" (default)
```

The `[reload]` keyword is used to specify the amount of time the gateway should wait after it initialises following a reload. The `[sync]` keyword is used in conjunction with IP redundancy clients. This configuration is beyond the scope of the CCNA exam requirements but is very useful in production environments because it prevents an unnecessary change of roles in the case of a flapping interface that is being tracked, or similar activity.

Configuring HSRP Interface Tracking

HSRP interface tracking allows administrators to configure HSRP in order to track the state of interfaces and decrement the current priority value by the default value (10) or a preconfigured value, allowing another gateway to assume the role of primary gateway for the specified HSRP group.

In the following output, VTP-Server-1 is configured to track the state of interface GigabitEthernet5/1, which is connected to an imaginary WAN router. In the event that the state of that interface transitions to "down," the gateway will decrement its priority value by 10 (which is the default):

```
VTP-Server-1(config)#interface vlan172
VTP-Server-1(config-if)#standby 1 track GigabitEthernet5/1
```

This configuration may be validated using the `show standby [interface]` command. This is illustrated in the following output:

```
VTP-Server-1#show standby vlan172
Vlan172 - Group 1
  State is Active
    5 state changes, last state change 00:33:22
  Virtual IP address is 172.16.31.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.085 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.31.2, priority 100 (expires in 7.616 sec)
  Priority 105 (configured 105)
  IP redundancy name is "hsrp-Vl172-1" (default)
  Priority tracking 1 interfaces or objects, 1 up:
  Interface or object           Decrement  State
  GigabitEthernet5/1            10         Up
```

To configure the gateway to decrement its priority value by 50, for example, the `standby [name] track [interface] [decrement value]` command can be issued, as shown in the following

https://t.me/learningnets

output:

```
VTP-Server-1(config)#interface vlan172
VTP-Server-1(config-if)#standby 1 track GigabitEthernet5/1 50
```

This configuration may be validated using the `show standby [interface]` command. This is illustrated in the following output:

```
VTP-Server-1#show standby vlan172
Vlan172 - Group 1
  State is Active
    5 state changes, last state change 00:33:22
  Virtual IP address is 172.16.31.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.085 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.31.2, priority 100 (expires in 7.616 sec)
  Priority 105 (configured 105)
  IP redundancy name is "hsrp-Vl172-1" (default)
  Priority tracking 1 interfaces or objects, 1 up:
  Interface or object           Decrement  State
  GigabitEthernet5/1            50         Up
```

Configuring the HSRP Version

As stated previously in this module, by default, when HSRP is enabled, version 1 is enabled. HSRP version 2 can be manually enabled using the `standby version [1|2]` interface configuration command. HSRP version 2 configuration is illustrated in the following output:

```
VTP-Server-1(config)#interface vlan172
VTP-Server-1(config-if)#standby version 2
```

This configuration may be validated using the `show standby [interface]` command. This is illustrated in the following output:

```
VTP-Server-1#show standby vlan172
Vlan172 - Group 1 (version 2)
  State is Active
    5 state changes, last state change 00:43:42
  Virtual IP address is 172.16.31.254
  Active virtual MAC address is 0000.0c9f.f001
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.419 secs
```

https://t.me/learningnets

```
  Preemption enabled
  Active router is local
  Standby router is 172.16.31.2, priority 100 (expires in 4.402 sec)
  Priority 105 (configured 105)
  IP redundancy name is "hsrp-Vl172-1" (default)
```

Enabling HSRP automatically changes the MAC address range used by HSRP from an address in the 0000.0C07.AC*xx* range to one in the 0000.0C9F.F000 to 0000.0C9F.FFFF range. It is therefore important to understand that this may cause some packet loss in a production network, as devices must learn the new MAC address of the gateway. Such changes are always recommended during a maintenance window or planned outage window.

Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol (VRRP) is a gateway election protocol that dynamically assigns responsibility for one or more virtual gateways to the VRRP routers on a LAN, which allows several routers on a Multi-Access segment, such as Ethernet, to use the same virtual IP address as their default gateway.

VRRP operates in a similar manner to HSRP; however, unlike HSRP, VRRP is an open standard that is defined in RFC 2338, which was made obsolete by RFC 3768. VRRP sends advertisements to the Multicast destination address 224.0.0.18 (VRRP), using IP protocol number 112. At the Data Link Layer, advertisements are sent from the master virtual router MAC address 00-00-5e-00-01*xx*, where "*xx*" represents the two-digit hexadecimal group number. This is illustrated below in Figure 34.18:

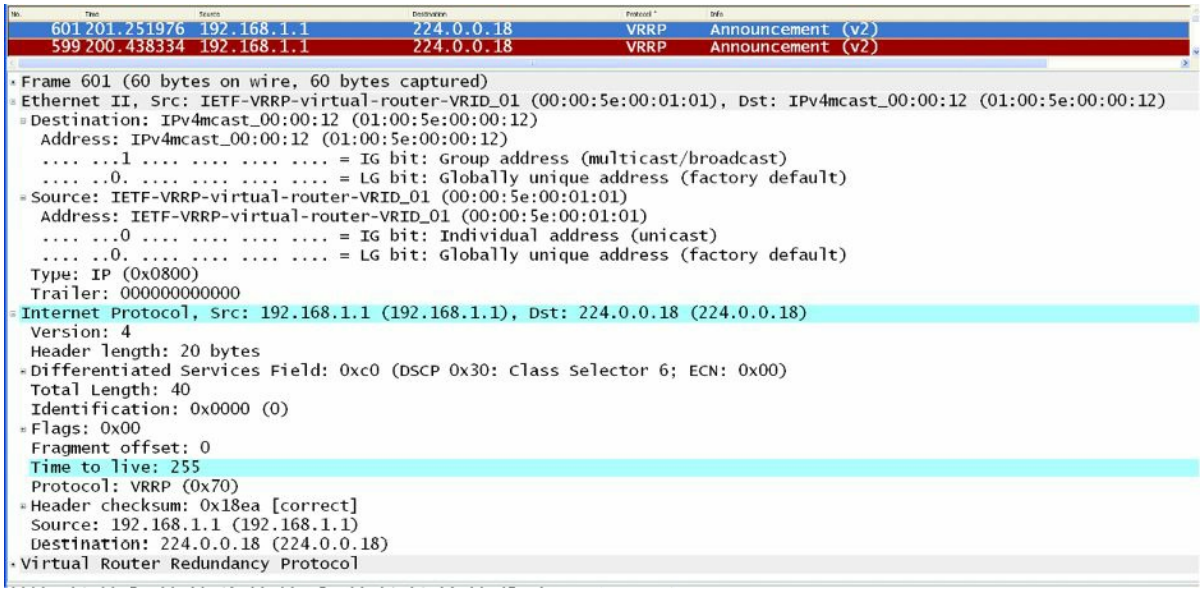


Figure 34.18 – VRRP Multicast Addresses

NOTE: The protocol number is in hexadecimal value. The hexadecimal value 0x70 is the equivalent of the decimal value 112. Similarly, the 12 in the destination Data Link Layer address 01-00-5e-00-00-12 is the hexadecimal value of 18 in decimal value (i.e., 224.0.0.18). If you are unable to determine how these values are reached, hexadecimal to decimal conversion is covered in detail in the current CCNA guide that is available online.

https://t.me/learningnets



Real-World Implementation

Unlike HSRP, VRRP does not have the option of allowing the gateway to use the BIA or a statically configured address as the MAC address for VRRP groups. Therefore, in production networks with more than one VRRP group, it is important to understand the implications of multiple MAC addresses on a particular interface, especially when features such as port security have been implemented. Remember to look at the overall picture; otherwise, you may find that, even though correctly configured, certain features and protocols are not working as they should.

A VRRP gateway is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one gateway is elected as the master virtual router, with the other gateways acting as backup virtual routers in case the master virtual router fails. This concept is illustrated below in Figure 34.19:

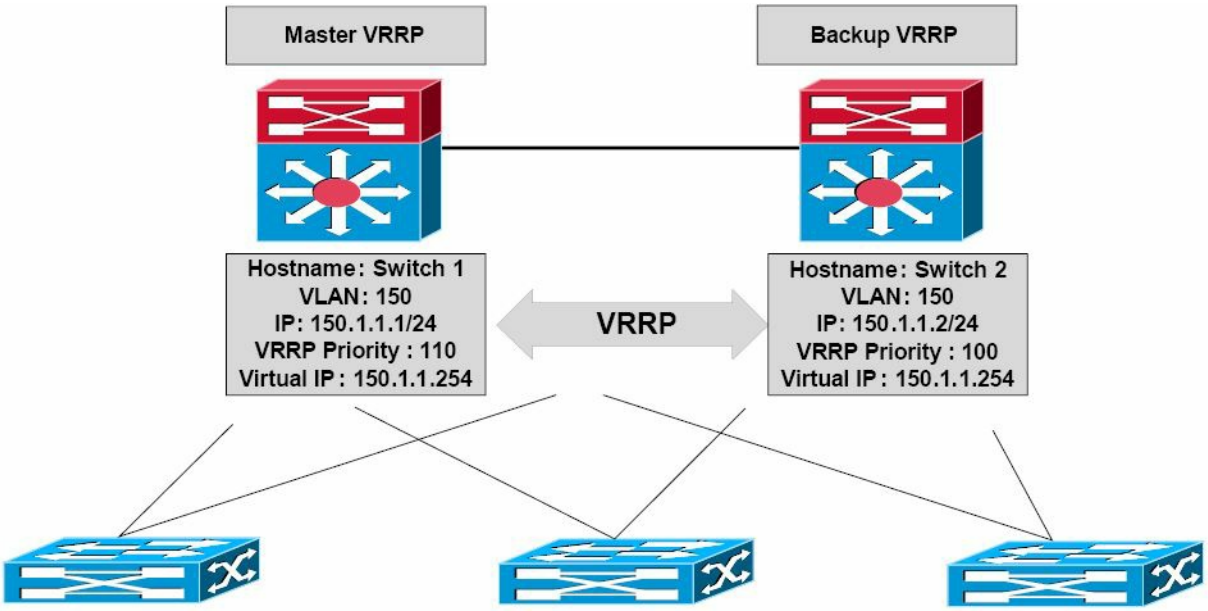


Figure 34.19 – VRRP Basic Operation

VRRP Multiple Virtual Router Support

You can configure up to 255 virtual routers on an interface. The actual number of virtual routers that a router interface can support depends upon the following factors:

- Router processing capability
- Router memory capability
- Router interface support of multiple MAC addresses

VRRP Master Router Election

By default, VRRP uses priority values to determine which router will be elected as the master virtual router. The default VRRP priority value is 100; however, this value can be manually

https://t.me/learningnets

adjusted to a value between 1 and 254. If gateways have the same priority values, the gateway with the highest IP address will be elected as the master virtual router, while the one with the lower IP address becomes the backup virtual router.

If more than two routers are configured as part of the VRRP group, the backup virtual router with the second-highest priority is elected as the master virtual router if the current master virtual router fails or becomes unavailable. If the backup virtual routers have the same priority value, the backup virtual router with the highest IP address is elected as the master virtual router. This concept is illustrated below in Figure 34.20:

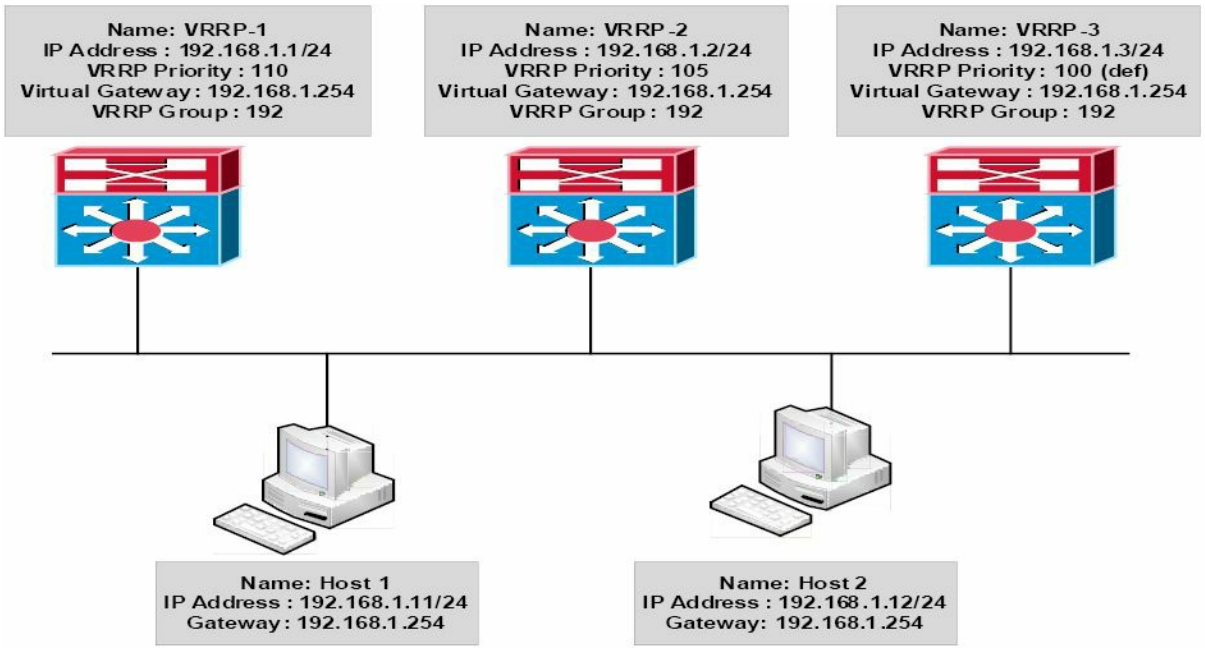


Figure 34.20 – VRRP Master Virtual Router and Backup Virtual Router Election

Figure 34.20 illustrates a network using VRRP for gateway redundancy. Hosts 1 and 2 are configured with a default gateway of 192.168.1.254, which is the virtual IP address configured for VRRP group 192 defined on Switches VRRP-1, VRRP-2, and VRRP-3.

VRRP-1 has a configured priority value of 110, VRRP-2 has a configured priority value of 105, and VRRP-3 is using the default VRRP priority of 100. Based on this configuration, VRRP-1 is elected as the master virtual router and VRRP-2 and VRRP-3 become backup virtual routers.

In the event that VRRP-1 fails, VRRP-2 becomes the master virtual router because it has a higher priority value than VRRP-3. However, if both switches had the same priority value, VRRP-3 would be elected as the master virtual router because it has the higher IP address.

VRRP Preemption

By default, unlike HSRP, preemption is enabled for VRRP and no explicit configuration is required by the administrator to enable this functionality. However, this functionality can be disabled by using the `no vrrp [number] preempt` interface configuration command.

VRRP Load Balancing

VRRP allows for load balancing in a manner similar to HSRP. For example, in a network where multiple virtual routers are configured on a gateway, the interface can act as a master for one virtual router and a backup for one or more virtual routers. This is illustrated below in Figure

https://t.me/learningnets

34.21:

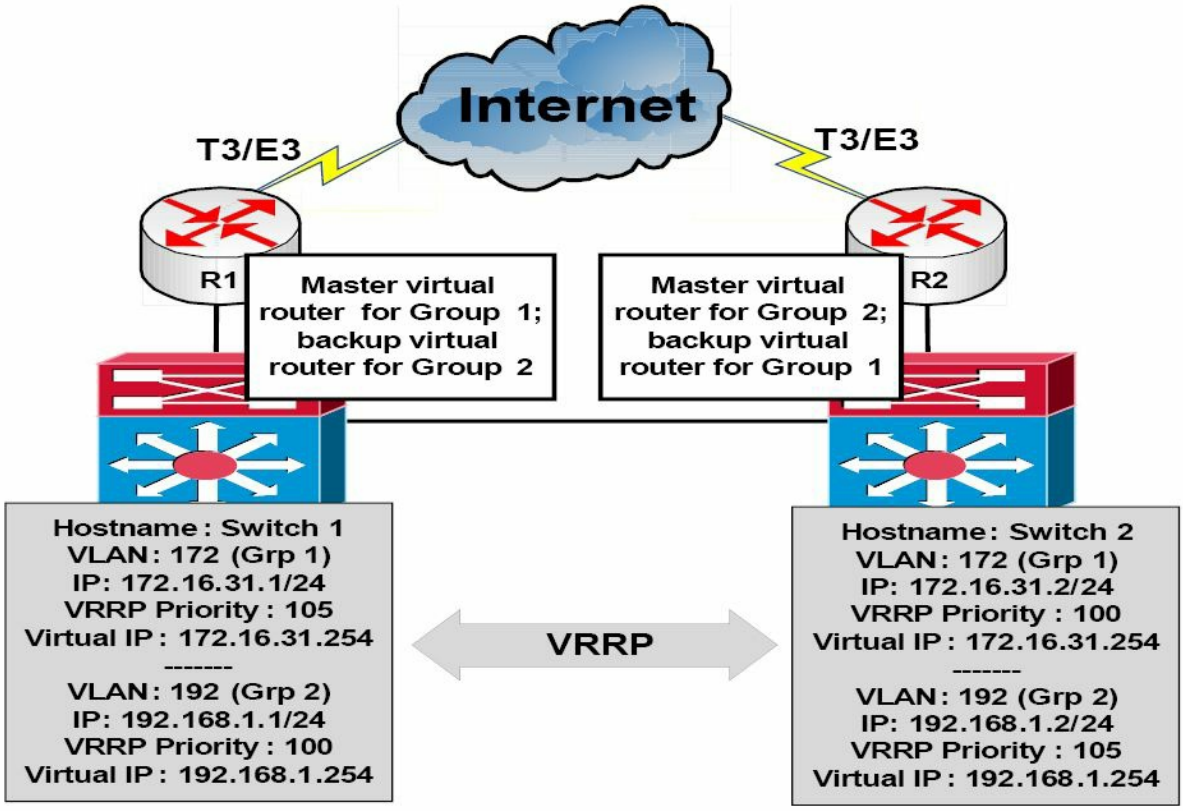


Figure 34.21 – VRRP Load Balancing

VRRP Versions

By default, VRRP version 2 (see Figure 34.22 below) is enabled when VRRP is configured on a gateway in Cisco IOS software. Version 2 is the default and current VRRP version. It is not possible to change the version as is the case with HSRP. There is no VRRP version 1 standard.

NOTE: As of the time this guide was written, VRRP version 3, which defines the VRRP for IPv4 and IPv6, is in draft form and has not yet been standardised.

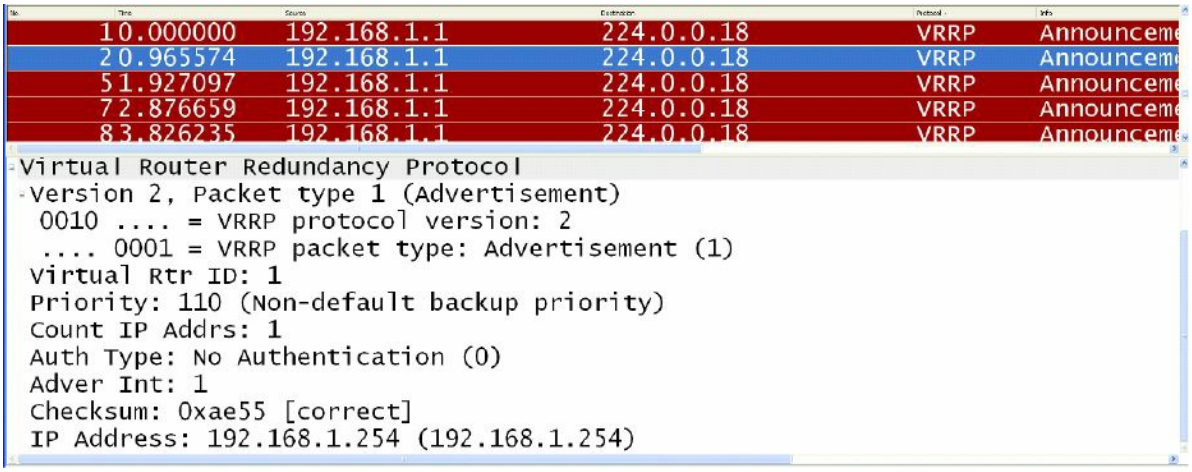


Figure 34.22 – VRRP Version 2 Packet

VRRP Advertisements

The master virtual router sends advertisements to other VRRP routers in the same group. The advertisements communicate the priority and the state of the master virtual router. The VRRP

https://t.me/learningnets

advertisements are encapsulated in IP packets and are sent to the IPv4 Multicast address assigned to the VRRP group, which was illustrated in Figure 34.18. The advertisements are sent every second by default; however, this interval is user-configurable and may be changed. Backup virtual routers also optionally learn the advertisement interval from the master virtual router.

Configuring VRRP on the Gateway

The following steps are required to configure VRRP on the gateway:

1. Configure the correct IP address and mask for the gateway interface using the `ip address [address] [mask] [secondary]` interface configuration command.
2. Create a VRRP group on the gateway interface and assign the group the virtual IP address via the `vrrp [number] ip [virtual address][secondary]` interface configuration command. The `[secondary]` keyword configures the virtual IP address as a secondary gateway address for the specified group.
3. Optionally, assign the VRRP group a description using the `vrrp [number] description[name]` interface configuration command.
4. Optionally, if you want to control the elections of the master virtual router and the backup virtual routers, configure the group priority via the `vrrp [number] priority [value]` interface configuration command.

The VRRP configuration outputs in this section will be based on Figure 34.23 below:

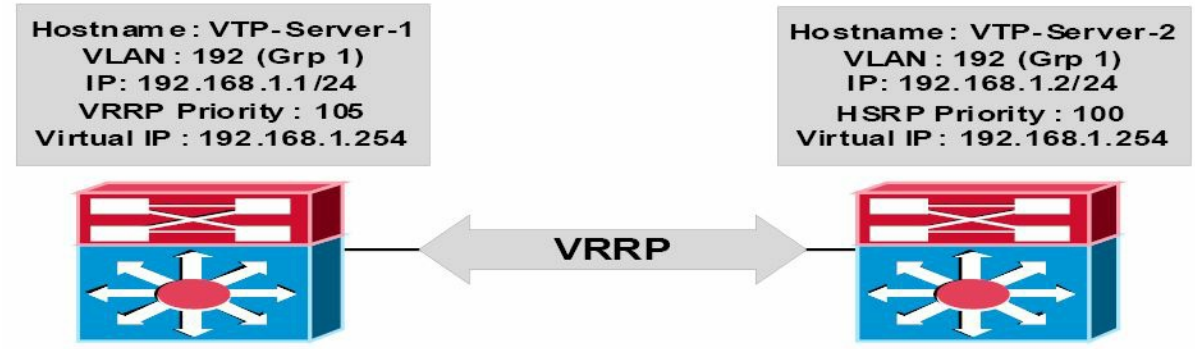


Figure 34.23 – VRRP Configuration Examples Topology

NOTE: It is assumed that the VLAN and trunking configuration between VTP-Server-1 and VTP-Server-2 is already in place and the switches are successfully able to ping each other across VLAN172. For brevity, this configuration output will be omitted from the configuration examples.

```
VTP-Server-1(config)#interface vlan192
VTP-Server-1(config-if)#ip address 192.168.1.1 255.255.255.0
VTP-Server-1(config-if)#vrrp 1 ip 192.168.1.254
VTP-Server-1(config-if)#vrrp 1 priority 105
VTP-Server-1(config-if)#vrrp 1 description 'SWITCH-VRRP-Example'
VTP-Server-1(config-if)#exit
VTP-Server-2(config)#interface vlan192
```

https://t.me/learningnets

```
VTP-Server-2(config-if)#ip address 192.168.1.2 255.255.255.0
VTP-Server-2(config-if)#vrrp 1 ip 192.168.1.254
VTP-Server-2(config-if)#vrrp 1 description 'SWITCH-VRRP-Example'
VTP-Server-2(config-if)#exit
```

NOTE: No priority value is manually assigned for the VRRP configuration applied to VTP-Server-2. By default, VRRP will use a priority value of 100, allowing VTP-Server-1, with a priority value of 105, to win the election and to be elected as the master virtual router for the VRRP group. In addition, a description has also optionally been configured for the group.

This configuration is validated using the `show vrrp [all|brief|interface]` command. The `[all]` keyword shows all information pertaining to the VRRP configuration, which includes the group state, description (if configured), local gateway priority, and master virtual router, among other things. The `[brief]` keyword prints a summary of the VRRP configuration. The `[interface]` keyword prints VRRP information for the specified interface. The following outputs show the `show vrrp all` command:

```
VTP-Server-1#show vrrp all
Vlan192 - Group 1
'SWITCH-VRRP-Example'
  State is Master
  Virtual IP address is 192.168.1.254
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 105
  Master Router is 192.168.1.1 (local), priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.589 sec
VTP-Server-2#show vrrp all
Vlan192 - Group 1
'SWITCH-VRRP-Example'
  State is Backup
  Virtual IP address is 192.168.1.254
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.1.1, priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 3.328 sec)
```

The following outputs show the information printed by the `show vrrp brief` command:

```
VTP-Server-1#show vrrp brief
```

https://t.me/learningnets

```
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Vl192              1   105 3589       Y  Master  192.168.1.1     192.168.1.254
VTP-Server-2#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Vl192              1   100 3609       Y  Backup  192.168.1.1     192.168.1.254
```

Configuring VRRP Interface Tracking

In order to configure VRRP to track an interface, a tracked object must be created in Global Configuration mode using the `track [object number] interface [line-protocol|ip routing]` global configuration command for interface tracking or the `track [object number] ip route [address | prefix] [reachability | metric threshold]` command for IP prefix tracking. Up to 500 tracked objects may be tracked on the switch, depending on the software and platform. Tracked objects are then tracked by VRRP using the `vrrp [number] track [object]` interface configuration command.

NOTE: You are not expected to perform any advanced object tracking configurations.

The following output shows how to configure tracking for VRRP, referencing object 1, which tracks the line protocol of the Loopback0 interface:

```
VTP-Server-1(config)#track 1 interface Loopback0 line-protocol
VTP-Server-1(config-track)#exit
VTP-Server-1(config)#interface vlan192
VTP-Server-1(config-if)#vrrp 1 track 1
VTP-Server-1(config-if)#exit
```

The following output shows how to configure tracking for VRRP, referencing object 2, which tracks the reachability of the 1.1.1.1/32 prefix. A tracked IP route object is considered to be up and reachable when a routing table entry exists for the route and the route is not inaccessible (i.e., has a route metric of 255), in which case the route is removed from the Routing Information Base (RIB) anyway:

```
VTP-Server-1(config)#track 2 ip route 1.1.1.1/32 reachability
VTP-Server-1(config-track)#exit
VTP-Server-1(config)#interface vlan192
VTP-Server-1(config-if)#vrrp 1 track 2
```

VRRP tracking configuration is verified using the `show vrrp interface [name]` command. This is illustrated in the following output:

```
VTP-Server-1#show vrrp interface vlan192
Vlan192 - Group 1
'SWITCH-VRRP-Example'
  State is Master
  Virtual IP address is 192.168.1.254
  Virtual MAC address is 0000.5e00.0101
```

https://t.me/learningnets

```
  Advertisement interval is 0.100 sec
  Preemption enabled
  Priority is 105
    Track object 1 state Up decrement 10
    Track object 2 state Up decrement 10
  Authentication MD5, key-string
  Master Router is 192.168.1.1 (local), priority is 105
  Master Advertisement interval is 0.100 sec
  Master Down interval is 0.889 sec
```

To view the parameters of the tracked objects, use the `show track [number][brief] [interface] [ip] [resolution][timers]` command. The output of the `show track` command is illustrated as follows:

```
VTP-Server-1#show track
Track 1
  Interface Loopback0 line-protocol
  Line protocol is Up
    1 change, last change 00:11:36
  Tracked by:
    VRRP Vlan192 1
Track 2
  IP route 1.1.1.1 255.255.255.255 reachability
  Reachability is Up (connected)
    1 change, last change 00:08:48
  First-hop interface is Loopback0
  Tracked by:
    VRRP Vlan192 1
```

NOTE: Tracked objects can also be used in conjunction with HSRP and GLBP. GLBP is described in a section to follow.

Debugging VRRP

The `debug vrrp` command provides several options that the administrator can use to view real-time information on VRRP operation. These options are illustrated in the following output:

```
VTP-Server-1#debug vrrp ?
  all      Debug all VRRP information
  auth     VRRP authentication reporting
  errors   VRRP error reporting
  events   Protocol and Interface events
  packets  VRRP packet details
  state    VRRP state reporting
  track    Monitor tracking
```

https://t.me/learningnets

<cr>

Gateway Load Balancing Protocol

Like HSRP, Gateway Load Balancing Protocol (GLBP) is a Cisco proprietary protocol. GLBP provides high network availability in a manner similar to HSRP and VRRP. However, unlike HSRP and VRRP, in which only a single gateway actively forwards traffic for a particular group at any given time, GLBP allows multiple gateways within the same GLBP group to actively forward network traffic at the same time.

GLBP gateways communicate through Hello messages that are sent every three seconds to the Multicast address 224.0.0.102, using UDP port 3222. This is illustrated below in Figure 34.24:

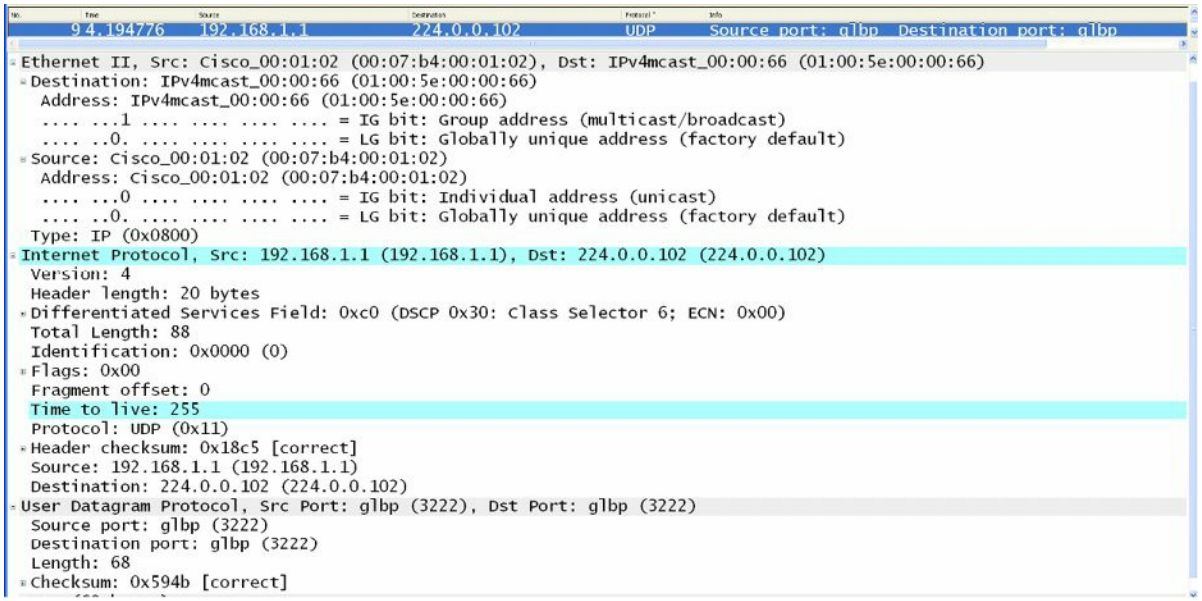


Figure 34.24 – GLBP Layer 3 and Layer 4 Protocols and Addresses

GLBP Operation

When GLBP is enabled, the GLBP group members elect one gateway to be the active virtual gateway (AVG) for that group. The AVG is the gateway that has the highest priority value. In the event that the priority values are equal, the AVG with the highest IP address in the group will be elected as the gateway. The other gateways in the GLBP group provide backup for the AVG in the event that the AVG becomes unavailable.

The AVG answers all Address Resolution Protocol (ARP) requests for the virtual router address. In addition, the AVG assigns a virtual MAC address to each member of the GLBP group. Each gateway is therefore responsible for forwarding packets that are sent to the virtual MAC address which has been assigned by the AVG. These gateways are referred to as active virtual forwarders (AVFs) for their assigned MAC addresses. This allows GLBP to provide load sharing. This concept is illustrated below in Figure 34.25:

https://t.me/learningnets

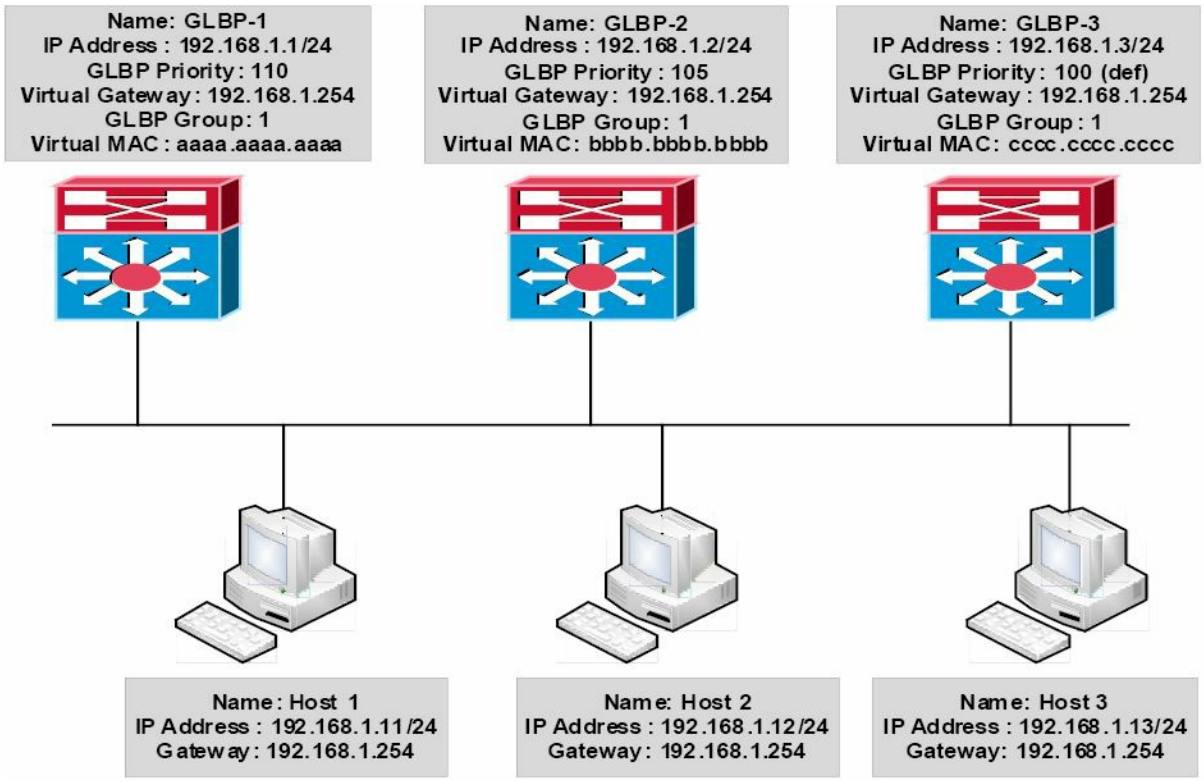


Figure 34.25 – GLBP Active Virtual Gateway and Active Virtual Forwarders

Figure 34.25 shows a network using GLBP as the FHRP. The three gateways are all configured in GLBP Group 1. Gateway GLBP-1 is configured with a priority of 110, gateway GLBP-2 is configured with a priority of 105, and gateway GLBP-3 is using the default priority of 100. GLBP-1 is elected AVG, and GLBP-2 and GLBP-3 are assigned virtual MAC addresses bbbb.bbbb.bbbb and cccc.cccc.cccc, respectively, and become AVFs for those virtual MAC addresses. GLBP-1 is also the AVF for its own virtual MAC address, aaaa.aaaa.aaaa.

Hosts 1, 2, and 3 are all configured with the default gateway address 192.168.1.254, which is the virtual IP address assigned to the GLBP group. Host 1 sends out an ARP Broadcast for its gateway IP address. This is received by the AVG (GLBP-1), which responds with its own virtual MAC address aaaa.aaaa.aaaa. Host 1 forwards traffic to 192.168.1.254 to this MAC address.

Host 2 sends out an ARP Broadcast for its gateway IP address. This is received by the AVG (GLBP-1), which responds with the virtual MAC address of bbbb.bbbb.bbbb (GLBP-2). Host 2 forwards traffic to 192.168.1.254 to this MAC address and GLBP-2 forwards this traffic.

Host 3 sends out an ARP Broadcast for its gateway IP address. This is received by the AVG (GLBP-1), which responds with the virtual MAC address of cccc.cccc.cccc (GLBP-3). Host 3 forwards traffic to 192.168.1.254 to this MAC address and GLBP-3 forwards this traffic.

By using all gateways in the group, GLBP allows for load sharing without having to configure multiple groups as would be required if either HSRP or VRRP was being used as the FHRP.

GLBP Virtual MAC Address Assignment

A GLBP group allows up to four virtual MAC addresses per group. The AVG is responsible for assigning the virtual MAC addresses to each member of the group. Other group members request a virtual MAC address after they discover the AVG through Hello messages.

https://t.me/learningnets

Gateways are assigned the next virtual MAC address in sequence. A gateway that is assigned a

virtual MAC address by the AVG is known as a primary virtual forwarder, while a gateway that has learned the virtual MAC address is referred to as a secondary virtual forwarder.

GLBP Redundancy

Within the GLBP group, a single gateway is elected as the AVG, and another gateway is elected as the standby virtual gateway. All other remaining gateways in the group are placed in a Listen state. If an AVG fails, the standby virtual gateway will assume responsibility for the virtual IP address. At the same time, an election is held and a new standby virtual gateway is then elected from the gateways currently in the Listen state.

In the event the AVF fails, one of the secondary virtual forwarders in the Listen state assumes responsibility for the virtual MAC address. However, because the new AVF is already a forwarder using another virtual MAC address, GLBP needs to ensure that the old forwarder MAC address ceases being used and hosts are migrated away from this address. This is achieved using the following two timers:

- The redirect timer
- The timeout timer

The redirect time is the interval during which the AVG continues to redirect hosts to the old virtual forwarder MAC address. When this timer expires, the AVG stops using the old virtual forwarder MAC address in ARP replies, although the virtual forwarder will continue to forward packets that were sent to the old virtual forwarder MAC address.

When the timeout timer expires, the virtual forwarder is removed from all gateways in the GLBP group. Any clients still using the old MAC address in their ARP caches must refresh the entry to obtain the new virtual MAC address. GLBP uses Hello messages to communicate the current state of these two timers.

GLBP Load Preemption

By default, GLBP preemption is disabled, which means that a backup virtual gateway can become the AVG only if the current AVG fails, regardless of the priorities assigned to the virtual gateways. This method of operation is similar to that used by HSRP.

Cisco IOS software allows administrators to enable preemption, which allows a backup virtual gateway to become the AVG if the backup virtual gateway is assigned a higher priority than the current AVG. By default, the GLBP virtual forwarder preemptive scheme is enabled with a delay of 30 seconds. However, this value can be manually adjusted by administrators.

GLBP Weighting

GLBP uses a weighting scheme to determine the forwarding capacity of each gateway that is in the GLBP group. The weighting assigned to a gateway in the GLBP group can be used to determine whether it will forward packets and, if so, the proportion of hosts in the LAN for which it will forward packets.

By default, each gateway is assigned a weight of 100. Administrators can additionally configure the gateways to make dynamic weighting adjustments by configuring object tracking, such as

https://mylearningnets

for interfaces and IP prefixes, in conjunction with GLBP. If an interface fails, the weighting is dynamically decreased by the specified value, allowing gateways with higher weighting values to be used to forward more traffic than those with lower weighting values.

In addition, thresholds can be set to disable forwarding when the weighting for a GLBP group falls below a certain value, and then when it rises above another threshold, forwarding is automatically re-enabled. A backup virtual forwarder can become the AVF if the current AVF weighting falls below the low weighting threshold for 30 seconds.

GLBP Load Sharing

GLBP supports the following three load-sharing methods:

- Host-dependent
- Round-robin
- Weighted

With host-dependent load sharing, each client that generates an ARP request for the virtual router address always receives the same virtual MAC address in reply. This method provides clients with a consistent gateway MAC address.

The round-robin load-sharing mechanism distributes the traffic evenly across all gateways participating as AVFs in the group. This is the default load-sharing mechanism.

The weighted load-sharing mechanism using the weighting value determines the proportion of traffic that should be sent to a particular AVF. A higher weighting value results in more frequent ARP replies containing the virtual MAC address of that gateway.

GLBP Client Cache

The GLBP client cache contains information about network hosts that are using a GLBP group as the default gateway. The cache entry contains information about the host that sent the IPv4 ARP or IPv6 Neighbor Discovery (ND) request and which forwarder the AVG has assigned to it, the number of the GLBP forwarder that each network host has been assigned to, and the total number of network hosts currently assigned to each forwarder in a GLBP group.

The AVG for a GLBP group can be enabled to store a client cache database of all the LAN clients using this group. The maximum number of entries that may be stored can be up to 2000, but it is recommended that this number never exceed 1000. While GLBP cache configuration is beyond the scope of the CCNA exam requirements, this feature can be configured using the `glbp client-cache` command and then verified using the `show glbp detail` command.

Configuring GLBP on the Gateway

The following steps are required to configure GLBP on the gateway:

1. Configure the correct IP address and mask for the gateway interface using the `ip address [address] [mask] [secondary]` interface configuration command.
2. Create a GLBP group on the gateway interface and assign the group the virtual IP address via the `glbp [number] ip [virtual address][secondary]` interface configuration

https://t.me/learningnets

command. The `[secondary]` keyword configures the virtual IP address as a secondary gateway address for the specified group.

3. Optionally, assign the VRRP group a name using the `glbp [number] name [name]` interface configuration command.
4. Optionally, if you want to control the election of the AVG, configure the group priority via the `glbp [number] priority [value]` interface configuration command.

The GLBP configuration examples in this section will be based on Figure 34.26 below:

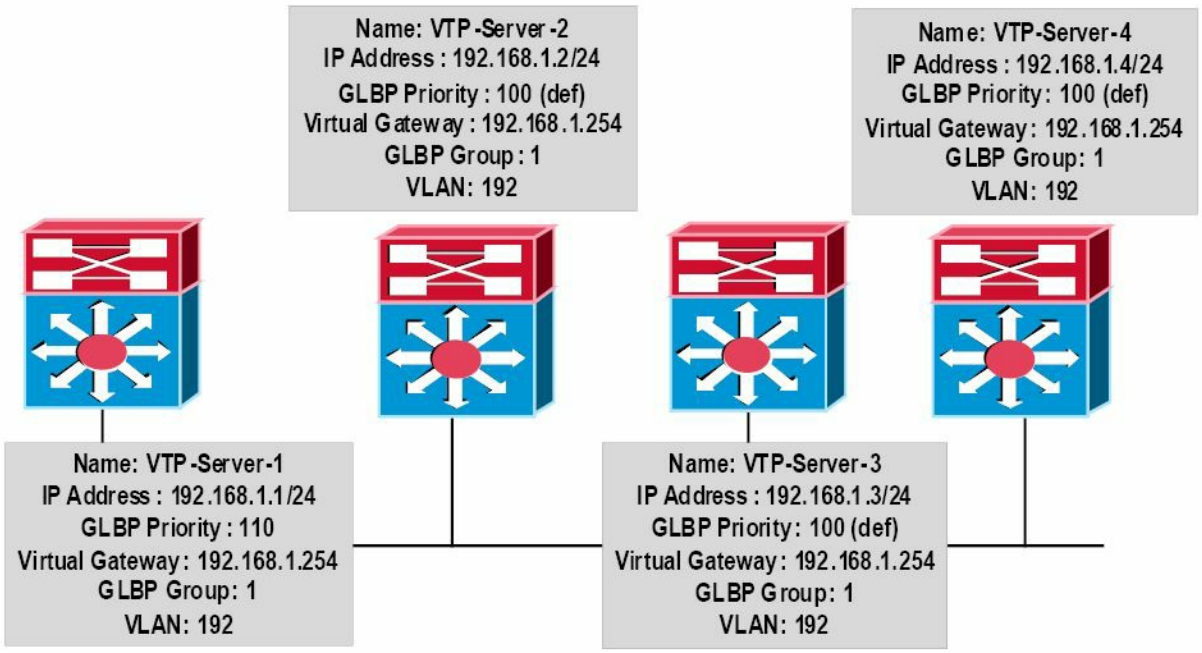


Figure 34.26 – GLBP Configuration Examples Topology

NOTE: It is assumed that VLAN and trunking configuration between the switches is already in place and the switches are successfully able to ping each other across VLAN192. For the sake of brevity, this configuration output will be omitted from the configuration examples.

```
VTP-Server-1(config)#interface vlan192
VTP-Server-1(config-if)#glbp 1 ip 192.168.1.254
VTP-Server-1(config-if)#glbp 1 priority 110
VTP-Server-1(config-if)#exit
VTP-Server-2(config)#interface vlan192
VTP-Server-2(config-if)#glbp 1 ip 192.168.1.254
VTP-Server-2(config-if)#exit
VTP-Server-3(config)#interface vlan192
VTP-Server-3(config-if)#glbp 1 ip 192.168.1.254
VTP-Server-3(config-if)#exit
VTP-Server-4(config)#interface vlan192
VTP-Server-4(config-if)#glbp 1 ip 192.168.1.254
VTP-Server-4(config-if)#exit
```

https://t.me/learningnets

Once the GLBP group has been configured, the `show glbp brief` command can be used to view a summary of the GLBP configuration, as shown in the following outputs:

```
VTP-Server-1#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router  Standby router
Vl192       1    -   110 Active   192.168.1.254   local          192.168.1.4
Vl192       1    1   -   Active   0007.b400.0101  local          -
Vl192       1    2   -   Listen   0007.b400.0102  192.168.1.2    -
Vl192       1    3   -   Listen   0007.b400.0103  192.168.1.3    -
Vl192       1    4   -   Listen   0007.b400.0104  192.168.1.4    -

VTP-Server-2#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router  Standby router
Vl192       1    -   100 Listen   192.168.1.254   192.168.1.1    192.168.1.4
Vl192       1    1   -   Listen   0007.b400.0101  192.168.1.1    -
Vl192       1    2   -   Active   0007.b400.0102  local          -
Vl192       1    3   -   Listen   0007.b400.0103  192.168.1.3    -
Vl192       1    4   -   Listen   0007.b400.0104  192.168.1.4    -

VTP-Server-3#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router  Standby router
Vl192       1    -   100 Listen   192.168.1.254   192.168.1.1    192.168.1.4
Vl192       1    1   -   Listen   0007.b400.0101  192.168.1.1    -
Vl192       1    2   -   Listen   0007.b400.0102  192.168.1.2    -
Vl192       1    3   -   Active   0007.b400.0103  local          -
Vl192       1    4   -   Listen   0007.b400.0104  192.168.1.4    -

VTP-Server-4#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router  Standby router
Vl192       1    -   100 Standby  192.168.1.254   192.168.1.1    local
Vl192       1    1   -   Listen   0007.b400.0101  192.168.1.1    -
Vl192       1    2   -   Listen   0007.b400.0102  192.168.1.2    -
Vl192       1    3   -   Listen   0007.b400.0103  192.168.1.3    -
Vl192       1    4   -   Active   0007.b400.0104  local          -
```

From the output above, you can see that VTP-Server-1 (192.168.1.1) has been elected as the AVG based on its priority value of 110, which is higher than that of all the other gateways. Gateway VTP-Server-4 (192.168.1.4) has been elected as the standby virtual gateway because it has the highest IP address of the remaining three gateways, even though they all share the same priority value. Gateways VTP-Server-2 and VTP-Server-3 are therefore placed in the Listen state.

https://t.me/learningnets

The `show glbp` command prints detailed information on the status of the GLBP group. The

output of this command is illustrated as follows:

```
VTP-Server-1#show glbp
Vlan192 - Group 1
  State is Active
    2 state changes, last state change 02:52:22
  Virtual IP address is 192.168.1.254
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.465 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption disabled
  Active is local
  Standby is 192.168.1.4, priority 100 (expires in 9.619 sec)
  Priority 110 (configured)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    0004.c16f.8741 (192.168.1.3)
    000c.cea7.f3a0 (192.168.1.2)
    0013.1986.0a20 (192.168.1.1) local
    0030.803f.ea81 (192.168.1.4)
  There are 4 forwarders (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 02:52:12
    MAC address is 0007.b400.0101 (default)
    Owner ID is 0013.1986.0a20
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
  Forwarder 2
    State is Listen
    MAC address is 0007.b400.0102 (learnt)
    Owner ID is 000c.cea7.f3a0
    Redirection enabled, 599.299 sec remaining (maximum 600 sec)
    Time to live: 14399.299 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.1.2 (primary), weighting 100 (expires in 9.295 sec)
  Forwarder 3
    State is Listen
    MAC address is 0007.b400.0103 (learnt)
```

https://t.me/learningnets

```
  Owner ID is 0004.c16f.8741
  Redirection enabled, 599.519 sec remaining (maximum 600 sec)
  Time to live: 14399.519 sec (maximum 14400 sec)
  Preemption enabled, min delay 30 sec
  Active is 192.168.1.3 (primary), weighting 100 (expires in 9.515 sec)
Forwarder 4
  State is Listen
  MAC address is 0007.b400.0104 (learnt)
  Owner ID is 0030.803f.ea81
  Redirection enabled, 598.514 sec remaining (maximum 600 sec)
  Time to live: 14398.514 sec (maximum 14400 sec)
  Preemption enabled, min delay 30 sec
  Active is 192.168.1.4 (primary), weighting 100 (expires in 8.510 sec)
```

When executed on the AVG, the `show glbp` command shows, among other things, the address of the standby virtual gateway and the number of AVFs in the group, as well as the states that it has assigned to them. The virtual MAC addresses for each AVF are also displayed.

https://t.me/learningnets

Day 34 Questions

1. Name two FHRP protocols that are Cisco proprietary.
2. Name the open standard FHRP protocol.
3. By default, when HSRP is enabled in Cisco IOS software, version 1 is enabled. True or false?
4. Which Multicast address does HSRP version 2 use to send Hello packets?
5. HSRP version 1 group numbers are restricted to the range of 0 to 255, whereas the version 2 group numbers have been extended from 0 to 4095. True or false?
6. Which parameter can be adjusted in order to influence the HSRP primary gateway election?
7. How does HSRP interface tracking influence the primary gateway election process?
8. Which command can you use to configure an HSRP address on an interface?
9. Just like HSRP, VRRP has the option of allowing the gateway to use the BIA or a statically configured address as the MAC address for VRRP groups. True or false?
10. Which command can you use to configure a GLBP group IP address on a router interface?

https://t.me/learningnets

Day 34 Answers

1. HSRP and GLBP.
2. VRRP.
3. True.
4. 224.0.0.102.
5. True.
6. HSRP priority.
7. It modifies HSRP priority based on interface status.
8. The `standby [number] ip [virtual address]` command.
9. False.
10. The `glbp [number] ip [virtual address]` command

https://t.me/learningnets

Day 34 Labs

HSRP Lab

Test the commands explained in this module, working on a scenario that includes two routers directly connected (i.e., Fa0/0 is connected to Fa0/0). Those routers should connect to a switch using, for example, ports Fa0/1. Connect a workstation on the switch.

- ☐ Configure a consistent IP addressing scheme on the two routers, for example, 192.168.0.1/24 and 192.168.0.2/24
- ☐ Configure HSRP 10 on the LAN-facing interfaces, using the 192.168.0.10 address
- ☐ Name the HSRP group as CCNA
- ☐ Control the election of the primary HSRP gateway using the `standby 10 priority 110` command
- ☐ Verify HSRP configuration using the `show standby [brief]` command
- ☐ Configure HSRP preemption on both routers
- ☐ Shut down Router 1 and see how Router 2 becomes primary
- ☐ Restart Router 1 and see how it becomes primary again due to preemption being enabled
- ☐ Configure the workstation with the IP address 192.168.0.100/24 and the gateway address 192.168.0.10; ping the gateway from the workstation
- ☐ Configure interface tracking: track an unused interface on the router using the `standby 10 track [int number]` command; cycle that interface through different states and see how the corresponding router priority changes based on the interface state
- ☐ Configure HSRP version 2 with the `standby version 2` command
- ☐ Adjust HSRP timers on both routers with the `standby 10 timers x y` command
- ☐ Configure MD5 HSRP authentication between the routers
- ☐ Debug HSRP using the `debug standby` command during a priority change on one of the routers and see how the second one is elected as the primary gateway

VRRP Lab

Repeat the previous lab but this time using VRRP instead of HSRP, with the applicable command changes.

GLBP Lab

Repeat the first lab but this time using GLBP instead of HSRP, with the applicable command changes. Configure GLBP load sharing on the routers using the `glbp 10 load-balancing round-robin` command and see how traffic from the LAN hits both routers.

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 35 – Booting and IOS

Day 35 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete the lab(s) of your choice
- Read the ICND2 cram guide

Architecture refers to the components which go into making the router and how they are used during the router booting process. This is all fundamental stuff to a Cisco CCNA engineer who needs to know what the various types of memory do and how to backup or manipulate them using IOS commands.

Today you will learn about the following:

- Router memory and files
- Managing the IOS

This lesson maps to the following ICND2 syllabus requirements:

- Describe the boot process of Cisco IOS routers
- POST
- Router bootup process
- Manage Cisco IOS Files
- Boot preferences
- Cisco IOS images (15)
- Licensing
- Show/Change license

Router Memory and Files

Figure 35.1 below illustrates the main memory components inside the router. Each type of memory performs a different role and contains different files:

https://t.me/learningnets

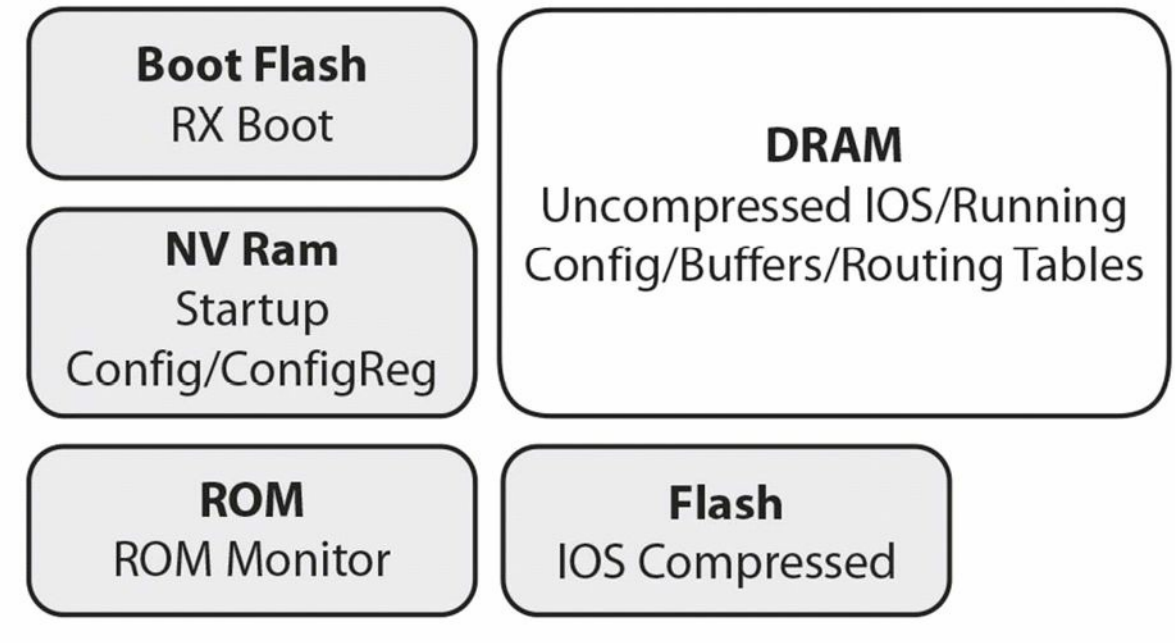


Figure 35.1 – Router Memory Components

You can usually see memory banks inside the router when the cover is removed. You can often also see flash memory cards inserted into router slots.



Figure 35.2 – DRAM SIMMs on a Router Motherboard

Here is what each memory and file type does:

Boot ROM – EEPROM for startup diagram/Rommon and loads IOS. When the router boots, if no IOS file is present, it will boot into an emergency mode called Rommon, which allows some limited commands to be entered to recover the router and load another IOS. This is known as bootstrap mode and you can recognise it with either of the router prompts below:

```
>
Rommon>
```

NVRAM – Stores router startup configuration and configuration register. The startup configuration is the file used to store the saved router configuration. It is not erased when the router reloads.

https://t.me/learningnets

Flash/PCMCIA – Contains IOS and some configuration files. Flash memory is also referred to as EEPROM, and Cisco IOS is usually stored here in a compressed form. You can in fact have more than one version of Cisco IOS on flash memory if there is room.

DRAM – Also known as RAM, it stores the full IOS, running configuration, and routing tables. This is the working memory, which is erased upon the router being rebooted.

ROM Monitor – System diagnostics and startup. The ROM monitor has a very small code called bootstrap or boothelper in it to check for attached memory and interfaces.

RxBoot – Mini-IOS, allows for an upload of the full IOS. It is also known as the boot loader and can be used to perform some router maintenance activities.

Router Configuration – Although not strictly a router component, it is stored in NVRAM and pulled into DRAM on boot up. You put the configuration from DRAM into NVRAM with the `copy run start` command, while you put files from NVRAM into DRAM with the `copy start run` command.

The Configuration Register – Sets instructions for booting. It is critical that you understand this because you will need to manipulate the configuration register on routers for use in labs (i.e., boot clean with no configuration) or to perform a password recovery. Some models differ but the two most common settings are as follows:

Boot and ignore startup configuration – 0x2142

Boot normally – 0x2102

```
Router(config)#config-register 0x2102
```

You can see the current configuration register setting with a `show version` command:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.1(17), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by Cisco Systems, Inc.
Compiled Wed 04-Sep-02 03:08 by kellythw Image text-base: 0x03073F40, data-base:
0x00001000

ROM: System Bootstrap, Version 11.0(10c)XB2, PLATFORM SPECIFIC RELEASE SOFTWARE (fc1)
BOOTLDR: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c)XB2, PLATFORM SPECIFIC
RELEASE SOFTWARE (fc1)

Router uptime is 12 minutes
System returned to ROM by reload
System image file is "flash:c2500-js-l.121-17.bin"

Cisco 2500 (68030) processor (revision L) with 14336K/2048K bytes of memory.
Processor board ID 01760497, with hardware revision 00000000 Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read ONLY)
```

https://t.me/learningnets

```
Configuration register is 0x2102
```

The command also displays how long the router has been online and the reason for the last reload – handy if you need to troubleshoot a booting issue.

```
Router uptime is 12 minutes
System returned to ROM by reload
```

And the same command will display the various types of memory on the router:

```
Router#show version Cisco Internetwork Operating System Software IOS (tm) 2500 Software
(C2500-IS-L), Version 12.2(4)T1, RELEASE SOFTWARE Copyright (c) 1986-2001 by Cisco
Systems, Inc.

ROM: System Bootstrap, Version 11.0(10c), SOFTWARE ← ROM code
BOOTLDR: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c)

System image file is "flash:c2500-is-l_122-4_T1.bin" ← Flash image
Cisco 2522 (68030) processor  CPU ← CPU
with 14336K/2048K bytes of memory. ← DRAM
Processor board ID 18086064, with hardware revision 00000003
32K bytes of non-volatile configuration memory. ← NVRAM
16384K bytes of processor System flash (Read ONLY) ← EEPROM/FLASH
```

Here is a graphical representation of the router booting process:

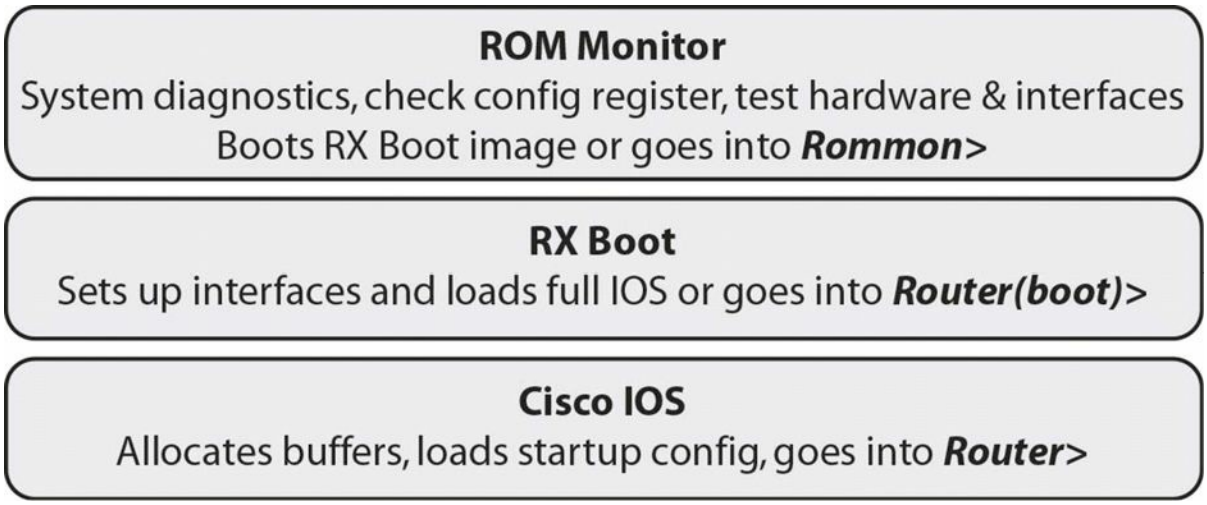


Figure 35.3 – Router Booting Process

Managing the IOS

Many network disasters could have been avoided with simple router and switch housekeeping. If your router configuration file is important to you and your business, then you should back it up.

If you are happy that the current running configuration of the router is going to be your working version, then you can copy this into NVRAM with the `copy run start` command.

In order to save the router configuration, you need to have a PC or server on your network running TFTP server software. You can download this free software from companies such as SolarWinds. The same process is used to upgrade the flash image.

Router configurations can be moved around the router or stored on a PC or server on the

https://hellotraining.com

network. The running configuration on the router is stored in DRAM. Any changes to the configuration will remain in DRAM and will be lost if the router is reloaded for any reason.

You can copy the configuration onto a PC or server running TFTP server software:

`Router#copy startup-config tftp:` ← You need to include the colon

You can also copy your IOS to a TFTP server. You must always do this if you are updating the router IOS to a newer version just in case of issues with the new version (often, network administrators try to fit a file onto the router which is too big for the installed memory).

`Router#copy flash tftp:`

The router will prompt you for the IP address of the TFTP server, which I recommend you have in the same subnet as your router. If you want to reverse the process, then you simply reverse the commands:

`Router#copy tftp flash:`

The issue with these commands is that most engineers use them only a couple of times a year or when there has been a network disaster. Usually, you will find that your Internet access has also gone down with your network, so you have to do this all from memory!

I strongly recommend that you do some backup and restoring of your configurations and IOS on your home network. In addition, check out my recovery lab on YouTube:

www.youtube.com/user/paulwbrowning

You can view the flash filename with the `show version` command or the `show flash` command, or you can drill down into the flash with the `dir flash:` command and this will show you all the files present in flash memory:

```
RouterA#show flash
System flash directory:
File      Length        Name/status
1         14692012      c2500-js-l.121-17.bin
[14692076 bytes used, 2085140 available, 16777216 total]
16384K bytes of processor board System flash (Read ONLY)
```

I would like to dwell on this subject in more detail, but you should focus on the CCNA exam and your daily tasks. Disaster recovery should be on your list of stuff to research and lab up, though.

Booting Options

There are several options available when the router boots. Usually, there is one IOS image in flash memory so the router will boot using that. You may have more than one image, or the image may be too big for the flash memory to hold, so you might prefer the router to boot from a TFTP server on the network which holds the IOS.

The commands differ slightly, depending upon which boot options you want to configure. Try all of the options on a live router.

```
RouterA(config)#boot system ?
WORD  TFTP filename or URL
```

https://t.me/learningnets

```
flash           Boot from flash memory
mop             Boot from a Decnet MOP server
ftp             Boot from server via ftp
rcp             Boot from server via rcp
tftp            Boot from tftp server
```

For flash:

```
RouterA(config)#boot system flash ? WORD System image filename <cr>
```

For TFTP:

```
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#boot system tftp: c2500-js-l.121-17.bin ? Hostname or A.B.C.D Address
from which to download the file <cr>
RouterA(config)#boot system tftp:
```

Booting Process and POST

A standard router boot sequence looks like this:

1. The device powers on and will first perform the POST (Power on Self Test). The POST tests the hardware in order to verify that all the components are present and healthy (interfaces, memory, CPU, ASICs, etc.). The POST is stored in and run from ROM (read only memory).
2. The bootstrap looks for and loads the Cisco IOS software. The bootstrap is a programme in ROM that is used to execute programmes and is responsible for finding where each IOS is located, and then loading the file. The bootstrap programme locates the Cisco IOS software and loads it into RAM. Cisco IOS files can be located in one of three places: flash memory, a TFTP server, or another location indicated in the startup configuration file. By default, the IOS software is loaded from flash memory in all Cisco routers. The configuration settings must be changed to load from one of the other locations.
3. The IOS software looks for a valid configuration file in NVRAM (i.e., the startup-config file).
4. If a startup-config file is present in NVRAM, the router will load this file and the router will be operational. If a startup-config file is not present in NVRAM, the router will start the setup-mode configuration.

Any further modification on a running router will be stored on RAM, where you need to manually execute the command `copy running-config startup-config` to make your current configuration as a startup-config every time you boot your router.

IOS Licensing

Since the creation of the first Internetwork Operating System (IOS) for the first Cisco router, Cisco have followed the same method, each model of router having it's own version and release built. Major versions were given the numbering system 12.0. Changes to these versions were then numbered 12.1, 12.2, etc. Within those versions were releases fixing bugs and adding support for modules and other features, such as 12.1(1a).

https://t.me/learningnets

Unfortunately, as support was added and bugs fixed, the releases were split into trains so each model had it's own IOS, which led to various versions and releases. If you wanted a security or voice image, then you would have to buy that specific image with the correct version for your router, with the correct feature support and bug fixes.

Cisco eventually released entire training tools and presentations so you could understand the naming conventions, release levels, and supported modules. As the software was tested and matured it was also given different names, such as ED for Early Deployment and GD for General Deployment! It all got very confusing for customers. Here is an image from some of Cisco's documentation explaining IOS releases:

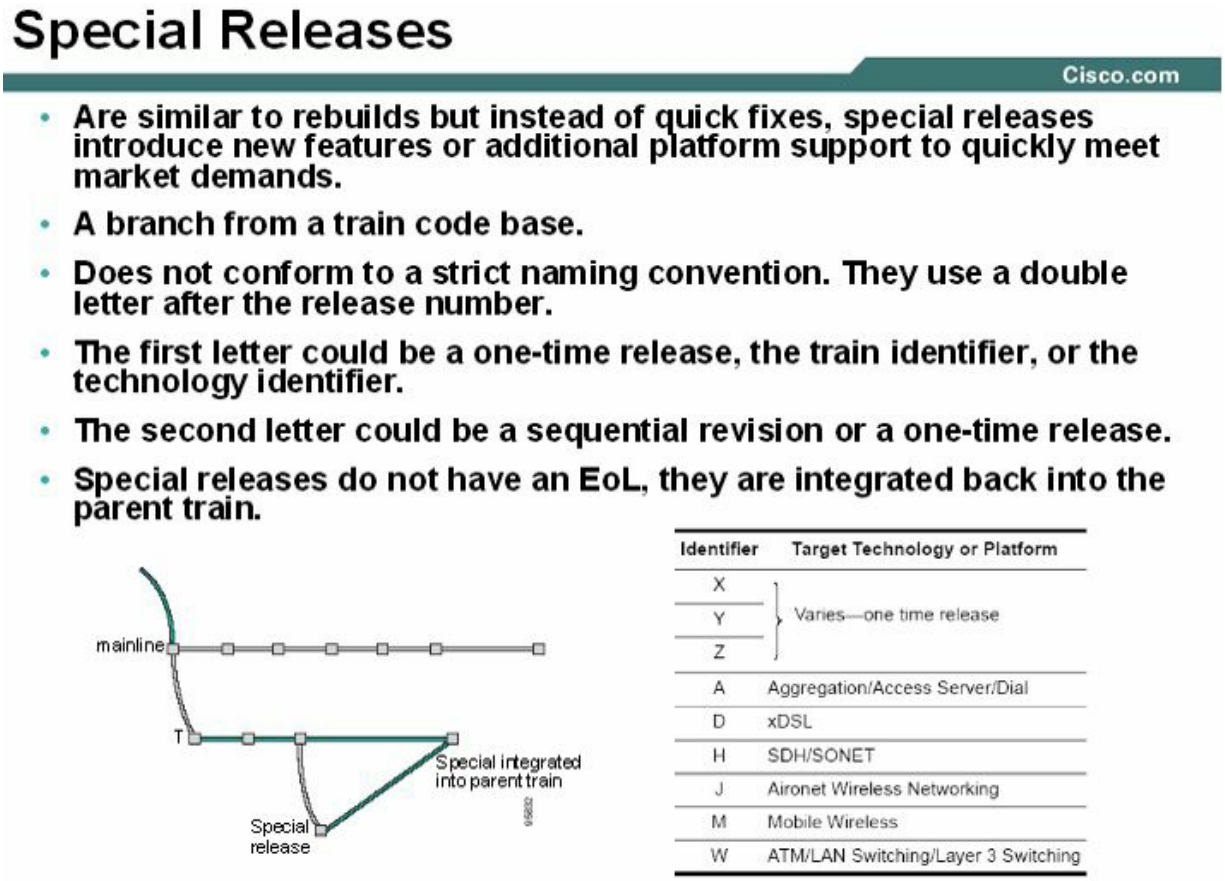


Figure 35.4 – IOS Special Releases (Image Copyright Cisco Systems Inc.)

I can't tell you how many times while working at Cisco TAC I had to deal with confused and angry customers who had bought a router and IOS only to find it didn't support the features they required for their network infrastructure. Remember also that for large, enterprise networks, an IOS upgrade may have to be arranged months in advance during a tiny maintenance window.

A New Model

Cisco have now changed their IOS model and jumped from IOS release 12 to 15. Currently, there is one universal image built per model. This image features all the feature sets you require, but in order to gain access to the advanced features you need to buy the appropriate license and verify it on the actual device. This was done for convenience for both Cisco and their customers and to prevent theft or unauthorised sharing of Cisco software, which costs a considerable amount to develop, as you can imagine.

https://t.me/learningnets

All new models bought from Cisco (resellers) come with a base image installed and the license enabled on the router. If the customer wants to enable advanced security or voice features, then these features need to be enabled. This is usually achieved using a free Cisco application called Cisco License Manager (CLM). You can easily search for this on Cisco.com:

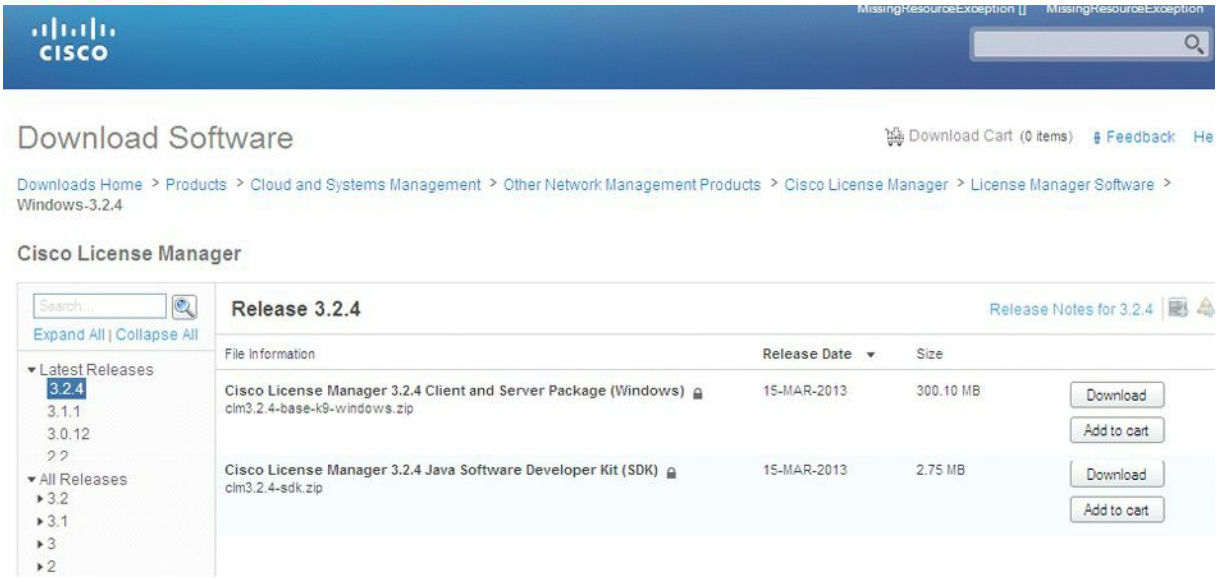


Figure 35.5 – Cisco License Manager Download Page

CLM can be installed on a server or host enabling the customer to interface between their devices and Cisco's license portal. CLM takes care of tracking current licenses and features per device using a GUI.

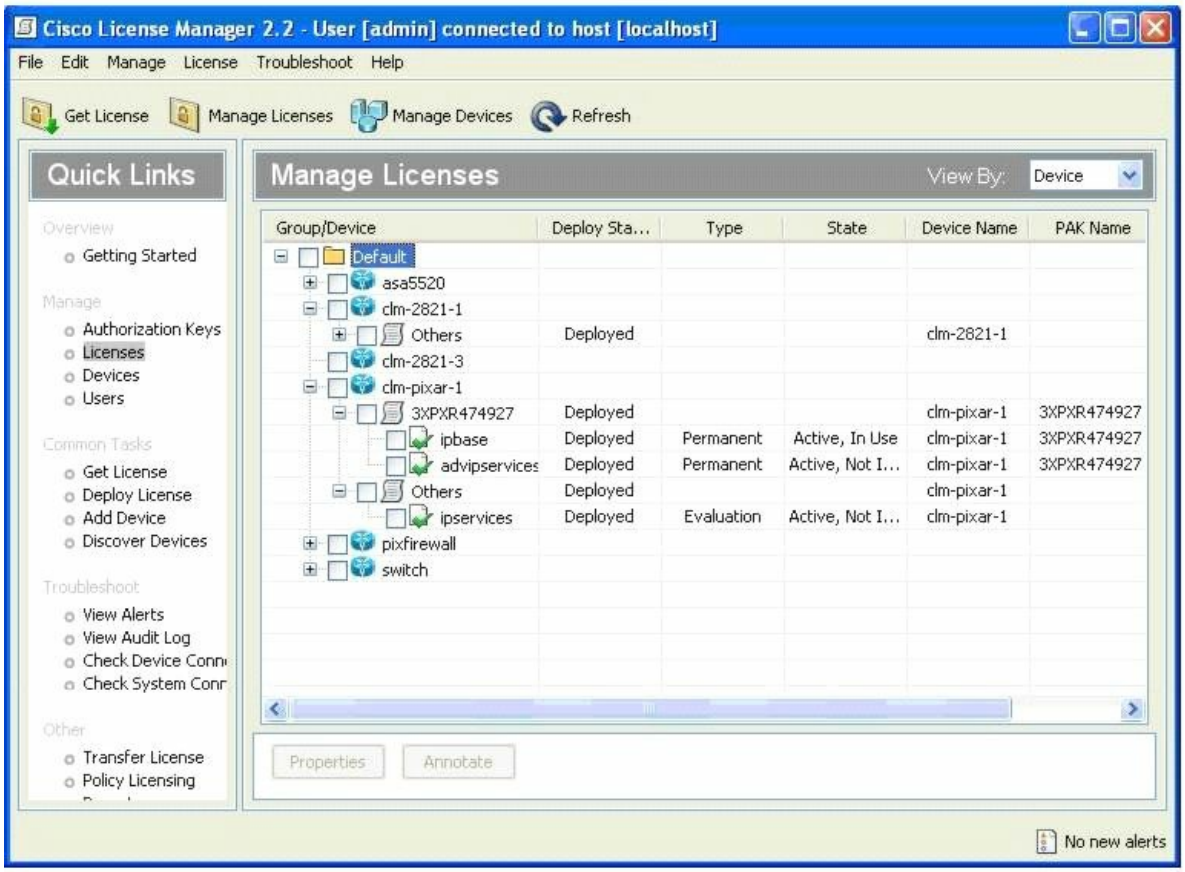


Figure 35.6 – Cisco License Manager GUI (Image Copyright Cisco Systems Inc.)

License Activation

https://t.me/learningnets

Each model of Cisco router (that supports licensing) has been allocated a unique identifying number known as the unique device identifider (UDI). This is comprised of the serial number (SN) and the product identification (PID). Issue the `show license udi` command to see this information.

```
Router#show license ?
  all      Show license all information
  detail   Show license detail information
  feature  Show license feature information
  udi      Show license udi information
Router#show license udi
Device#   PID               SN              UDI
------------------------------------------------------------------
*0        CISCO1941/K9      FTX15240000     CISCO1941/K9:FTX15240000
```

You would enter the UDI when registering the IOS with Cisco at www.cisco.com/go/license. You would also add the license you were issued by the reseller when you paid for the IOS (Product Authorization Key or PAK), which is checked against the UDI. If this is verified, you are e-mailed a license key by Cisco.

You can see below which features have been activated. The `ipbasek9` feature will always be enabled.

```
Router#show license all
License Store: Primary License Storage
StoreIndex: 0   Feature: ipbasek9                     Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
License Store: Evaluation License Storage
StoreIndex: 0   Feature: securityk9                   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period: 208 weeks 2 days
            Evaluation period left: 208 weeks 2 days
        License Count: Non-Counted
        License Priority: None
StoreIndex: 1   Feature: datak9                       Version: 1.0
        License Type:
        License State: Inactive
            Evaluation total period: 208 weeks 2 days
            Evaluation period left: 208 weeks 2 days
        License Count: Non-Counted
```

https://t.me/learningnets

```
        License Priority: None
```

The `show license feature` command will print a summary of features enabled:

```
Router#show license feature
Feature name        Enforcement  Evaluation  Subscription   Enabled
ipbasek9            no           no          no             yes
securityk9          yes          yes         no             no
datak9              yes          no          no             no
```

Once the license has been verified, the license key must be added to the router via the USB drive or network server and the `license install [url]` command issued from the command line. Notice the ".lic" filename.

```
Router#dir usbflash0:

Directory of usbflash0:/

   1  -rw-        3064  Apr 18 2013 03:31:18 +00:00  FHH1216P07R_20090528163510702.lic

255537152 bytes total (184524800 bytes free)
Router#
Router#license install  usbflash0:FHH1216P07R_20090528163510702.lic
Installing...Feature:datak9...Successful:Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
Router#
*Jun 25 11:18:20.234: %LICENSE-6-INSTALL: Feature datak9 1.0 was installed in this
device. UDI=CISCO2951:FHH1216P07R; StoreIndex=0:Primary License Storage
*Jun 25 11:18:20.386: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = c2951
Next reboot level = datak9 and License = datak9
```

The router will now have to be rebooted to activate the new feature set.

https://t.me/learningnets

Day 35 Questions

1. Which files would you usually find in DRAM?
2. Where is the compressed IOS held?
3. You want to boot the router and skip the startup configuration. Which command do you use to modify the configuration register?
4. Which command puts the running configuration into NVRAM?
5. Which command will copy your startup configuration onto a network server?
6. You want to boot your router from a network server holding the IOS. Which command will achieve this?
7. The universal image includes all the feature sets you require, but in order to gain access to the advanced features you need to buy the appropriate license and verify it on the actual device. True or false?
8. The ROM monitor has a very small code called bootstrap or boothelper in it to check for attached memory and interfaces. True or false?
9. Which command do you use to view the files stored on the flash memory on a Cisco router?
10. What is the purpose of the POST?

https://t.me/learningnets

Day 35 Answers

1. Uncompressed IOS, running configuration, and routing tables.
2. On the flash memory.
3. The `config-register [version]` command in Global Configuration mode.
4. The `copy run start` command.
5. The `copy start tftp:` command.
6. The `boot system [option]`command.
7. True.
8. True.
9. The `show flash/dir` command.
10. The POST tests the hardware in order to verify that all the components are present and healthy (interfaces, memory, CPU, ASICs, etc.).

https://t.me/learningnets

Day 35 Lab

Test the configuration commands detailed in this module:

- ☐ Issue a `show version` on a Cisco device and inspect the output; correlate them with the exaplanations detailed in the module
- ☐ Copy the startup-config to a TFTP server
- ☐ Copy a config file from a TFTP server to the router
- ☐ Copy an IOS from a TFTP server to the router flash memory
- ☐ Verify the flash contents with the `show flash` command
- ☐ Boot the device using the new IOS file with the `boot system flash:[name]` command

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 36 – EIGRP

Day 36 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's lab
- Read the ICND2 cram guide

Enhanced Interior Gateway Routing Protocol (EIGRP) is a proprietary Interior Gateway Protocol (IGP) that was developed by Cisco. EIGRP includes traditional Distance Vector characteristics, such as split horizon, as well as characteristics that are similar to those used by Link State routing protocols, such as incremental updates.

Although EIGRP has Link State routing protocol characteristics, EIGRP falls under the Distance Vector routing protocol classification and is referred to as an advanced Distance Vector routing protocol instead. EIGRP runs directly over IP using protocol number 88.

Today you will learn about the following:

- Cisco EIGRP overview and fundamentals
- EIGRP configuration fundamentals
- EIGRP messages
- EIGRP neighbour discovery and maintenance
- Metrics, DUAL, and the topology table
- Equal cost and unequal cost load sharing
- Default routing using EIGRP
- Split horizon in EIGRP networks
- EIGRP stub routing
- EIGRP route summarisation
- Understanding passive interfaces
- Understanding the use of the EIGRP router ID
- EIGRP logging and reporting

This lesson maps to the following CCNA syllabus requirements:

- Configure and verify EIGRP (single AS)
- Feasible Distance / Feasible Successor routes / Reported Distance / Advertised Distance
- Feasibility condition

https://t.me/learningnets

- Metric composition
- Router ID
- Auto summary
- Path selection
- Load balancing
  - Equal
  - Unequal
- Passive interfaces

Cisco EIGRP Overview and Fundamentals

Cisco developed Enhanced IGRP to overcome some of the limitations of its proprietary Distance Vector routing protocol, Interior Gateway Routing Protocol (IGRP). IGRP offered improvements over Routing Information Protocol (RIP), such as support for an increased number of hops; however, IGRP still succumbed to the traditional Distance Vector routing protocol limitations, which included the following:

- Sending full periodic routing updates
- A hop limitation
- The lack of VLSM support
- Slow convergence
- The lack of loop prevention mechanisms

Unlike the traditional Distance Vector routing protocols, which send their neighbours periodic routing updates that contain all routing information, EIGRP sends non-periodic incremental routing updates to distribute routing information throughout the routing domain. The EIGRP incremental updates are sent when there is a change in the network topology.

By default, RIP (a former CCNA-level topic) has a hop-count limitation of up to 15 hops, which makes RIP suitable only for smaller networks. EIGRP has a default hop-count limitation of 100; however, this value can be manually adjusted by the administrator using the `metric maximum-hops <1-255>` router configuration command when configuring EIGRP. This allows EIGRP to support networks that contain hundreds of routers, making it more scalable and better suited for larger networks.

Enhanced IGRP uses two unique Type/Length/Value (TLV) triplets to carry route entries. These TLVs are the Internal EIGRP Route TLV and the External EIGRP Route TLV, which are used for internal and external EIGRP routes, respectively. Both TLVs include an 8-bit Prefix Length field that specifies the number of bits used for the subnet mask of the destination network. The information that is contained in this field allows EIGRP to support variably subnetted networks.

Enhanced IGRP converges much faster than the traditional Distance Vector routing protocols. Instead of relying solely on timers, EIGRP uses information contained in its topology table to

https://t.me/learningnets

locate alternate paths. EIGRP can also query neighbouring routers for information if an alternate path is not located in the local router's topology table. The EIGRP topology table will be described in detail later in this module.

In order to ensure that there are loop-free paths through the network, EIGRP uses the Diffusing Update Algorithm (DUAL), which is used to track all routes advertised by neighbours and then select the best loop-free path to the destination network. DUAL is a core EIGRP concept that will be described in detail later in this module.

EIGRP Configuration Fundamentals

Enhanced IGRP is enabled in Cisco IOS software using the `router eigrp [ASN]` global configuration command. The `[ASN]` keyword designates the EIGRP autonomous system number (ASN). This is a 32-bit integer between 1 and 65535. In addition to other factors, which will be described later in this lesson, routers running EIGRP must reside within the same autonomous system to form a neighbour relationship successfully. Following the configuration of the `router eigrp [ASN]` global configuration command, the router transitions to EIGRP Router Configuration mode wherein you can configure parameters pertaining to EIGRP. The configured ASN can be verified in the output of the `show ip protocols` command, as follows:

```
R1#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
...

[Truncated Output]
```

In addition to the `show ip protocols` command, the `show ip eigrp neighbors` command prints information on all known EIGRP neighbours and their respective autonomous systems. This command, and its available options, will be described in detail later in this module. On routers running multiple instances of EIGRP, the `show ip eigrp [ASN]` command can be used to view information pertaining only to the autonomous system that is specified in this command. The use of this command is illustrated in the following output:

```
R1#show ip eigrp 150 ?
  interfaces  IP-EIGRP interfaces
  neighbors   IP-EIGRP neighbors
  topology    IP-EIGRP topology table
  traffic     IP-EIGRP traffic statistics
```

https://t.me/learningnets

In the output above, 150 is the ASN. The default in Cisco IOS software is to print information on all EIGRP instances if an autonomous system is not specified with any `show ip eigrp` commands.

Once in Router Configuration mode, the `network` command is used to specify the network(s) (interfaces) for which EIGRP routing will be enabled. When the `network` command is used and a major classful network is specified, the following actions are performed on the EIGRP-enabled router:

- EIGRP is enabled for networks that fall within the specified classful network range.
- The topology table is populated with these directly connected subnets.
- EIGRP Hello packets are sent out of the interfaces associated with these subnets.
- EIGRP advertises the network(s) to EIGRP neighbours in Update messages.
- Based on the exchange of messages, EIGRP routes are then added to the IP routing table.

For example, assume that the router has the following Loopback interfaces configured:

- Loopback0 – IP Address 10.0.0.1/24
- Loopback1 – IP Address 10.1.1.1/24
- Loopback2 – IP Address 10.2.2.1/24
- Loopback3 – IP Address 10.3.3.1/24

If EIGRP is enabled for use and the major classful 10.0.0.0/8 network is used in conjunction with the `network` router configuration command, all four Loopback interfaces are enabled for EIGRP routing. This is illustrated in the following output:

```
R1#show ip eigrp interfaces
IP-EIGRP interfaces for process 150
                    Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface      Peers Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Lo0              0        0/0         0       0/10           0           0
Lo1              0        0/0         0       0/10           0           0
Lo2              0        0/0         0       0/10           0           0
Lo3              0        0/0         0       0/10           0           0
```

You can use the `show ip protocols` command to verify that EIGRP is enabled for the major classful 10.0.0.0/8 network. The output of this command is illustrated below:

```
R1#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
```

https://t.me/learningnets

```
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 150
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

The EIGRP topology table can be viewed using the `show ip eigrp topology` command. The output of this command is illustrated below:

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(150)/ID(10.3.3.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.3.3.0/24, 1 successors, FD is 128256
        via Connected, Loopback3
P 10.2.2.0/24, 1 successors, FD is 128256
        via Connected, Loopback2
P 10.1.1.0/24, 1 successors, FD is 128256
        via Connected, Loopback1
P 10.0.0.0/24, 1 successors, FD is 128256
        via Connected, Loopback0
```

NOTE: The topology table, EIGRP Hello packets, and Update messages are described in detail later in this module. The focus of this section is restricted to EIGRP configuration implementation.

Using the `network` command to specify a major classful network allows multiple subnets that fall within the classful network range to be advertised at the same time with minimal configuration. However, there may be situations where administrators may not want all of the subnets within a classful network to be enabled for EIGRP routing. For example, referencing the Loopback interfaces configured on R1 in the previous example, assume that you want EIGRP routing enabled only for the 10.1.1.0/24 and 10.3.3.0/24 subnets, and not for the 10.0.0.0/24 and 10.2.2.0/24 subnets. While it appears that this would be possible if you specified the networks (i.e., 10.1.1.0 and 10.3.3.0) when using the `network` command, Cisco IOS software still converts these statements to the major classful 10.0.0.0/8 network, as illustrated below:

```
R1(config)#router eigrp 150
R1(config-router)#network 10.1.1.0
```

https://t.me/learningnets

```
R1(config-router)#network 10.3.3.0
R1(config-router)#exit
```

Despite the configuration above, the `show ip protocols` command reveals the following:

```
R1#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 150
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
Distance: internal 90 external 170
```

NOTE: A common misconception is that disabling the EIGRP automatic summarisation feature addresses this issue; however, this has nothing to do with the `auto-summary` command. For example, assume that you issued the `no auto-summary` command to the configuration used in the previous example, as follows:

```
R1(config)#router eigrp 150
R1(config-router)#network 10.1.1.0
R1(config-router)#network 10.3.3.0
R1(config-router)#no auto-summary
R1(config-router)#exit
```

The `show ip protocols` command still shows that EIGRP is enabled for network 10.0.0.0/8, as illustrated below:

```
R1#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
```

https://t.me/learningnets

```
  EIGRP maximum hopcount 100
```

```
  EIGRP maximum metric variance 1
  Redistributing: eigrp 150
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

In order to provide more granular control of the networks that are enabled for EIGRP routing, Cisco IOS software supports the use of wildcard masks in conjunction with the `network` statement when configuring EIGRP. The wildcard mask operates in a manner similar to the wildcard mask used in ACLs and is independent of the subnet mask for the network.

As an example, the command `network 10.1.1.0 0.0.0.255` would match the 10.1.1.0/24 network, the 10.1.1.0/26 network, and the 10.1.1.0/30 network. Referencing the Loopback interfaces configured in the previous output, R1 would be configured as follows to enable EIGRP routing for the 10.1.1.0/24 and 10.3.3.0/24 subnets, and not for the 10.0.0.0/24 subnet or the 10.2.2.0/24 subnet:

```
R1(config)#router eigrp 150
R1(config-router)#network 10.1.1.0 0.0.0.255
R1(config-router)#network 10.3.3.0 0.0.0.255
R1(config-router)#exit
```

This configuration can be validated using the `show ip protocols` command, as follows:

```
R1#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 150
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.1.1.0/24
    10.3.3.0/24
```

https://t.me/learningnets

```
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

Additionally, the `show ip eigrp interfaces` command can be used to validate that EIGRP routing has been enabled only for Loopback1 and Loopback3:

```
R1#show ip eigrp interfaces
IP-EIGRP interfaces for process 150
                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface     Peers   Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Lo1             0        0/0         0       0/10           0           0
Lo3             0        0/0         0       0/10           0           0
```

As illustrated in the output above, EIGRP routing is enabled only for Loopback1 and Loopback3 because of the wildcard mask configuration.

It is important to remember that the `network` command can be configured using the subnet mask, rather than the wildcard mask. When this is the case, Cisco IOS software inverts the subnet mask and the command is saved using the wildcard mask. For example, referencing the same Loopback interfaces on the router, R1 could also be configured as follows:

```
R1(config-router)#router eigrp 150
R1(config-router)#network 10.1.1.0 255.255.255.0
R1(config-router)#network 10.3.3.0 255.255.255.0
R1(config-router)#exit
```

Based on this configuration, the following is entered in the running configuration (I've used a pipe to drill down to the part of config I'm interested in):

```
R1#show running-config | begin router eigrp
router eigrp 150
network 10.1.1.0 0.0.0.255
network 10.3.3.0 0.0.0.255
auto-summary
```

You can see by the above configuration that you can use pipes with show commands in order to get more granularity. This will be a familiar concept to anyone with previous programming knowledge.

If a specific address on the network is used, in conjunction with the wildcard mask, Cisco IOS software performs a logical AND operation to determine the network that will be enabled for EIGRP. For example, if the `network 10.1.1.15 0.0.0.255` command is issued, Cisco IOS software performs the following actions:

- Inverts the wildcard mask to the subnet mask value of 255.255.255.0
- Performs a logical AND operation
- Adds the `network 10.1.1.0 0.0.0.255` command to the configuration

https://t.me/learningnets

The `network` configuration used in this example is illustrated in the following output:

```
R1(config)#router eigrp 150
R1(config-router)#network 10.1.1.15 0.0.0.255
R1(config-router)#exit
```

Based on this, the running configuration on the router displays the following:

```
R1#show running-config | begin router eigrp
router eigrp 150
network 10.1.1.0 0.0.0.255
auto-summary
```

If a specific address on the network is used in conjunction with the subnet mask, the router performs the same logical AND operation and adds the network command to the running configuration using the wildcard mask format. This is illustrated in the configuration below:

```
R1(config)#router eigrp 150
R1(config-router)#network 10.1.1.15 255.255.255.0
R1(config-router)#exit
```

Based on this configuration, the following is added to the current configuration on the router:

```
R1#show running-config | begin router eigrp
router eigrp 150
network 10.1.1.0 0.0.0.255
auto-summary
```

As illustrated in the configuration above, the use of either the wildcard mask or the subnet mask results in the same operation and `network` statement configuration in Cisco IOS software.



Real-World Implementation

When configuring EIGRP in production networks, it is common practice to use a wildcard mask of all zeros or a subnet mask of all 1s. For example, the `network 10.1.1.1 0.0.0.0` and `network 10.1.1.1 255.255.255.255` commands perform the same actions. Using all zeros in the wildcard mask or all ones in the subnet mask configures Cisco IOS software to match an exact interface address, regardless of the subnet mask configured on the interface itself. Either one of these commands would match interfaces configured with the 10.1.1.1/8, 10.1.1.1/16, 10.1.1.1/24, and 10.1.1.1/30 address, for example. The use of these commands is illustrated in the following output:

```
R1(config)#router eigrp 150
R1(config-router)#network 10.0.0.1 0.0.0.0
R1(config-router)#network 10.1.1.1 255.255.255.255
R1(config-router)#exit
```

https://t.me/learningnets

The `show ip protocols` command verifies that the configuration of both network statements is treated in a similar manner on the router, as illustrated below:

```
R1#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 150
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.1/32
    10.1.1.1/32
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

When a subnet mask with all ones or a wildcard mask with all zeros is used, EIGRP is enabled for the specified (matched) interface and the network the interface resides on is advertised. In other words, EIGRP will not advertise the /32 address in the output above but, instead, the actual network based on the subnet mask configured on the matched interface. The use of this configuration is independent of the subnet mask configured on the actual interface matched.

EIGRP Messages

This section describes the different types of messages used by EIGRP. However, before delving into the specifics of the different message types, it is important to have a solid understanding of the EIGRP packet header, wherein these messages are contained.

EIGRP Packet Header

Although going into specifics on the EIGRP packet formats is beyond the scope of the CCNA exam requirements, a fundamental understanding of the EIGRP packet header is important in order to understand completely the overall operation of the EIGRP routing protocol. Figure 36.1 below illustrates the format of the EIGRP packet header:

https://t.me/learningnets

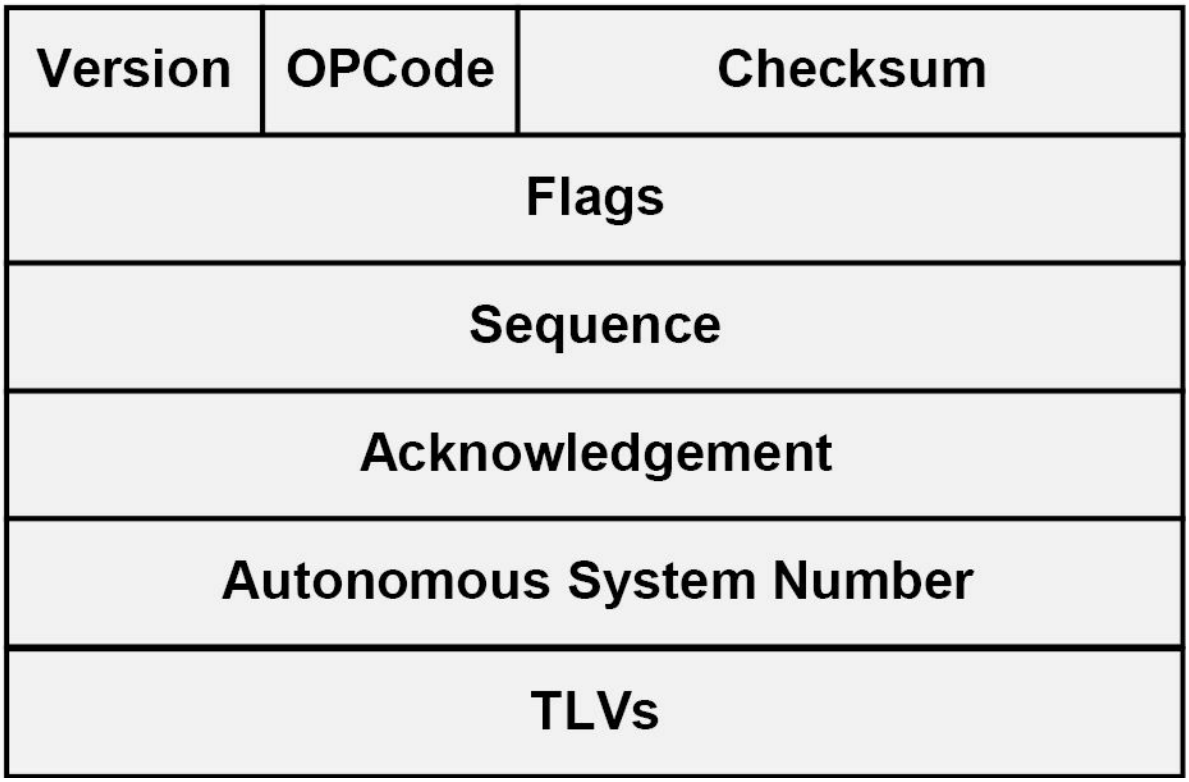


Figure 36.1 – EIGRP Packet Header Fields

Within the EIGRP packet header, the 4-bit Version field is used to indicate the protocol version. Current Cisco IOS images support EIGRP version 1.x. The 4-bit OPCode field specifies the EIGRP packet or message type. The different EIGRP packet types are each assigned a unique OPCode value, which allows them to be differentiated from other packet types. These messages will be described in detail later in this module.

The 24-bit Checksum field is used to run a sanity check on the EIGRP packet. This field is based on the entire EIGRP packet, excluding the IP header. The 32-bit Flags field is used to indicate an INIT either for a new EIGRP neighbour or for the Conditional Receive (CR) for EIGRP Reliable Transport Protocol (RTP). RTP and CR will be described in detail later in this module.

The 32-bit Sequence field specifies the sequence number used by EIGRP RTP to ensure orderly delivery of reliable packets. The 32-bit Acknowledgment field is used to acknowledge the receipt of an EIGRP reliable packet.

The 32-bit Autonomous System Number field specifies the ASN of the EIGRP domain. Finally, the 32-bit Type/Length/Value (TLV) triplet field is used to carry route entries and provides EIGRP DUAL information. EIGRP supports several different types of TLVs, with the most common being the following:

- The Parameters TLV, which has the parameters to establish neighbour relationships
- The Sequence TLV, which is used by RTP
- The Next Multicast Sequence TLV, which is used by RTP
- The EIGRP Internal Route TLV, which is used for internal EIGRP routes
- The EIGRP External Route TLV, which is used for external EIGRP routes

https://t.me/learningnets

NOTE: You are not required to go into detail on the different EIGRP TLVs.

Figure 36.2 below illustrates the different fields as they appear in a wire capture of an EIGRP packet:

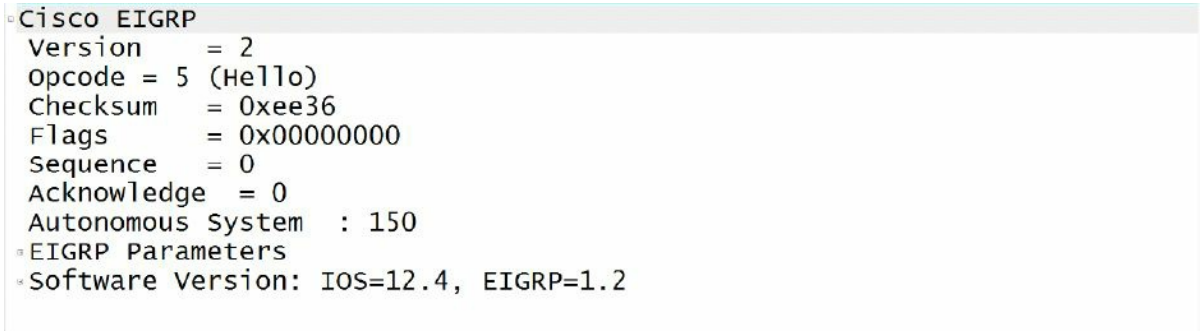


Figure 36.2 – EIGRP Packet Header Wire Capture

Within the EIGRP packet header, the 4-bit OPCode field is used to specify the EIGRP packet type or message. EIGRP uses different message or packet types, which are Hello packets, Acknowledgement packets, Update packets, Query packets, Reply packets, and Request packets. These packet types are described in detail in the following sections.

Hello Packets

Enhanced IGRP sends Hello packets once it has been enabled on a router for a particular network. These messages are used to identify neighbours and, once identified, serve or function as a keepalive mechanism between neighbours. EIGRP neighbour discovery and maintenance is described in detail later in this module.

Enhanced IGRP Hello packets are sent to the Link Local Multicast group address 224.0.0.10. Hello packets sent by EIGRP do not require an Acknowledgment to be sent confirming that they were received. Because they require no explicit acknowledgment, Hello packets are classified as unreliable EIGRP packets. EIGRP Hello packets have an OPCode of 5.

Acknowledgement Packets

An EIGRP Acknowledgment (ACK) packet is simply an EIGRP Hello packet that contains no data. Acknowledgement packets are used by EIGRP to confirm reliable delivery of EIGRP packets. The ACK packets are always sent to a Unicast address, which is the source address of the sender of the reliable packet, and not to the EIGRP Multicast group address. In addition, ACK packets will always contain a non-zero acknowledgment number. The ACK packet uses the same OPCode as the Hello packet because it is essentially a Hello packet that contains no information. The OPCode is 5.

Update Packets

Enhanced IGRP Update packets are used to convey reachability of destinations. In other words, Update packets contain EIGRP routing updates. When a new neighbour is discovered, Update packets are sent via Unicast so that the neighbour can build up its EIGRP topology table. In other cases, such as a link cost change, updates are sent via Multicast. It is important to know that Update packets are always transmitted reliably and always require explicit

https://t.me/learningnets

acknowledgement. Update packets are assigned an OPCode of 1. An EIGRP Update packet is illustrated in Figure 36.3 below:

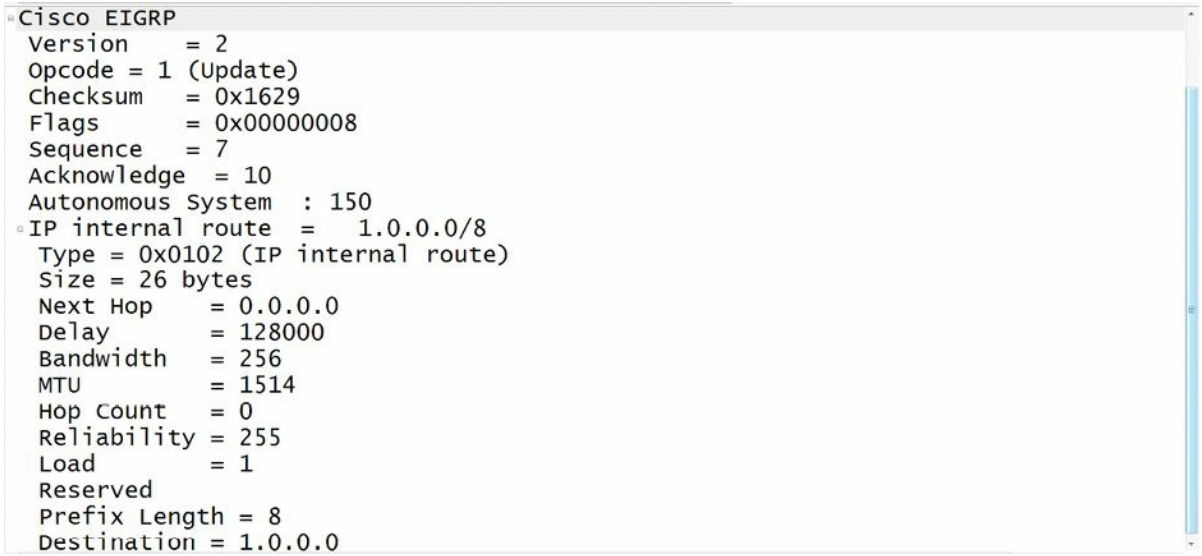


Figure 36.3 – EIGRP Update Packet

NOTE: You are not required to go into detail on the information contained in EIGRP packets.

Query Packets

Enhanced IGRP Query packets are Multicast and are used to request reliable routing information. EIGRP Query packets are sent to neighbours when a route is not available and the router needs to ask about the status of the route for fast convergence. If the router that sends out a Query does not receive a response from any of its neighbours, it resends the Query as a Unicast packet to the non-responsive neighbour(s). If no response is received in 16 attempts, the EIGRP neighbour relationship is reset. This concept will be described in further detail later in this module. EIGRP Query packets are assigned an OPCode of 3.

Reply Packets

Enhanced IGRP Reply packets are sent in response to Query packets. The Reply packets are used to respond reliably to a Query packet. Reply packets are Unicast to the originator of the Query. The EIGRP Reply packets are assigned an OPCode of 4.

Request Packets

Enhanced IGRP Request packets are used to get specific information from one or more neighbours and are used in route server applications. These packet types can be sent via either Multicast or Unicast but are always transmitted unreliably. In other words, they do not require an explicit acknowledgment.

NOTE: While EIGRP Hello and ACK packets have been described as two individual packet types, it is important to remember that in some texts, EIGRP Hello and ACK packets are considered the same type of packet. This is because, as was stated earlier in this section, an ACK packet is simply an EIGRP Hello packet that contains no data.

https://t.me/learningnets

The `debug eigrp packets` command may be used to print real-time debugging information on

the different EIGRP packets described in this section. Keep in mind that this command also includes additional packets that are not described, as they are beyond the scope of the current CCNA exam requirements. The following output illustrates the use of this command:

```
R1#debug eigrp packets ?
  SIAquery  EIGRP SIA-Query packets
  SIAreply  EIGRP SIA-Reply packets
  ack       EIGRP ack packets
  hello     EIGRP hello packets
  ipxsap    EIGRP ipxsap packets
  probe     EIGRP probe packets
  query     EIGRP query packets
  reply     EIGRP reply packets
  request   EIGRP request packets
  retry     EIGRP retransmissions
  stub      EIGRP stub packets
  terse     Display all EIGRP packets except Hellos
  update    EIGRP update packets
  verbose   Display all EIGRP packets
  <cr>
```

The `show ip eigrp traffic` command is used to view the number of EIGRP packets sent and received by the local router. This command is also a powerful troubleshooting tool. For example, if the routing is sending out Hello packets but is not receiving any back, this could indicate that the intended neighbour is not configured, or even that an ACK may be blocking EIGRP packets. The following output illustrates this command:

```
R2#show ip eigrp traffic
IP-EIGRP Traffic Statistics for AS 150
  Hellos sent/received: 21918/21922
  Updates sent/received: 10/6
  Queries sent/received: 1/0
  Replies sent/received: 0/1
  Acks sent/received: 6/10
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 178
  PDM Process ID: 154
  IP Socket queue:   0/2000/2/0 (current/max/highest/drops)
  Eigrp input queue: 0/2000/2/0 (current/max/highest/drops)
```

Table 36.1 summarises the EIGRP packets described in this section and whether they are sent unreliably or reliably:

https://t.me/learningnets

Table 36.1 – EIGRP Packet Summary

Message Type	Description	Sent
Hello	Used for neighbour discovery, maintenance, and keepalives	Unreliably
Acknowledgement	Used to acknowledge receipt of information	Unreliably
Update	Used to convey routing information	Reliably
Query	Used to request specific routing information	Reliably
Reply	Used to respond to a Query	Reliably
Request	Used to request information in route server applications	Unreliably

EIGRP Neighbour Discovery and Maintenance

Enhanced IGRP may be configured to discover neighbouring routers dynamically (default) or via manual administrator configuration. Both methods, as well as other EIGRP neighbour-related topics, will be described in the following sections.

Dynamic Neighbour Discovery

Dynamic neighbour discovery is performed by sending EIGRP Hello packets to the destination Multicast group address 224.0.0.10. This is performed as soon as the `network` command is issued when configuring EIGRP on the router. In addition, as stated earlier, EIGRP packets are sent directly over IP using protocol number 88. Figure 36.4 below illustrates the basic EIGRP neighbour discovery and route exchange process:

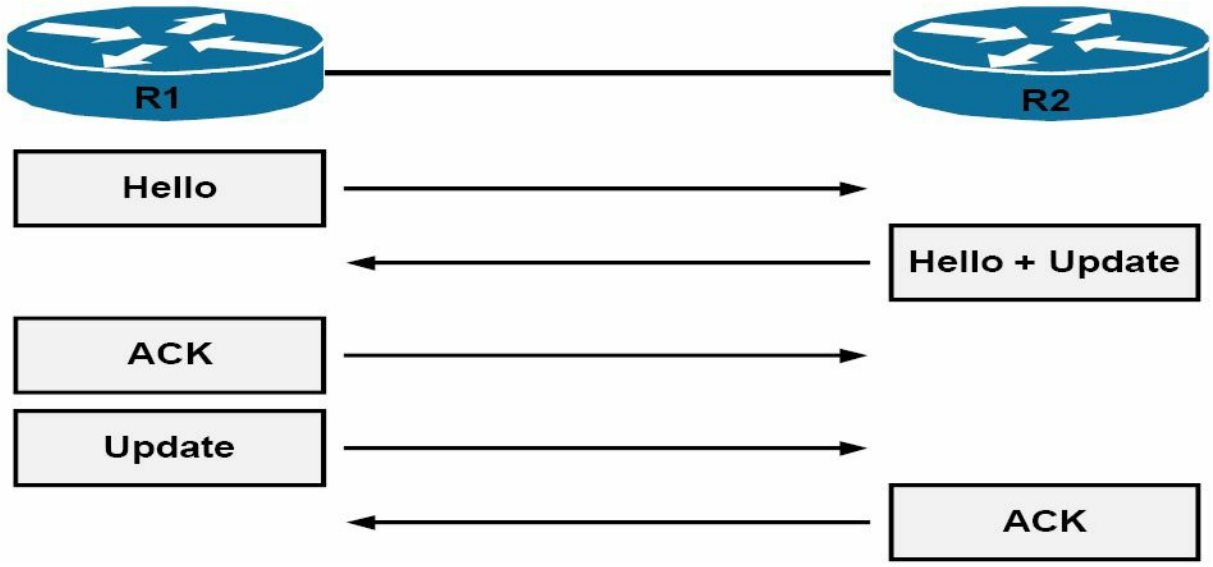


Figure 36.4 – EIGRP Neighbour Discovery and Route Exchange

Referencing Figure 36.4, upon initialisation, the EIGRP neighbours send Hello packets to discover other neighbours. The neighbours then exchange their full routing tables via full Updates. These Updates contain information about all known routes. Because Update packets are sent reliably, they must be explicitly acknowledged by the recipient.

After the neighbours have exchanged their routing information, they continue to exchange Hello packets to maintain the neighbour relationship. Additionally, the EIGRP neighbour routers will only send incremental updates to advise neighbours of status or routing changes. They will no longer send full Updates to neighbour routers.

https://t.me/learningnets

It is important to understand that simply enabling EIGRP between two or more routers does not guarantee that a neighbour relationship will be established. Instead, some parameters must match in order for the routers to become neighbours. The EIGRP neighbour relationship may not establish due to any of the following circumstances:

- Mismatched EIGRP authentication parameters (if configured)
- Mismatched EIGRP K values
- Mismatched EIGRP autonomous system number
- Using secondary addresses for EIGRP neighbour relationships
- The neighbours are not on a common subnet

While the `show ip eigrp neighbors` command does not differentiate between dynamically and statically configured neighbours, the `show ip eigrp interfaces detail <name>` command can be used to verify that the router interface is sending out Multicast packets to discover and maintain neighbour relationships. The output of this command on a router enabled for dynamic neighbour discovery is illustrated below:

```
R2#show ip eigrp interfaces detail FastEthernet0/0
IP-EIGRP interfaces for process 150
                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface      Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0            1        0/0        1        0/1           50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/2  Un/reliable ucasts: 2/2
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
  Retransmissions sent: 1  Out-of-sequence rcvd: 0
  Authentication mode is not set
  Use multicast
```

NOTE: The `show ip eigrp neighbors` command will be described in detail later. When looking at the output of the `show ip eigrp interfaces detail <name>` command, keep in mind that because EIGRP uses both Multicast and Unicast packets, the command counters will include values for both types of packets, as shown in the output above.

Static Neighbour Discovery

Unlike the dynamic EIGRP neighbour discovery process, static EIGRP neighbour relationships require manual neighbour configuration on the router. When static EIGRP neighbours are configured, the local router uses the Unicast neighbour address to send packets to these routers.

Static neighbour relationships are seldom used in EIGRP networks. The primary reason for this is the manual configuration of neighbours does not scale well in large networks. However, it is important to understand why this option is available in Cisco IOS software and the situations in

https://t.me/learningnets

which this feature can be utilised. A prime example of when static neighbour configuration could be used would be in a situation where EIGRP is being deployed across media that does not natively support Broadcast or Multicast packets, such as Frame Relay.

A second example would be to prevent sending unnecessary EIGRP packets on Multi-Access networks, such as Ethernet, when only a few EIGRP-enabled routers exist. In addition to basic EIGRP configuration, the `neighbor` command must be configured on the local router for all static EIGRP neighbours. EIGRP-enabled routers will not establish an adjacency if one router is configured to use Unicast (static) while another uses Multicast (dynamic).

In Cisco IOS software, static EIGRP neighbours are configured using the `neighbor <address> <interface>` router configuration command. Keep in mind that this is simply in addition to the basic EIGRP configuration. The simple network topology that is illustrated in Figure 36.5 below will be used both to demonstrate and to verify the configuration of static EIGRP neighbours:

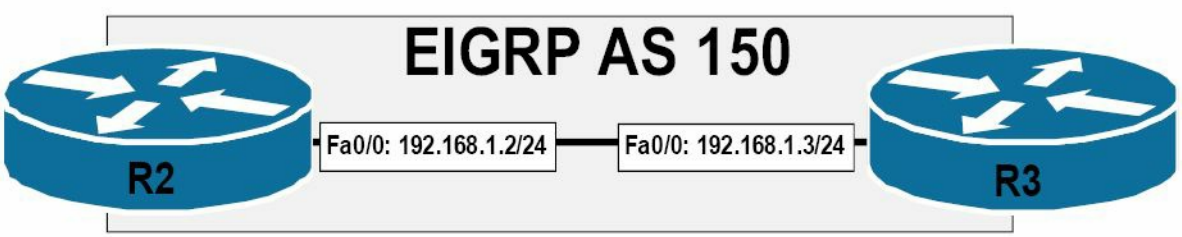


Figure 36.5 – Configuring Static EIGRP Neighbours

Referencing the topology illustrated in Figure 36.5, router R2 is configured as follows:

```
R2(config)#router eigrp 150
R2(config-router)#network 192.168.1.0 0.0.0.255
R2(config-router)#neighbor 192.168.1.3 FastEthernet0/0
R2(config-router)#no auto-summary
R2(config-router)#exit
```

The configuration implemented on router R3 is as follows:

```
R3(config)#router eigrp 150
R3(config-router)#network 192.168.1.0 0.0.0.255
R3(config-router)#neighbor 192.168.1.2 FastEthernet0/0
R3(config-router)#no auto-summary
R3(config-router)#exit
```

The `show ip eigrp interfaces detail <name>` command can be used to determine whether the router interface is sending Multicast (dynamic) or Unicast (static) packets for neighbour discovery and maintenance. This is illustrated in the following output:

```
R2#show ip eigrp interfaces detail FastEthernet0/0
IP-EIGRP interfaces for process 150
                    Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface      Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0            1        0/0        2        0/1           50           0
  Hello interval is 5 sec
```

https://t.me/learningnets

```
Next xmit serial <none>
Un/reliable mcasts: 0/1  Un/reliable ucasts: 3/8
Mcast exceptions: 1  CR packets: 1  ACKs suppressed: 2
Retransmissions sent: 1  Out-of-sequence rcvd: 0
Authentication mode is not set
Use unicast
```

Additionally, the `show ip eigrp neighbors [detail]` command can be used to determine the type of EIGRP neighbour. This command will be described in detail later in this module.

EIGRP Hello and Hold Timers

Enhanced IGRP uses different Hello and Hold timers for different types of media. Hello timers are used to determine the interval rate EIGRP Hello packets are sent. The Hold timer is used to determine the time that will elapse before a router considers an EIGRP neighbour as down. By default, the Hold time is three times the Hello interval.

Enhanced IGRP sends Hello packets every 5 seconds on Broadcast, Point-to-Point Serial, Point-to-Point subinterfaces, and Multipoint circuits greater than T1 speed. The default Hold time is 15 seconds. EIGRP sends Hello packets every 60 seconds on other link types. These include low-bandwidth WAN links less than T1 speed. The default Hold time for neighbour relationships across these links is also three times the Hello interval and therefore defaults to 180 seconds.

Enhanced IGRP timer values do not have to be the same on neighbouring routers in order for a neighbour relationship to be established. In addition, there is no mandatory requirement that the Hold time be three times the Hello interval. This is only a recommended guideline, which can be manually adjusted in Cisco IOS software. The EIGRP Hello time can be adjusted using the `ip hello-interval eigrp <ASN> <secs>` interface configuration command, while the EIGRP Hold time can be adjusted using the `ip hold-time eigrp <ASN> <secs>` interface configuration command.

It is important to understand the use of both Hello timers and Hold timers as they pertain to EIGRP. The Hold time value is advertised in the EIGRP Hello packet, while the Hello time value tells the local router how often to send its neighbour(s) Hello packets. The Hold time, on the other hand, tells the neighbour router(s) of the local router how long to wait before declaring the local router “dead.” The EIGRP Hello packet and the Hold Time field is illustrated in Figure 36.6 below:

https://t.me/learningnets

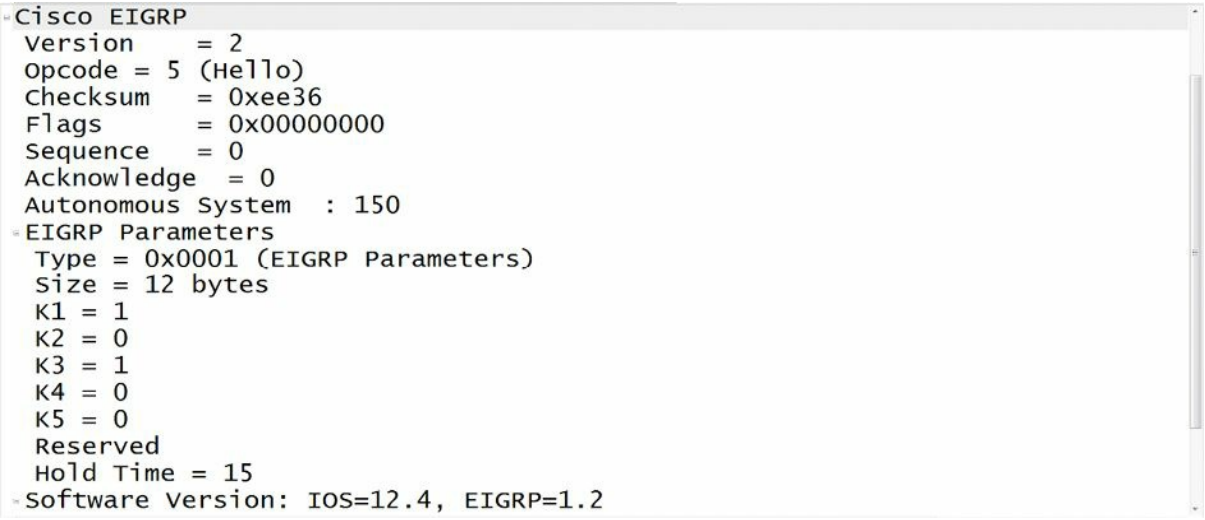


Figure 36.6 – EIGRP Hold Time in the EIGRP Hello Packet

Referencing Figure 36.6, the EIGRP Hello packet (OPCode 5) contains, among other things, the configured Hold time value. The value of 15 illustrated in Figure 36.6 is a non-default configured value implemented using the `ip hold-time eigrp <ASN> <secs>` interface configuration command. It is important to remember that the actual Hello time interval is not included. However, the configured Hello time can be viewed using the `show ip eigrp interfaces detail <name>` command. The information printed by this command is illustrated below:

```
R2#show ip eigrp interfaces detail FastEthernet0/0
IP-EIGRP interfaces for process 150
                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface      Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Fa0/0            1       0/0         7        0/1           50           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/1  Un/reliable ucasts: 2/5
  Mcast exceptions: 1  CR packets: 1  ACKs suppressed: 0
  Retransmissions sent: 1  Out-of-sequence rcvd: 0
  Authentication mode is not set
  Use multicast
```

The most common reason for adjusting the default EIGRP timer values is to speed up routing protocol convergence. For example, on a low-speed WAN link, a Hold time of 180 seconds might be a long time to wait before EIGRP declares a neighbour router down. Inversely, in some situations, it may be necessary to increase the EIGRP timer values on high-speed links in order to ensure a stable routing topology. This is common when implementing a solution for Stuck-In-Active (SIA) routes. SIA will be described in detail later in this module.

EIGRP Neighbour Table

The EIGRP neighbour table is used by routers running EIGRP to maintain state information about EIGRP neighbours. When newly discovered neighbours are learned, the address and interface of the neighbour is recorded. This is applicable to both dynamically discovered

https://t.me/learningnets

neighbours and statically defined neighbours. There is a single EIGRP neighbour table for each Protocol-Dependent Module (PDM).

When an EIGRP neighbour sends a Hello packet, it advertises a Hold time, which is the amount of time a router treats a neighbour as reachable and operational. After a router receives a Hello packet, the Hold time value begins to decrement and count down to zero. When another Hello packet is received, the Hold time value restarts from the beginning and the process is continually repeated. If a Hello packet is not received within the Hold time, then the Hold time expires (goes to 0). When the Hold time expires, DUAL is informed of the topology change and the neighbour is declared down by EIGRP. A message similar to the following is then printed and logged by the router:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.2 (Serial0/0) is down: holding time expired
```

The EIGRP neighbour table entry also includes information required by the Reliable Transport Protocol (RTP). RTP is used by EIGRP to ensure that Update, Query, and Reply packets are sent reliably. In addition, sequence numbers are also used to match acknowledgments with data packets. The last sequence number received from the neighbour is recorded in order to detect out-of-order packets. This ensures reliable packet delivery.

NOTE: RTP is described in detail later in this module.

The neighbour table includes a transmission list that is used to queue packets for possible retransmission on a per-neighbour basis. Additionally, round-trip timers are kept in the neighbour data structure to estimate an optimal retransmission interval. All of this information is printed in the output of the `show ip eigrp neighbors` command, as illustrated below:

```
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 150
H   Address      Interface  Hold   Uptime    SRTT   RTO   Q    Seq
                            (sec)            (ms)         Cnt  Num
0   192.168.1.3  Fa0/0      14     00:43:08  2      200   0    12
```

It is important to understand the information printed by this command, both as a basis for demonstrating competency on a core EIGRP component and for troubleshooting EIGRP issues. Table 36.2 below lists and describes the fields contained in the output of this command:

Table 36.2 – EIGRP Neighbour Table Fields

Field	Description
H	The list of neighbours in the order they are learned, starting at 0
Address	The IP address of the neighbour
Interface	The interface via which the neighbour is learned
Hold	The Hold timer for the neighbour; if it gets to 0, the neighbour is down
Uptime	Timer for how long the neighbour relationship has been up
SRTT	Smooth Round-Trip Time, which is the time it takes to send and receive a reliable EIGRP packet

https://t.me/learningnets

RTO	Retransmission Timeout, which is the amount of time the router will wait to retransmit the EIGRP reliable packet if an ACK is not received
Q Cnt	The number of EIGRP packets (Update, Query, and Reply) that the software is waiting to send
Sequence Number	The sequence number of the last EIGRP reliable packets being received from the neighbour to ensure that packets received from the neighbour are in order

While the `show ip eigrp neighbors` command prints out information on known EIGRP neighbours, it does not differentiate between dynamically discovered and manually configured neighbours. For example, the output of the `show ip eigrp neighbors` command on R2 indicates that the router has two EIGRP neighbour relationships. Based on this configuration, one is a statically configured neighbour, while the other is dynamically discovered. As you can see, it is not possible to determine which is which based on the following output:

```
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 150
H   Address         Interface  Hold  Uptime    SRTT   RTO   Q   Seq
                               (sec)           (ms)          Cnt Num
1   150.2.2.2       Se0/0      13    00:00:48  153    918   0   4
0   192.168.1.3     Fa0/0      10    08:33:23  1      200   0   20
```

In environments where the router has both dynamically discovered and manually configured neighbour relationships, the `show ip eigrp neighbors detail` command can be used to determine which neighbour is statically configured and which is dynamically discovered, as illustrated below:

```
R2#show ip eigrp neighbors detail
IP-EIGRP neighbors for process 150
H   Address       Interface   Hold  Uptime    SRTT   RTO   Q     Seq
                              (sec)           (ms)          Cnt   Num
1   150.2.2.2     Se0/0       11    00:04:22  153    918   0     4
   Version 12.3/1.2, Retrans: 0, Retries: 0, Prefixes: 1
0   192.168.1.3   Fa0/0       10    08:36:58  1      200   0     20
   Static neighbor
   Version 12.4/1.2, Retrans: 0, Retries: 0, Prefixes: 1
```

Referencing the output above, neighbour 192.168.1.3 is a manually configured neighbour and neighbour 150.2.2.2 is a dynamically discovered neighbour. The static neighbours can also be viewed using the `show ip eigrp neighbors static <interface>` command, as illustrated below:

```
R2#show ip eigrp neighbors static FastEthernet0/0
IP-EIGRP neighbors for process 150
Static Address          Interface
192.168.1.3             FastEthernet0/0
```

Reliable Transport Protocol

https://t.me/learningnets

Enhanced IGRP needs its own transport protocol to ensure the reliable delivery of packets. RTP

is used by EIGRP to ensure that Update, Query, and Reply packets are sent reliably. The use of sequence numbers also ensures that the EIGRP packets are received in the correct order.

When reliable EIGRP packets are sent to a neighbour, the sending router expects an ACK from the receiving routers stating that the packet has been received. Using RTP, EIGRP maintains a transport window of one unacknowledged packet, which means that every single reliable packet that is sent out must be acknowledged before the next reliable packet can be sent. The sending router will retransmit the unacknowledged reliable packet until it receives an ACK.

It is important to note, however, that the unacknowledged packet will be retransmitted only up to 16 times. If there is still no acknowledgment after 16 retransmissions, EIGRP will reset the neighbour relationship. RTP uses both Multicast and Unicast packets. On Broadcast Multi-Access networks such as Ethernet, EIGRP uses Multicast packets instead of sending an individual packet (Unicast) to each router on the segment. However, packets may also be sent using Unicast if a response is not received from one or more of the neighbours on the Multi-Access segment. This is described referencing the diagram in Figure 36.7 below:

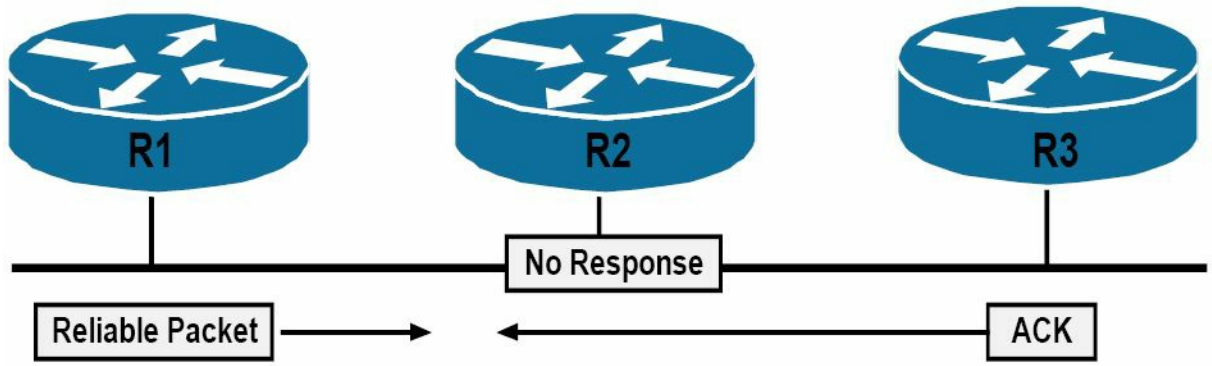


Figure 36.7 – EIGRP RTP Operation

In Figure 36.7, routers R1, R2, and R3 reside on a common subnet on the Multi-Access segment. Given the media, EIGRP will use Multicast to send reliable packets between the routers. Assume, for example, that R1 sends out a packet that requires acknowledgment to routers R2 and R3. R1 then waits for acknowledgement from R2 and R3 confirming receipt of this packet.

Assume that R3 responds but R2 is unable to respond to this packet. Given that EIGRP maintains a transport window of one unacknowledged packet, which means that every individual reliable packet that is sent out must be acknowledged explicitly by the neighbour router(s) before the next reliable packet can be sent, this presents a possible issue on the Multi-Access segment because R1 will not be able to send out packets until it has received the acknowledgment from R2. R3 is therefore indirectly affected by the issues on R2.

To avoid this potential pitfall, R1 will wait for the Multicast Flow Timer (MFT) on the Ethernet interface connected to the Multi-Access segment to expire. The MFT, or simply the Flow Timer, is the maximum amount of time that the sending router will wait for an ACK packet from a group member. When the timer expires, R1 will Multicast a special EIGRP packet called a Sequence TLV. This packet lists R2 (the offender) and indicates an out-of-sequence Multicast packet. Because R3 is not listed in this packet, it enters Conditional Receive (CR) mode and continues listening to Multicast packets. R1 uses Unicast to retransmit the packet to R2. The Retransmission Timeout (RTO) indicates the time that the router waits for an acknowledgement

https://t.me/learningnets

of that Unicast packet. If after 16 total attempts there is still no response from R2, then EIGRP will reset the neighbour.

NOTE: You are not required to go into any detail on MFT or RTO in the current CCNA exam.

Metrics, DUAL, and the Topology Table

When implementing EIGRP, it is important to understand the various aspects used within and by the protocol before routes are actually placed into the IP routing table. In this section, you will learn about the EIGRP composite metric and how it is calculated. You will also learn about the different ways to influence metric calculation, as well as to adjust the calculated metric.

Following that, you will learn about the Diffusing Update Algorithm (DUAL) and the EIGRP topology table. This section concludes with a discussion on how all this information meshes when it comes to populating the IP routing table on a router running EIGRP.

EIGRP Composite Metric Calculation

Enhanced IGRP uses a composite metric, which includes different variables referred to as the K values. The K values are constants that are used to distribute weight to different path aspects, which may be included in the composite EIGRP metric. The default values for the K values are K1 = K3 = 1 and K2 = K4 = K5 = 0. In other words, K1 and K3 are set to a default value of 1, while K2, K4, and K5 are set to a default value of 0.

Assuming the default K value settings, the complete EIGRP metric can be calculated using the following mathematical formula:

[K1 * bandwidth + (K2 * bandwidth) / (256 - load) + K3 * delay] * [K5 / (reliability + K4)]

However, given that only K1 and K3 have any positive values by default, the default EIGRP metric calculation is performed using the following mathematical formula:

$[(10^7 / \text{least bandwidth on path}) + (\text{sum of all delays})] \times 256$

This essentially means that, by default, EIGRP uses the minimum bandwidth on the path to a destination network and the total cumulative delay to compute routing metrics. However, Cisco IOS software allows administrators to set other K values to non-zero values to incorporate other variables into the composite metric. This may be performed using the `metric weights [tos] k1 k2 k3 k4 k5` router configuration command.

When using the `metric weights` command, `[tos]` stands for Type of Service. Although Cisco IOS software shows that any value between 0 and 8 may be used, as of the time this guide was written, this field can currently be set only to zero. The K values can be set to any value between 0 and 255. The default EIGRP K values can be viewed by issuing the `show ip protocols` command. This is illustrated in the following output:

```
R2#show ip protocols

Routing Protocol is "eigrp 150"

  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
```

https://t.me/learningnets

```
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 150
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.3           90      00:00:15
  Distance: internal 90 external 170
```

When adjusting the EIGRP K values, it is important to remember that the same values must be configured on all routers within the EIGRP domain. If the K values are mismatched, EIGRP neighbour relationships will not be established.

NOTE: Adjusting the default K value settings is not recommended. It should be done only with the assistance of seasoned senior-level engineers who have a solid understanding of the implications of such actions within the network or based upon the recommendation of the Cisco Technical Assistance Centre (TAC).

Using Interface Bandwidth to Influence EIGRP Metric Calculation

Enhanced IGRP metric calculation can be directly influenced by adjusting the default bandwidth values assigned to individual interfaces using the `bandwidth` command. The bandwidth values specified by this command are in Kilobits. The bandwidth used in EIGRP metric calculation is also in Kilobits. Figure 36.8 below illustrates a network comprised of two routers connected via two Serial (T1) links that have a bandwidth value of 1544Kbps:

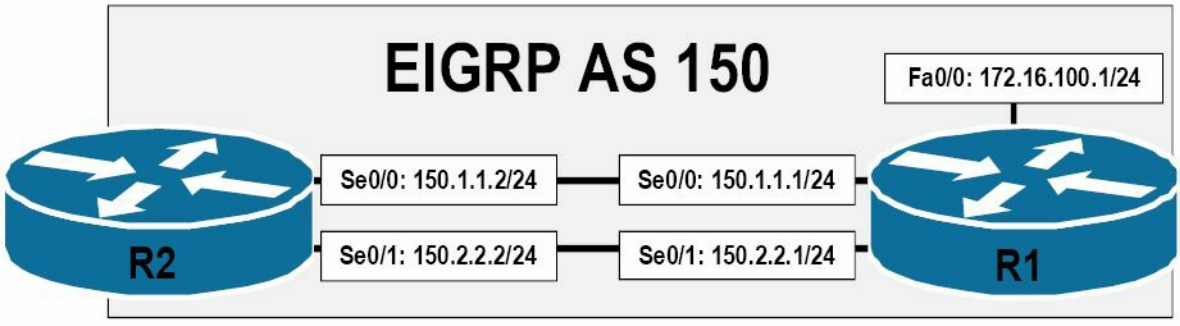


Figure 36.8 – EIGRP Metric Bandwidth Manipulation

Referencing the diagram in Figure 36.8, because of the equal bandwidth (and delay) values of the links between R1 and R2, the same EIGRP metric will be derived for both paths from R2 to the 172.16.100.0/24 subnet. EIGRP will load-share traffic between the two Serial links, as illustrated in the following output on R2:

https://t.me/learningnets

```
R2#show ip route 172.16.100.0 255.255.255.0
Routing entry for 172.16.100.0/24
  Known via "eigrp 150", distance 90, metric 2172416, type internal
  Redistributing via eigrp 150
  Last update from 150.2.2.1 on Serial0/1, 00:48:09 ago
  Routing Descriptor Blocks:
    150.2.2.1, from 150.2.2.1, 00:48:09 ago, via Serial0/1
      Route metric is 2172416, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
  * 150.1.1.1, from 150.1.1.1, 00:48:09 ago, via Serial0/0
      Route metric is 2172416, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

Adjusting the default bandwidth value on either interface will directly influence the EIGRP metric calculation for the path to the destination network. Such actions can be used for path control within larger networks (i.e., controlling the path that traffic takes based on administrator-defined values and configurations). For example, if it was preferred that EIGRP use Serial0/0 as the primary path to the destination network and Serial0/1 as the backup path to the destination, one of two actions could be taken.

The first is that the bandwidth value on Serial0/0 could be incremented, resulting in a better (lower) metric for this path. The second is that the bandwidth value on Serial0/1 could be decremented, resulting in a worse (higher) metric for this path. Either option is acceptable and will achieve the desired result. The following output illustrates how to decrement the default bandwidth value on Serial0/1, effectively ensuring that Serial0/0 is used as the primary path between R2 and the 172.16.100.0/24 network:

```
R2(config)#interface Serial0/1
R2(config-if)#bandwidth 1024
R2(config-if)#exit
```

NOTE: As stated in Day 1, this configuration does not mean that Serial0/1 is now capable of only 1024Kbps of throughput through this interface.

The result of this configuration is that Serial0/0 is the primary path used by R2 to get to the 172.16.100.0/24 destination network. This is illustrated in the following output:

```
R2#show ip route 172.16.100.0 255.255.255.0
Routing entry for 172.16.100.0/24
  Known via "eigrp 150", distance 90, metric 2172416, type internal
  Redistributing via eigrp 150
```

https://t.me/learningnets

```
Last update from 150.1.1.1 on Serial0/0, 00:01:55 ago
Routing Descriptor Blocks:
* 150.1.1.1, from 150.1.1.1, 00:01:55 ago, via Serial0/0
    Route metric is 2172416, traffic share count is 1
    Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 1
```

NOTE: The asterisk (*) points to the interface over which the next packet is sent. In the event that there are multiple equal-cost routes in the routing table, the position of the * rotates among the equal-cost paths.

Although the path via the Serial0/1 interface is not installed into the routing table, when using EIGRP as the routing protocol, it is important to remember that this path is not completely ignored. Instead, this path is stored in the EIGRP topology table, which contains the primary and alternate (backup) paths to remote destination networks. The EIGRP topology table will be described in detail later in this module.

NOTE: By default, when EIGRP is enabled, it can use up to 50% of the interface bandwidth to send EIGRP packets (EIGRP is a very chatty protocol, so it limits itself in possible bandwidth usage). EIGRP determines the bandwidth amount based on the `bandwidth` interface configuration command. Therefore, when adjusting interface bandwidth values, it is important to keep this fact in mind. This default setting can be adjusted by using the `ip bandwidth-percent eigrp [ASN] [percentage]` interface configuration command.

In summation, when using the bandwidth command to influence EIGRP metric calculation, it is important to remember that EIGRP uses the minimum bandwidth on the path to a destination network, along with the cumulative delay, to compute routing metrics. It is important to have a solid understanding of the network topology to best determine where to use the bandwidth command to influence EIGRP metric calculation. In the real world, however, delay is the preferred method of influencing EIGRP metrics.

Using Interface Delay to Influence EIGRP Metric Calculation

The interface delay value is presented in microseconds. The delay value used in EIGRP metric calculation is in tens of microseconds. Therefore, the delay value on the interface must be divided by 10 in order to compute the EIGRP metric. Table 36.3 below shows the default interface bandwidth and delay values used in Cisco IOS software:

Table 36.3 – Default Interface Bandwidth and Delay Values

Interface	Bandwidth (Kilobits)	Delay (Microseconds)
Ethernet	10000	1000
FastEthernet	100000	100
GigabitEthernet	1000000	10
Ten-GigabitEthernet	10000000	10
Serial (T1)	1544	20000

https://t.me/learningnets

Serial (E1)	2048	20000
Serial (T3)	44736	200
Serial (E3)	34010	200

When working with the interface bandwidth and delay values, it is very important to remember that adjusting the interface bandwidth value does not automatically adjust the interface delay value, and vice-versa. The two values are independent of each other. As an example, the output that follows shows the default bandwidth and delay values for a FastEthernet interface:

```
R2#show interfaces FastEthernet0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0013.1986.0a20 (bia 0013.1986.0a20)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
...
[Truncated Output]
```

To reinforce this concept, the bandwidth value on the FastEthernet interface is adjusted to 1544Kbps using the `bandwidth` interface configuration command, as follows:

```
R2(config)#interface FastEthernet0/0
R2(config-if)#bandwidth 1544
R2(config-if)#exit
```

While the bandwidth value now displayed in the output of the `show interfaces` command reflects the implemented configuration, the default interface delay value remains the same, as illustrated below:

```
R2#show interfaces FastEthernet0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0013.1986.0a20 (bia 0013.1986.0a20)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

The cumulative delay used by EIGRP is the sum of all interface delays between the source and the destination network. Changing any of the delay values in the path influences EIGRP metric calculation. The interface delay value is adjusted using the `delay` interface configuration command. This value is then divided by 10 when used in EIGRP metric calculation. Figure 36.9 below illustrates a network comprised of two routers connected via two Serial (T1) links that have a bandwidth value of 1544Kbps and a default delay of 20000 microseconds. In addition, the 172.16.100.0/24 network is directly connected to a FastEthernet interface, which has a default bandwidth of 100000Kbps and a default delay value of 100 microseconds:

https://t.me/learningnets

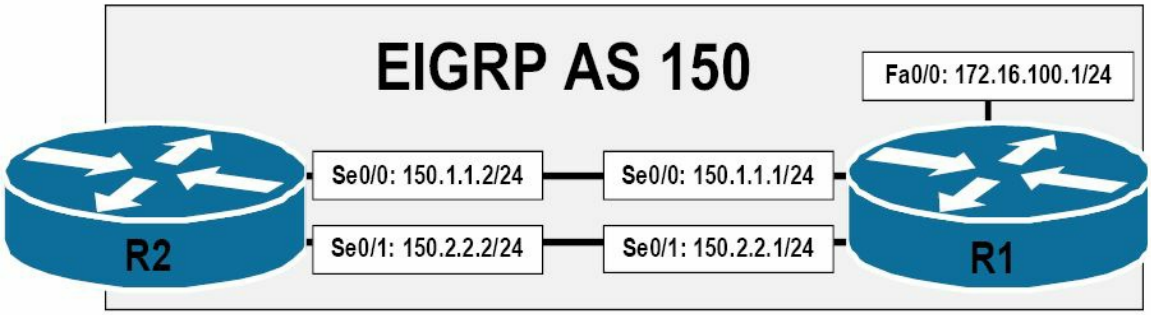


Figure 36.9 – EIGRP Metric Delay Manipulation

The EIGRP metric from R2 to the 172.16.100.0/24 network is calculated as follows:

Metric = [(10^7 / least bandwidth on path) + (sum of all delays)] × 256

Metric = [(10000000 / 1544) + (2000 + 10)] × 256

NOTE: Remember to divide the interface delay values by 10 for EIGRP metric calculation.

Metric = [(10000000 / 1544) + (2000 + 10)] × 256

NOTE: The calculated value should always be rounded down to the nearest integer.

Metric = [6476 + 2010] × 256

Metric = 8486 × 256

Metric = 2172416

This calculation can be verified by the `show ip route` command, as follows:

```
R2#show ip route 172.16.100.0 255.255.255.0
Routing entry for 172.16.100.0/24
  Known via "eigrp 150", distance 90, metric 2172416, type internal
  Redistributing via eigrp 150
  Last update from 150.2.2.1 on Serial0/1, 00:03:28 ago
  Routing Descriptor Blocks:
    150.2.2.1, from 150.2.2.1, 00:03:28 ago, via Serial0/1
      Route metric is 2172416, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
  * 150.1.1.1, from 150.1.1.1, 00:03:28 ago, via Serial0/0
      Route metric is 2172416, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

https://t.me/learningnets

As with the `bandwidth` command, you can either increment or decrement the interface delay value using the `delay` command to influence EIGRP metric calculation. For example, to configure R2 to use the Serial0/0 link to get to the 172.16.100.0/24 network, with Serial0/1 being used as a backup link only, the delay value on Serial0/0 could be decremented as follows:

```
R2(config)#int s0/0
R2(config-if)#delay 100
R2(config-if)#exit
```

This configuration adjusts the EIGRP metric for the path via Serial0/0, as illustrated below:

```
R2#show ip route 172.16.100.0 255.255.255.0
Routing entry for 172.16.100.0/24
  Known via "eigrp 150", distance 90, metric 1686016, type internal
  Redistributing via eigrp 150
  Last update from 150.1.1.1 on Serial0/0, 00:01:09 ago
  Routing Descriptor Blocks:
  * 150.1.1.1, from 150.1.1.1, 00:01:09 ago, via Serial0/0
      Route metric is 1686016, traffic share count is 1
      Total delay is 1100 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

The path via Serial0/1 is retained in the topology table as an alternate path to the network.

The Diffusing Update Algorithm (DUAL)

The Diffusing Update Algorithm is at the crux of the EIGRP routing protocol. DUAL looks at all routes received from neighbour routers, compares them, and then selects the lowest metric (best) loop-free path to the destination network, which is the Feasible Distance (FD), resulting in the Successor route. The FD includes both the metric of a network as advertised by the connected neighbour plus the cost of reaching that particular neighbour.

The metric that is advertised by the neighbour router is referred to as the Reported Distance (RD) or as the Advertised Distance (AD) to the destination network. Therefore, the FD includes the RD plus the cost of reaching that particular neighbour. The next-hop router for the Successor route is referred to as the Successor. The Successor route is placed into the IP routing table and the EIGRP topology table and points to the Successor.

Any other routes to the same destination network that have a lower RD than the FD of the Successor path are guaranteed to be loop-free and are referred to as Feasible Successor (FS) routes. These routes are not placed into the IP routing table; however, they are still placed into the EIGRP topology table, along with the Successor routes.

In order for a route to become an FS route, it must meet the Feasibility Condition (FC), which occurs only when the RD to the destination network is less than the FD. In the event that the RD is more than the FD, the route is not selected as an FS. This is used by EIGRP to prevent the possibility of loops. The network topology illustrated in Figure 36.10 below will be used to

https://t.me/learningnets

clarify the terminology referred to in this section:

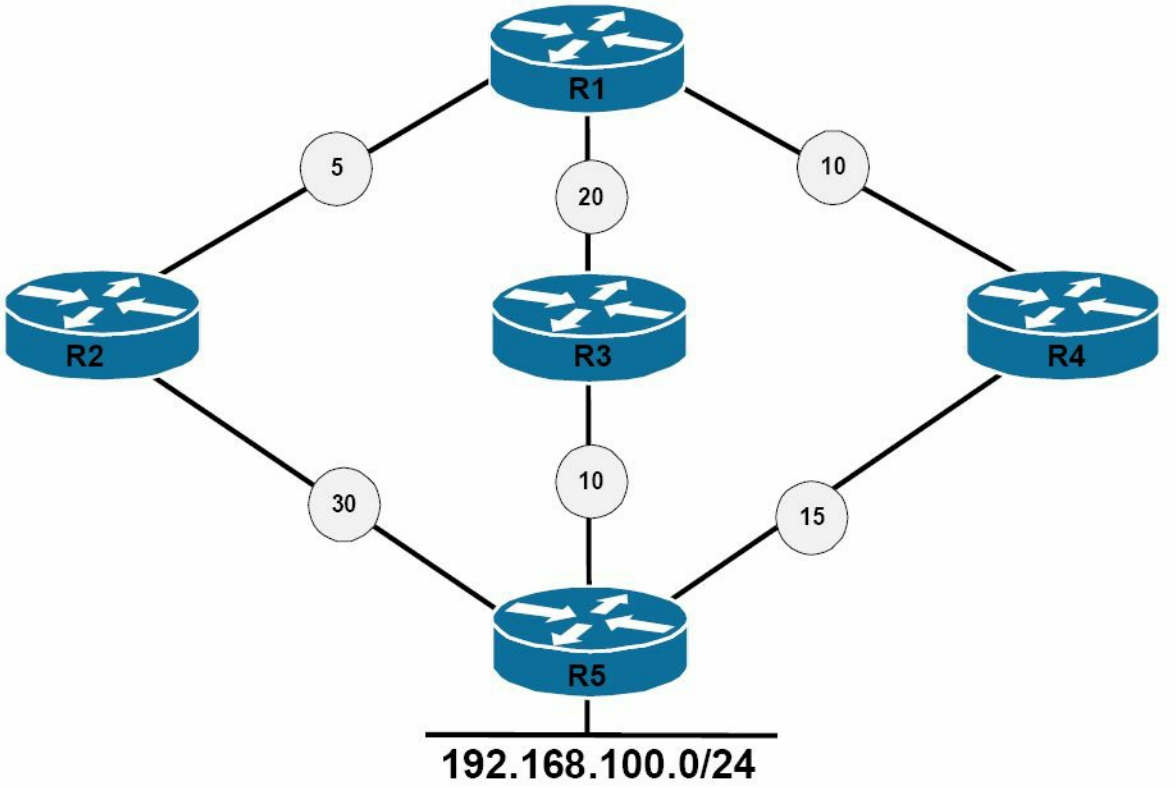


Figure 36.10. – Understanding the Diffusing Update Algorithm

Referencing Figure 36.10, Table 36.4 below shows the Feasible Distance and the Reported Distance values as seen on R1 for the 192.168.100.0/24 network:

Table 36.4 – R1 Paths and Distances

Network Path	R1 Neighbour	Neighbour Metric (RD)	R1 Feasible Distance
R1 – R2 – R5	R2	30	35
R1 – R3 – R5	R3	10	30
R1 – R4 – R5	R4	15	25

Based on the information in Table 36.4, R1 will select the path through R4 as the Successor route based on the FD for the route, which is 25. This route will be placed into the IP routing table as well as the EIGRP topology table. R1 then looks at alternate paths to the 192.168.100.0/24 network. The metric for neighbour R3 to the 192.168.100.0/24 network, also referred to as the RD or AD, is 10. This is less than the FD and so this route meets the FC and is placed into the EIGRP topology table. The metric for neighbour R2 to the 192.168.100.0/24 network is 30. This value is higher than the FD of 25. This route does not meet the FC and is not considered an FS. The route, however, is still placed into the EIGRP topology table. This is illustrated in the section on the EIGRP topology table that follows.

When a neighbour changes a metric, or when a topology change occurs, and the Successor route is removed or changes, DUAL checks for FSs for the route and if one is found, then DUAL uses it to avoid re-computing the route unnecessarily. This is referred to as local computation. Performing a local computation saves CPU power because the FS has been chosen and already exists before the Successor or primary route fails.

https://t.me/learningnets

When no FS for the destination network exists, the local router will send a Query to neighbouring routers asking if they have information on the destination network. If the information is available and another neighbour does have a route to the destination network, then the router performs a diffusing computation to determine a new Successor.

The EIGRP Topology Table

The EIGRP topology table is populated by EIGRP PDMs acted upon by the DUAL Finite State Machine. All known destination networks and subnets that are advertised by neighbouring EIGRP routers are stored in the EIGRP topology table. This includes Successor routes, FS routes, and even routes that have not met the FC.

The topology table allows all EIGRP routers to have a consistent view of the entire network. It also allows for rapid convergence in EIGRP networks. Each individual entry in the topology table contains the destination network and the neighbour(s) that have advertised the destination network. Both the FD and the RD are stored in the topology table. The EIGRP topology table contains the information needed to build a set of distances and vectors to each reachable network, including the following:

- The lowest bandwidth on the path to the destination network
- The total or cumulative delay to the destination network
- The reliability of the path to the destination network
- The loading of the path to the destination network
- The minimum Maximum Transmission Unit (MTU) to the destination network
- The Feasible Distance to the destination network
- The Reported Distance by the neighbour router to the destination network
- The route source (only external routes) of the destination network

NOTE: While the MTU is included in the topology table, EIGRP does not use this value in actual metric computation. Instead, the MTU is simply tracked to determine the minimum value to the destination network. The interface MTU specifies the largest size of datagram that can be transferred across a certain link without the need for fragmentation, or breaking the datagram or packet into smaller pieces.

The contents of the EIGRP topology table are viewed using the `show ip eigrp topology` command. The options that are available with this command are illustrated below:

```
R2#show ip eigrp topology ?
  <1-65535>       AS Number
  A.B.C.D         IP prefix <network>/<length>, e.g., 192.168.0.0/16
  A.B.C.D         Network to display information about
  active          Show only active entries
  all-links       Show all links in topology table
  detail-links    Show all links in topology table
```

https://t.me/learningnets

```
  pending          Show only entries pending transmission
  summary          Show a summary of the topology table
  zero-successors  Show only zero successor entries
  |                Output modifiers
  <cr>
```

The `show ip eigrp topology` command with no options prints only the Successor and Feasible Successor information for routes in the topology table and for all of the EIGRP instances enabled on the router. The output printed by this command is illustrated below:

```
R2#show ip eigrp topology
IP-EIGRP Topology Table for AS(150)/ID(2.2.2.2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 150.2.2.0/24, 1 successors, FD is 20512000
        via Connected, Serial0/1
        via 150.1.1.1 (2195456/2169856), Serial0/0
P 150.1.1.0/24, 1 successors, FD is 1683456
        via Connected, Serial0/0
P 172.16.100.0/24, 1 successors, FD is 1686016
        via 150.1.1.1 (1686016/28160), Serial0/0
```

The `show ip eigrp topology [network]/[prefix]` and `show ip eigrp topology [network] [mask]` commands print Successor routes, FS routes, and routes that have not met the FC for the route specified in either command. The following illustrates the use of the `show ip eigrp topology [network]/[prefix]` command:

```
R2#show ip eigrp topology 172.16.100.0/24
IP-EIGRP (AS 150): Topology entry for 172.16.100.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 1686016
  Routing Descriptor Blocks:
  150.1.1.1 (Serial0/0), from 150.1.1.1, Send flag is 0x0
      Composite metric is (1686016/28160), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 1100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
  150.2.2.1 (Serial0/1), from 150.2.2.1, Send flag is 0x0
      Composite metric is (2167998207/2147511807), Route is Internal
      Vector metric:
        Minimum bandwidth is 128 Kbit
```

https://t.me/learningnets

```
        Total delay is 83906179 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```

In the output above, you can see that the path via Serial0/1 does not meet the FC because the RD exceeds the FD. This is why the path is not printed in the output of the `show ip eigrp topology` command. Instead of viewing each prefix on an individual basis to determine Successor routes, FS routes, and routes that did not meet the FC, you can use the `show ip eigrp topology all-links` command to view all possible routes for all of the prefixes in the EIGRP topology table. The output of this command is illustrated below:

```
R2#show ip eigrp topology all-links
IP-EIGRP Topology Table for AS(150)/ID(2.2.2.2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 150.2.2.0/24, 1 successors, FD is 20512000, serno 42
        via Connected, Serial0/1
        via 150.1.1.1 (2195456/2169856), Serial0/0
P 150.1.1.0/24, 1 successors, FD is 1683456, serno 32
        via Connected, Serial0/0
        via 150.2.2.1 (21024000/2169856), Serial0/1
P 172.16.100.0/24, 1 successors, FD is 1686016, serno 47
        via 150.1.1.1 (1686016/28160), Serial0/0
        via 150.2.2.1 (2167998207/2147511807), Serial0/1
```

Within the EIGRP topology table, entries may be marked either as Passive (P) or as Active (A). A route in the Passive state indicates that EIGRP has completed actively computing the metric for the route and traffic can be forwarded to the destination network using the Successor route. This is the preferred state for all routes in the topology table.

Enhanced IGRP routes are in an Active state when the Successor route has been lost and the router sends out a Query packet to determine an FS. Usually, an FS is present and EIGRP promotes that to the Successor route. This way, the router converges without involving other routers in the network. This process is referred to as a local computation.

However, if the Successor route has been lost or removed, and there is no FS, then the router will begin diffused computation. In diffused computation, EIGRP will send a Query out to all neighbours and out of all interfaces, except for the interface to the Successor route. When an EIGRP neighbour receives a Query for a route, and if that neighbour's EIGRP topology table does not contain an entry for the route, then the neighbour immediately replies to the Query with an unreachable message, stating that there is no path for this route through this neighbour.

If the EIGRP topology table on the neighbour lists the router sending the Query as the

https://t.me/learningnets

Successor for that route, and an FS exists, then the FS is installed and the router replies to the neighbour Query that it has a route to the lost destination network.

However, if the EIGRP topology table lists the router sending the Query as the Successor for this route and there is no FS, then the router queries all of its EIGRP neighbours, except those that were sent out of the same interface as its former Successor. The router will not reply to the Query until it has received a Reply to all Queries that it originated for this route.

Finally, if the Query was received from a neighbour that is not the Successor for this destination, then the router replies with its own Successor information. If the neighbouring routers do not have the lost route information, then Queries are sent from those neighbouring routers to their neighbouring routers until the Query boundary is reached. The Query boundary is either the end of the network, the distribute list boundary, or the summarisation boundary.

Once the Query has been sent, the EIGRP router must wait for all replies to be received before it calculates the Successor route. If any neighbour has not replied within three minutes, the route is said to be Stuck-in-Active (SIA). When a route is SIA, the neighbour relationship of the router(s) that did not respond to the Query will be reset. In such cases, you will see a message logged by the router similar to the following:

```
%DUAL-5-NBRCHANGE: IP-EIGRP 150:
    Neighbor 150.1.1.1(Serial0/0) is down: stuck in active
%DUAL-3-SIA:
    Route 172.16.100.0/24 stuck-in-active state in IP-EIGRP 150.
Cleaning up
```

There are several reasons why the EIGRP neighbour router(s) may not respond to the Query, which include the following:

- The neighbour router's CPU is overloaded and it cannot respond in time
- The neighbour router itself has no information about the lost route
- Quality issues on the circuit are causing packets to be lost
- Low-bandwidth links are congested and packets are being delayed

To prevent SIA issues due to delayed responses from other EIGRP neighbours, the local router can be configured to wait for longer than the default of three minutes to receive responses back to its Query packets using the `timers active-time` command in Router Configuration mode.

NOTE: It is important to note that if you change this default parameter on one EIGRP router in your network, you must change it on all the other routers within your EIGRP routing domain.

Equal Cost and Unequal Cost Load Sharing

Cisco IOS software supports equal cost load sharing for a default of up to four paths for all routing protocols. This is illustrated below in the output of the `show ip protocols` command:

https://t.me/learningnets

```
R2#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 150
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    150.1.1.2/32
    150.2.2.2/32
  Routing Information Sources:
    Gateway         Distance      Last Update
    Gateway         Distance      Last Update
    150.2.2.1            90      00:00:52
    150.1.1.1            90      00:00:52
  Distance: internal 90 external 170
```

The `maximum-paths <1-6>` router configuration command can be used to change the default value of four maximum paths up to a maximum of six equal cost paths. When performing equal cost load balancing, the router distributes the load evenly among all paths. The traffic share count identifies the number of outgoing packets on each path. When performing equal cost load balancing, one packet is sent on each individual path, as illustrated in the following output:

```
R2#show ip route 172.16.100.0 255.255.255.0
Routing entry for 172.16.100.0/24
  Known via "eigrp 150", distance 90, metric 2172416, type internal
  Redistributing via eigrp 150
  Last update from 150.2.2.1 on Serial0/1, 00:04:00 ago
  Routing Descriptor Blocks:
    150.2.2.1, from 150.2.2.1, 00:04:00 ago, via Serial0/1
      Route metric is 2172416, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
  * 150.1.1.1, from 150.1.1.1, 00:04:00 ago, via Serial0/0
```

https://t.me/learningnets

```
    Route metric is 2172416, traffic share count is 1
    Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 1
```

In addition to equal cost load balancing capabilities, EIGRP is also able to perform unequal cost load sharing. This unique ability allows EIGRP to use unequal cost paths to send outgoing packets to the destination network based on weighted traffic share values. Unequal cost load sharing is enabled using the `variance <multiplier>` router configuration command.

The `<multiplier>` keyword is an integer between 1 and 128. A multiplier of 1, which is the default, implies that no unequal cost load sharing is being performed. This default setting is illustrated below in the output of the `show ip protocols` command:

```
R2#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 150
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    150.1.1.2/32
    150.2.2.2/32
  Routing Information Sources:
    Gateway         Distance      Last Update
    150.2.2.1              90      00:00:52
    150.1.1.1              90      00:00:52
  Distance: internal 90 external 170
```

The multiplier is a variable integer that tells the router to load share across routes that have a metric that is less than the minimum metric multiplied by the multiplier. For example, specifying a variance of 5 instructs the router to load share across routes whose metric is less than 5 times the minimum metric. The default variance of 1 tells the router to perform equal cost load balancing. When the variance command is used and a value other than 1 is specified as the multiplier, the router will distribute traffic among the routes proportionately, with respect to the metric of each individual route. In other words, the router will send more traffic using those paths with lower metric values than those with higher metric values.

https://t.me/learningnets

Figure 36.11 below illustrates a basic network running EIGRP. R1 and R2 are connected via back-to-back Serial links. The 150.1.1.0/24 link between the two routers has a bandwidth of 1024Kbps. The 150.2.2.0/24 link between the routers has a bandwidth of 768Kbps. R1 is advertising the 172.16.100.0/24 prefix via EIGRP to R2:

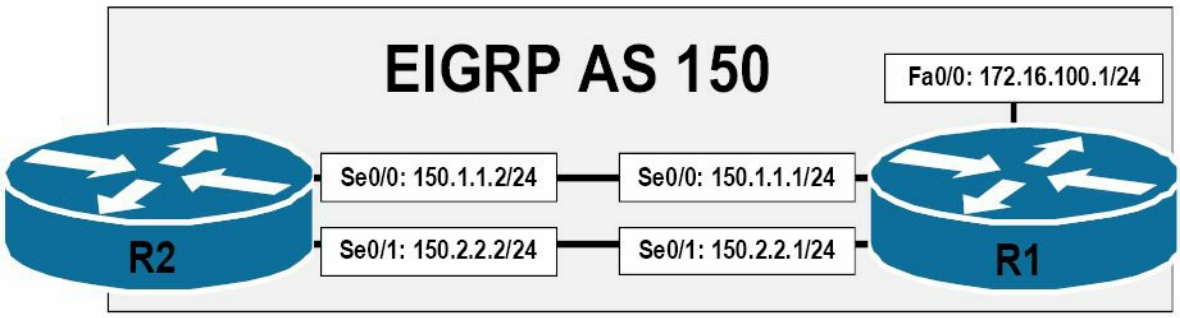


Figure 36.11 – Understanding EIGRP Variance

Based on the topology illustrated in Figure 36.11, the routing table on R2 for the 172.16.100.0/24 prefix is shown in the following output:

```
R2#show ip route 172.16.100.0 255.255.255.0
Routing entry for 172.16.100.0/24
  Known via "eigrp 150", distance 90, metric 3014400, type internal
  Redistributing via eigrp 150
  Last update from 150.1.1.1 on Serial0/0, 00:00:11 ago
  Routing Descriptor Blocks:
  * 150.1.1.1, from 150.1.1.1, 00:00:11 ago, via Serial0/0
      Route metric is 3014400, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 1024 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

The following EIGRP topology table shows both the Successor and the Feasible Successor routes:

```
R2#show ip eigrp topology 172.16.100.0 255.255.255.0
IP-EIGRP (AS 150): Topology entry for 172.16.100.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 3014400
  Routing Descriptor Blocks:
  150.1.1.1 (Serial0/0), from 150.1.1.1, Send flag is 0x0
      Composite metric is (3014400/28160), Route is Internal
      Vector metric:
        Minimum bandwidth is 1024 Kbit
        Total delay is 20100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```

https://t.me/learningnets

```
  150.2.2.1 (Serial0/1), from 150.2.2.1, Send flag is 0x0
      Composite metric is (3847680/28160), Route is Internal
      Vector metric:
        Minimum bandwidth is 768 Kbit
        Total delay is 20100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```

To determine the variance value to configure on the router, you can use the following formula:

Variance = Highest metric for the paths being considered / Metric for the best route

Using this formula, you can calculate the variance value to configure on R2 as follows:

Variance = Highest metric for the paths being considered / Metric for the best route

Variance = 3847680 / 3014400

Variance = 1.28

This value must then be rounded up to the nearest whole integer, which in this case is 2. Given this, R2 can be configured to perform unequal cost load sharing by implementing the following configuration in Router Configuration mode:

```
R2(config)#router eigrp 150
R2(config-router)#variance 2
R2(config-router)#exit
```

Following this configuration, the routing table entry for 172.16.100.0/24 is illustrated below:

```
R2#show ip route 172.16.100.0 255.255.255.0
Routing entry for 172.16.100.0/24
  Known via "eigrp 150", distance 90, metric 3014400, type internal
  Redistributing via eigrp 150
  Last update from 150.2.2.1 on Serial0/1, 00:00:36 ago
  Routing Descriptor Blocks:
    150.2.2.1, from 150.2.2.1, 00:00:36 ago, via Serial0/1
      Route metric is 3847680, traffic share count is 47
      Total delay is 20100 microseconds, minimum bandwidth is 768 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
  * 150.1.1.1, from 150.1.1.1, 00:00:36 ago, via Serial0/0
      Route metric is 3014400, traffic share count is 60
      Total delay is 20100 microseconds, minimum bandwidth is 1024 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

https://t.me/learningnets

The traffic share count indicates that for every 60 packets forwarded via Serial0/0, the router will forward 47 packets via Serial0/1. This is performed proportionally in respect to the route metric of either path. This is the default behaviour when the `variance` command is implemented. This intelligent traffic sharing functionality is enabled via the `traffic-share balanced` router configuration command, which requires no explicit configuration.

NOTE: The `traffic-share balanced` command is enabled by default and does not appear in the running configuration, even if manually configured. This is illustrated below:

```
R2(config)#router eigrp 150
R2(config-router)#vari 2
R2(config-router)#traffic-share balanced
R2(config-router)#exit
R2(config)#do show run | begin router
router eigrp 150
variance 2
network 150.1.1.2 0.0.0.0
network 150.2.2.2 0.0.0.0
no auto-summary
```

As stated previously in this section, when the `variance` command is used, all paths that both meet the Feasibility Condition and have a metric that is less than the minimum metric multiplied by the multiplier will be installed into the routing table. The router will then use all paths and load share traffic proportionally based on the route metric.

In some cases, you may want to allow alternate routes, such as the Feasible Successor route, to be placed into the routing table but not be used unless the Successor route is removed. Such actions are typically performed to reduce convergence times in EIGRP-enabled networks. To understand this concept, recall that, by default, the router only places the Successor route into the IP routing table. In the event that the Successor route is no longer available, the Feasible Successor route is promoted to the Successor route. This route is then installed into the routing table as the primary path to the destination network.

The `traffic-share min across-interfaces` router configuration command can be used in conjunction with the `variance` command to install all routes that have a metric less than the minimum metric multiplied by the multiplier into the routing table, but use only the route with the minimum (best) metric to forward packets until that route becomes unavailable. The primary objective of this configuration is that in the event that the primary route is lost, the alternative route is already in the routing table and can be used immediately.

The following configuration example uses the topology shown in Figure 36.11 above to illustrate how to configure the router to place routes with a metric less than two times the minimum metric into the routing table, but use only the route with the lowest metric to actually forward packets:

```
R2(config)#router eigrp 150
```

https://t.me/learningnets

```
R2(config-router)#vari 2
R2(config-router)#traffic-share min across-interfaces
R2(config-router)#exit
```

This configuration results in the following output for 172.16.100.0/24 in the routing table:

```
R2#show ip route 172.16.100.0 255.255.255.0
Routing entry for 172.16.100.0/24
  Known via "eigrp 150", distance 90, metric 3014400, type internal
  Redistributing via eigrp 150
  Last update from 150.2.2.1 on Serial0/1, 00:09:01 ago
  Routing Descriptor Blocks:
    150.2.2.1, from 150.2.2.1, 00:09:01 ago, via Serial0/1
      Route metric is 3847680, traffic share count is 0
      Total delay is 20100 microseconds, minimum bandwidth is 768 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
  * 150.1.1.1, from 150.1.1.1, 00:09:01 ago, via Serial0/0
      Route metric is 3014400, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 1024 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

As is illustrated in the output above, the two different metric routes have been installed into the routing table based on the variance configuration. However, notice the traffic share count for the route via Serial0/1 is 0 while the traffic share count for the route via Serial0/0 is 1. This means that the router will not send any packets to 172.16.100.0/24 via Serial0/1, even though the route entry is installed into the routing table, until the path via Serial0/0 is no longer available.

Default Routing Using EIGRP

Enhanced IGRP supports numerous ways to advertise dynamically the gateway or network of last resort to other routers within the routing domain. A gateway of last resort, or default route, is a method for the router to direct traffic when the destination network is not specifically listed in the routing table. These methods are as follows:

- Using the `ip default-network` command
- Using the `network` command to advertise network 0.0.0.0/0
- Redistributing the default static route
- Using the `ip summary-address eigrp [asn] [network] [mask]` command

The use of the `ip default-network` command is considered a legacy method of advertising the default route dynamically using EIGRP. However, because it is still supported in current IOS software versions, it is worth mentioning.

https://t.me/learningnets

The `ip default-network` configuration command flags a network as the default network by inserting an asterisk (*) next to the network in the routing table. Traffic for destinations to which there is no specific routing table entry is then forwarded by the router to this network. The implementation of this feature is illustrated referencing the EIGRP topology in Figure 36.12 below:

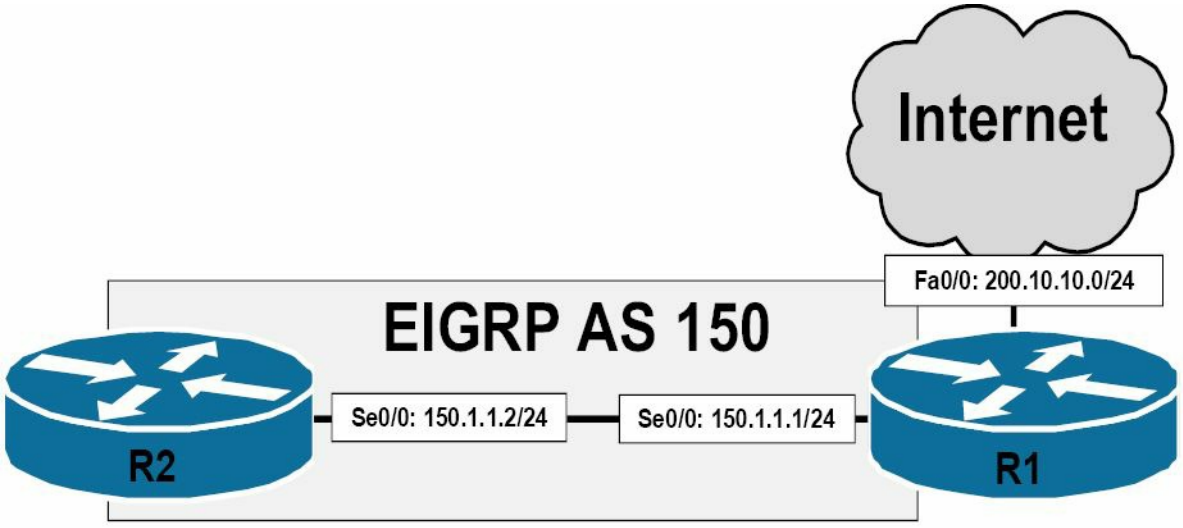


Figure 36.12 – EIGRP Default Routing

Referencing Figure 36.12, assume that the 200.10.10.0/24 subnet is connected to the Internet. This subnet resides off the FastEthernet0/0 interface of R1. R1 and R2 are in turn connected via a back-to-back Serial connection. Both routers reside in EIGRP AS 150. To flag the 200.10.10.0/24 network as the network of last resort, the following configuration is implemented on R1:

```
R1(config)#router eigrp 150
R1(config-router)#network 200.10.10.0 0.0.0.255
R1(config-router)#exit
R1(config)#ip default-network 200.10.10.0
R1(config)#exit
```

Based on this configuration, R2 receives 200.10.10.0/24 as the network of last resort, as follows:

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 150.2.2.1 to network 200.10.10.0
D*   200.10.10.0/24 [90/2172416] via 150.2.2.1, 00:01:03, Serial0/0
     150.1.0.0/24 is subnetted, 1 subnets
C       150.1.1.0 is directly connected, Serial0/0
```

https://t.me/learningnets

The `network` command can be used to advertise an existing static default route point to either a physical or a logical interface, typically the Null0 interface.

NOTE: The Null0 interface is a virtual interface on the router that discards all traffic that is routed to it. If you have a static route pointing to Null0, all traffic destined for the network specified in the static route is simply discarded. Think of the Null0 interface as a black hole: packets enter, but none ever leaves. It is essentially a bit-bucket on the router.

Referencing the diagram in Figure 36.12 above, the use of the `network` command in conjunction with an existing default static route is illustrated in the following configuration on R1:

```
R1(config)#ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
R1(config)#router eigrp 150
R1(config-router)#network 0.0.0.0
R1(config-router)#exit
```

Based on this configuration, the IP routing table on R2 is illustrated in the following output:

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 150.1.1.1 to network 0.0.0.0
D    200.10.10.0/24 [90/2172416] via 150.1.1.1, 00:01:11, Serial0/0
     150.1.0.0/24 is subnetted, 1 subnets
C       150.1.1.0 is directly connected, Serial0/0
D*   0.0.0.0/0 [90/2172416] via 150.1.1.1, 00:00:43, Serial0/0
```

Although route redistribution isn't part of the CCNA exam, it will be outlined here. This is the third method of advertising a default route via EIGRP. To redistribute the existing static default route into EIGRP, use the `redistribute static metric [bandwidth] [delay] [reliability] [load] [MTU]` router configuration command. The same network topology used for the previous outputs in this section will be used to illustrate the implementation of this method, as illustrated in Figure 36.13 below:

https://t.me/learningnets

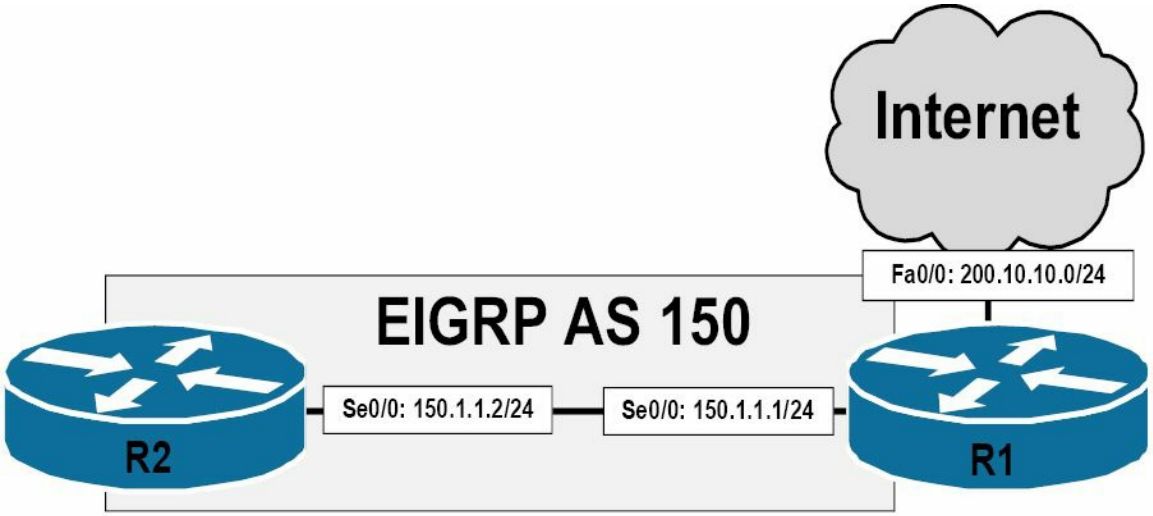


Figure 36.13 – EIGRP Default Routing (Continued)

Referencing Figure 36.13, which is the same as Figure 36.12, the following is performed on R1:

```
R1(config)#ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
R1(config)#router eigrp 150
R1(config-router)#redistribute static metric 100000 100 255 1 1500
R1(config-router)#exit
```

NOTE: The values used in the metric can be derived from the interface, or you can specify any values that you want when using this command.

Based on this configuration, the routing table on R2 is illustrated below:

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 150.1.1.1 to network 0.0.0.0
     150.1.0.0/24 is subnetted, 1 subnets
C       150.1.1.0 is directly connected, Serial0/0
D*EX 0.0.0.0/0 [170/2195456] via 150.1.1.1, 00:01:16, Serial0/0
```

Because the route was redistributed into EIGRP on R1, it is an external EIGRP route, as reflected in the output above. For external routes, the EIGRP topology table includes information such as the router that originated the route, the protocol the route was received for, and the metric of the external route, for example. This is illustrated in the following output:

```
R2#show ip eigrp topology 0.0.0.0/0
IP-EIGRP (AS 150): Topology entry for 0.0.0.0/0
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2195456
```

https://t.me/learningnets

```
  Routing Descriptor Blocks:
  150.1.1.1 (Serial0/0), from 150.1.1.1, Send flag is 0x0
      Composite metric is (2195456/51200), Route is External
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 21000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 1.1.1.1
        AS number of route is 0
        External protocol is Static, external metric is 0
        Administrator tag is 0 (0x00000000)
        Exterior flag is set
```

From the information in bold, you can see that the default route is a static route that was redistributed into EIGRP on R1. This route has a metric of 0. In addition, you can also see that the EIGRP router ID (RID) of R1 is 1.1.1.1.

The final method of advertising the default route is by using the `ip summary-address eigrp [asn] [network] [mask]` interface configuration command. EIGRP route summarisation will be described in detail later in this module. For the moment, concentrate on the use of this command to advertise the default route when using EIGRP.

Referencing the network topology diagram illustrated in Figure 36.13 above, R1 is configured with the `ip summary-address eigrp [asn] [network] [mask]` interface configuration command to advertise the default route to R2, as follows:

```
R1(config)#interface Serial0/0
R1(config-if)#description 'Back-to-Back Serial Connection To R2 Serial0/0'
R1(config-if)#ip summary-address eigrp 150 0.0.0.0 0.0.0.0
R1(config-if)#exit
```

The primary advantage to using this command is that a default route or network does not need to exist in the routing table in order for EIGRP to advertise network 0.0.0.0/0 to its neighbour routers. When this command is issued, the local router generates a summary route to the Null0 interface and flags the entry as the candidate default route. This is illustrated below:

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

https://t.me/learningnets

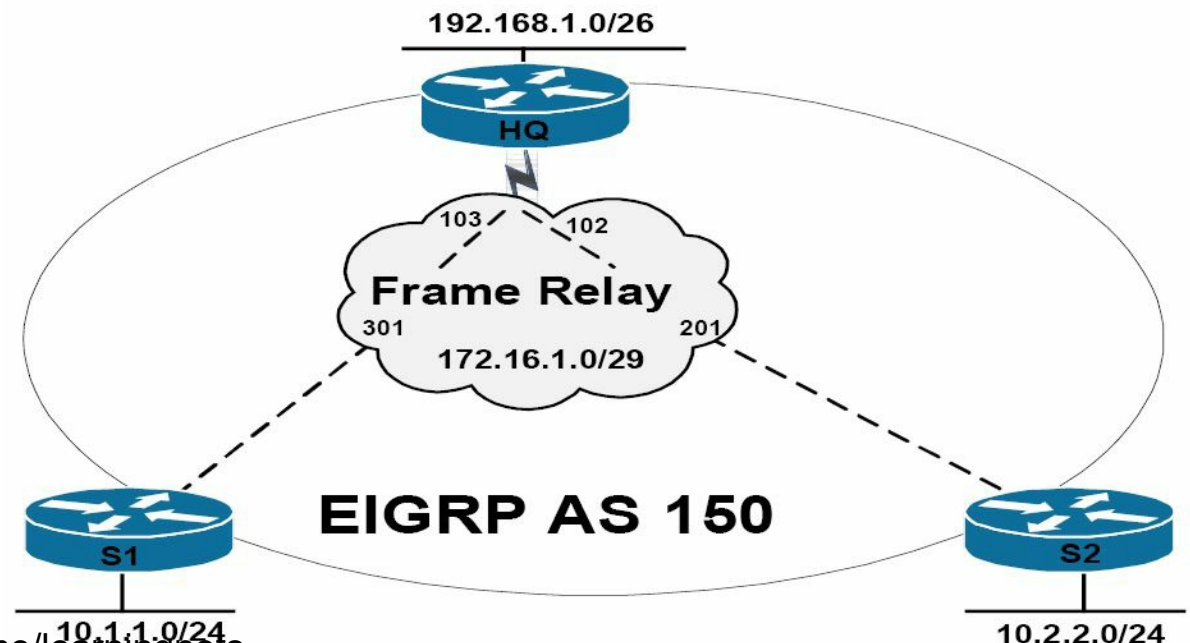
```
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
     150.1.0.0/24 is subnetted, 1 subnets
C       150.1.1.0 is directly connected, Serial0/0
D*   0.0.0.0/0 is a summary, 00:02:26, Null0
```

The summary route is received as an internal EIGRP route on R2, as illustrated below:

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 150.1.1.1 to network 0.0.0.0
     150.1.0.0/24 is subnetted, 1 subnets
C       150.1.1.0 is directly connected, Serial0/0
D*   0.0.0.0/0 [90/2297856] via 150.1.1.1, 00:03:07, Serial0/0
```

Split Horizon in EIGRP Networks

Previously, you learned that split horizon is a Distance Vector protocol feature mandating that routing information cannot be sent back out of the same interface through which it was received. This prevents the re-advertising of information back to the source from which it was learned. While this characteristic is a great loop prevention mechanism, it is also a significant drawback, especially in hub-and-spoke networks. To better understand the drawbacks of this feature, refer to the EIGRP hub-and-spoke network in Figure 36.14 below:



https://t.me/learningnets

Figure 36.14 – EIGRP Split Horizon

The topology in Figure 36.14 illustrates a classic hub-and-spoke network, with router HQ as the hub router and routers S1 and S2 as the two spoke routers. On the Frame Relay WAN, each spoke router has a single DLCI provisioned between itself and the HQ router in a partial-mesh topology. The Frame Relay configuration on the routers is verified as follows:

```
HQ#show frame-relay map
Serial0/0 (up): ip 172.16.1.2 dlci 102(0x66,0x1860), static,
              broadcast,
              CISCO, status defined, active
Serial0/0 (up): ip 172.16.1.1 dlci 103(0x67,0x1870), static,
              broadcast,
              CISCO, status defined, active
S1#show frame-relay map
Serial0/0 (up): ip 172.16.1.2 dlci 301(0x12D,0x48D0), static,
              broadcast,
              CISCO, status defined, active
Serial0/0 (up): ip 172.16.1.3 dlci 301(0x12D,0x48D0), static,
              broadcast,
              CISCO, status defined, active
S2#show frame-relay map
Serial0/0 (up): ip 172.16.1.1 dlci 201(0xC9,0x3090), static,
              broadcast,
              CISCO, status defined, active
Serial0/0 (up): ip 172.16.1.3 dlci 201(0xC9,0x3090), static,
              broadcast,
              CISCO, status defined, active
```

We will cover Frame Relay later on in the WAN section. Enhanced IGRP has been enabled on all three routers, using AS 150. The following output illustrates the EIGRP neighbour relationships between the HQ router and the spoke routers:

```
HQ#show ip eigrp neighbors
IP-EIGRP neighbors for process 150
H   Address         Interface     Hold  Uptime   SRTT  RTO  Q   Seq
                                 (sec)           (ms)       Cnt Num
1   172.16.1.1      Se0/0          165   00:01:07 24    200  0   2
0   172.16.1.2      Se0/0          153   00:01:25 124   744  0   2
```

The following output illustrates the EIGRP neighbour relationship between the first spoke router, S1, and the HQ router:

```
S1#show ip eigrp neighbors
IP-EIGRP neighbors for process 150
```

https://t.me/learningnets

```
H   Address         Interface     Hold  Uptime   SRTT RTO   Q   Seq
```

```
                                (sec)           (ms)       Cnt Num
0   172.16.1.3    Se0/0          128   00:00:53 911   5000  0   4
```

The following output illustrates the EIGRP neighbour relationship between the second spoke router, S2, and the HQ router:

```
S2#show ip eigrp neighbors
IP-EIGRP neighbors for process 150
H   Address       Interface     Hold   Uptime   SRTT  RTO  Q   Seq
                                (sec)           (ms)       Cnt Num
0   172.16.1.3    Se0/0          156    00:02:20 8     200  0   4
```

By default, EIGRP split horizon is enabled, which is undesirable in partial-mesh NBMA networks. This means that the HQ router will not advertise routing information learned on Serial0/0 out of the same interface. The effect of this default behaviour is that the HQ router will not advertise the 10.1.1.0/24 prefix received from S1 to S2 because the route is received via the Serial0/0 interface, and the split horizon feature prevents the router from advertising information learned on that interface back out onto the same interface. The same is also applicable for the 10.2.2.0/24 prefix the HQ router receives from S2.

This default behaviour means that while the HQ router is aware of both prefixes, the spoke routers have only partial routing tables. The routing table on the HQ router is as follows:

```
HQ#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2195456] via 172.16.1.1, 00:12:04, Serial0/0
D       10.2.2.0/24 [90/2195456] via 172.16.1.2, 00:12:06, Serial0/0
```

The routing table on spoke S1 is as follows:

```
S1#show ip route eigrp
     192.168.1.0/26 is subnetted, 1 subnets
D       192.168.1.0 [90/2195456] via 172.16.1.3, 00:10:53, Serial0/0
```

The routing table on spoke S2 is as follows:

```
S2#show ip route eigrp
     192.168.1.0/26 is subnetted, 1 subnets
D       192.168.1.0 [90/2195456] via 172.16.1.3, 00:10:55, Serial0/0
```

The result of this default behaviour is that while the HQ router will be able to reach both of the spoke router networks, neither spoke router will be able to reach the network of the other. There are several ways such a situation can be addressed and they are as follows:

- Disabling split horizon on the HQ (hub) router
- Advertising a default route from the HQ router to the spoke routers
- Manually configuring EIGRP neighbours on the routers

Disabling split horizon is performed at the interface level using the `no ip split-horizon eigrp [AS]` interface configuration command on the hub router. The command `show ip split-horizon`

https://t.me/learningnets

`interface_name` does not show the state of EIGRP split horizon as it does for RIP. To see if it is disabled, you have to examine the interface configuration section (i.e, `show run interface_name`). Referencing the network topology illustrated in Figure 36.14 above, this interface configuration command would be applied to the Serial0/0 interface on the HQ router. This is performed as follows:

```
HQ(config)#interface Serial0/0
HQ(config-if)#no ip split-horizon eigrp 150
```

After split horizon is disabled, the HQ router can advertise information back out onto the same interface on which it was received. For example, the routing table on spoke S2 now shows a routing entry for the 10.1.1.0/24 prefix advertised by spoke S1 to the HQ router:

```
S2#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2707456] via 172.16.1.3, 00:00:47, Serial0/0
     192.168.1.0/26 is subnetted, 1 subnets
D       192.168.1.0 [90/2195456] via 172.16.1.3, 00:00:47, Serial0/0
```

A simple ping test from spoke router S2 to the 10.1.1.0/24 subnet can be used to verify connectivity, as illustrated below:

```
S2#ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/27/32 ms
```

The second method of disabling split horizon is simply to advertise a default route from the HQ router to the spoke routers. In this situation, the `ip summary-address eigrp 150 0.0.0.0 0.0.0.0` interface configuration command could be applied to the Serial0/0 interface of the HQ router. This would allow the spoke routers to reach each other through the HQ router, which contains the full routing table, negating the need to disable split horizon.

The final alternative method of disabling split horizon is to configure manually EIGRP neighbour statements on all routers using the `neighbor` router configuration command. Because updates between neighbours are Unicast when this configuration is used, the split horizon limitation is removed. This option works well in small networks; however, as the network grows and the number of spoke routers increases, so does the configuration overhead.

Given that the configuration of both EIGRP default routing and static neighbours was described in detail in earlier sections in this module, the configuration of these features is omitted for brevity.

EIGRP Route Summarisation

Route summarisation reduces the amount of information that routers must process, which allows for faster convergence within the network. Summarisation also restricts the size of the area that is affected by network changes by hiding detailed topology information from certain

https://t.me/learningnets

areas within the network. Finally, as was stated earlier in this module, summarisation is used to define a Query boundary for EIGRP, which supports two types of route summarisation, as follows:

- Automatic route summarisation
- Manual route summarisation

By default, automatic route summarisation is in effect when EIGRP is enabled on the router. This is implemented using the `auto-summary` command. This command allows EIGRP to perform automatic route summarisation at classful boundaries. The operation of this default feature is illustrated referencing the network topology in Figure 36.15 below:

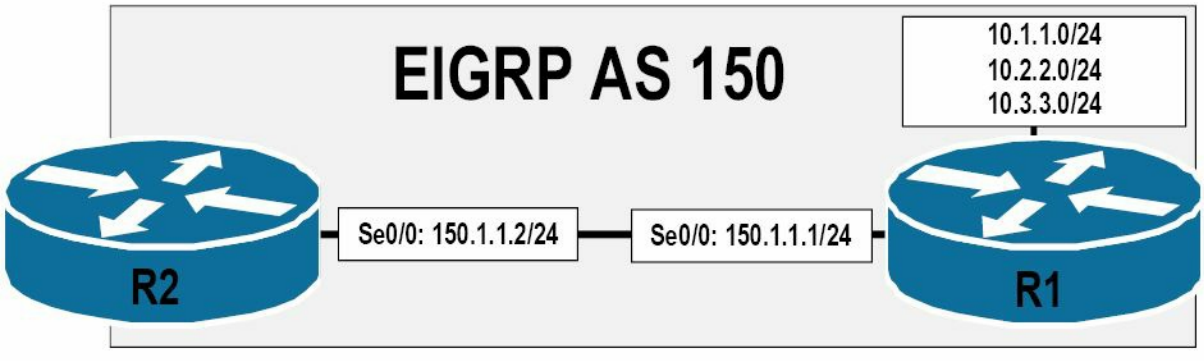


Figure 36.15 – EIGRP Automatic Route Summarisation

Referencing the EIGRP network illustrated in Figure 36.15, R1 and R2 are running EIGRP and are using autonomous system 150. The 10.1.1.0/24, 10.2.2.0/24, and 10.3.3.0/24 subnets are directly connected to R1. R1 is advertising these routes to R2. R1 and R2 are connected using a back-to-back Serial connection on the 150.1.1.0/24 subnet (which is a different major network than the 10.1.1.0/24, 10.2.2.0/24, and 10.3.3.0/24 subnets). Based on the networks connected to these routers, by default, EIGRP will perform automatic summarisation, as follows:

- The 10.1.1.0/24, 10.2.2.0/24, and 10.3.3.0/24 subnets will be summarised to 10.0.0.0/8
- The 150.1.1.0/24 subnet will be summarised to 150.1.0.0/16

This default behaviour can be validated by viewing the output of the `show ip protocols` command. The output of this command on R1 is illustrated below:

```
R1#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 150
  EIGRP NSF-aware route hold timer is 240s
```

https://t.me/learningnets

```
  Automatic network summarization is in effect
  Automatic address summarization:
    150.1.0.0/16 for Loopback1, Loopback2, Loopback3
      Summarizing with metric 2169856
    10.0.0.0/8 for Serial0/0
      Summarizing with metric 128256
  Maximum path: 4
  Routing for Networks:
    10.1.1.0/24
    10.2.2.0/24
    10.3.3.0/24
    150.1.1.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)          90      00:03:12
    150.1.1.2              90      00:03:12
  Distance: internal 90 external 170
```

In the output above, the 10.1.1.0/24, 10.2.2.0/24, and 10.3.3.0/24 subnets have been automatically summarised to 10.0.0.0/8. This summary address is advertised out of Serial0/0. The 150.1.1.0/24 subnet has been summarised to 150.1.0.0/16. This summary address is advertised out of Loopback1, Loopback2, and Loopback3. Remember, by default, EIGRP will send out updates on all interfaces for which EIGRP routing is enabled.

Referencing the output printed above, you can see that sending updates on a Loopback interface is a waste of resources because a device cannot be connected physically to a router Loopback interface listening for such updates. This default behaviour can be disabled by using the `passive-interface` router configuration command, as follows:

```
R1(config)#router eigrp 150
R1(config-router)#passive-interface Loopback1
R1(config-router)#passive-interface Loopback2
R1(config-router)#passive-interface Loopback3
R1(config-router)#exit
```

The result of this configuration is that EIGRP packets are no longer sent out of the Loopback interfaces. Therefore, as illustrated below, the summary address is not advertised out of these interfaces:

```
R1#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
```

https://t.me/learningnets

```
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 150
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Automatic address summarization:
    10.0.0.0/8 for Serial0/0
      Summarizing with metric 128256
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
    150.1.0.0
  Passive Interface(s):
    Loopback0
    Loopback1
    Loopback2
    Loopback3
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)          90      00:03:07
    150.1.1.2              90      00:01:12
  Distance: internal 90 external 170
```

NOTE: The `passive-interface` command is described in detail later in this module.

Continuing with automatic summarisation, following automatic summarisation at the classful boundary, EIGRP installs a route to the summary address into the EIGRP topology table and the IP routing table. The route is highlighted below in the EIGRP topology table, along with the more specific entries and their respective directly connected interfaces:

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(150)/ID(10.3.3.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.0.0.0/8, 1 successors, FD is 128256
        via Summary (128256/0), Null0
P 10.3.3.0/24, 1 successors, FD is 128256
        via Connected, Loopback3
P 10.2.2.0/24, 1 successors, FD is 128256
        via Connected, Loopback2
```

https://t.me/learningnets

```
P 10.1.1.0/24, 1 successors, FD is 128256
        via Connected, Loopback1
...
[Truncated Output]
```

In the routing table, the summary route is connected directly to the Null0 interface. The route has a default administrative distance value of 5. This is illustrated in the following output:

```
R1#show ip route 10.0.0.0 255.0.0.0
Routing entry for 10.0.0.0/8
  Known via "eigrp 150", distance 5, metric 128256, type internal
  Redistributing via eigrp 150
  Routing Descriptor Blocks:
  * directly connected, via Null0
      Route metric is 128256, traffic share count is 1
      Total delay is 5000 microseconds, minimum bandwidth is 10000000 Kbit
      Reliability 255/255, minimum MTU 1514 bytes
      Loading 1/255, Hops 0
```

When EIGRP performs automatic summarisation, the router advertises the summary route and suppresses the more specific routes. In other words, while the summary route is advertised, the more specific prefixes are suppressed in updates to EIGRP neighbours. This can be validated by looking at the routing table on R2, as illustrated below:

```
R2#show ip route eigrp
D    10.0.0.0/8 [90/2298856] via 150.1.1.1, 00:29:05, Serial0/0
```

This default behaviour works well in basic networks, such as the one illustrated in Figure 36.15 above. However, it can have an adverse impact in a discontiguous network, which comprises a major network that separates another major network, as illustrated in Figure 36.16 below:

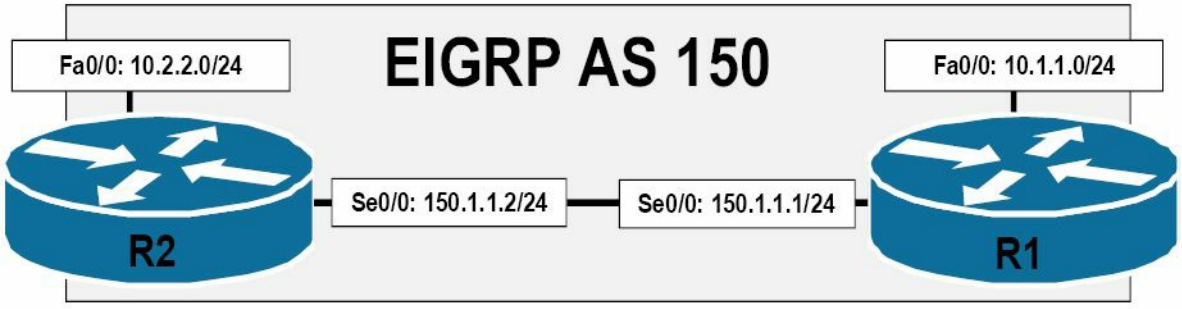


Figure 36.16 – Discontiguous Network

Referencing the diagram illustrated in Figure 36.16, the major 150.1.0.0/16 network separates the two major 10.0.0.0/8 networks. When automatic summarisation is enabled, both R1 and R2 will summarise the 10.1.1.0/24 and 10.2.2.0/24 subnets, respectively, to the 10.0.0.0/8 address. This summary route will be installed with a next-hop interface of Null0. The Null0 interface is a "bit-bucket." Any packets sent to this interface are effectively discarded.

Because both routers advertise to each other only the summary addresses, neither router will be able to reach the 10.*x.x.x*/24 subnet of the other router. To understand the ramifications of

https://t.me/learningnets

automatic summarisation in the network illustrated in Figure 36.16, let's go through the steps one at a time, beginning with the configuration on R1 and R2, which is as follows:

```
R1(config)#router eigrp 150
R1(config-router)#network 10.1.1.0 0.0.0.255
R1(config-router)#network 150.1.1.0 0.0.0.255
R1(config-router)#exit

R2(config)#router eigrp 150
R2(config-router)#network 10.2.2.0 0.0.0.255
R2(config-router)#network 150.1.1.0 0.0.0.255
R2(config-router)#exit
```

Because automatic summarisation at the classful boundary is enabled by default on both of the routers, they will both generate two summary addresses: one for 10.0.0.0/8 and another for 150.1.0.0/16. These summary addresses will both point to the Null0 interface, and the routing table on R1 will display the following entries:

```
R1#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:04:51, Null0
     150.1.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       150.1.0.0/16 is a summary, 00:06:22, Null0
```

Similarly, the routing table on R2 also reflects the same, as follows:

```
R2#show ip route eigrp
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:01:58, Null0
     150.1.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       150.1.0.0/16 is a summary, 00:01:58, Null0
```

Even though a summary address of 150.1.0.0/16 has been installed into the IP routing table, R1 and R2 are still able to ping each other because the more route-specific entry (150.1.1.0/24) resides on a directly connected interface. The more specific entries in a summary route can be viewed by issuing the `show ip route [address][mask] longer-prefixes` command. The output of this command is illustrated below for the 150.1.0.0/16 summary:

```
R1#show ip route 150.1.0.0 255.255.0.0 longer-prefixes
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
```

https://t.me/learningnets

```
     150.1.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       150.1.1.0/24 is directly connected, Serial0/0
D       150.1.0.0/16 is a summary, 00:10:29, Null0
```

Because the more specific 150.1.1.0/24 route entry exists, packets sent to the 150.1.1.2 address will be forwarded via the Serial0/0 interface. This allows connectivity between R1 and R2, as illustrated below:

```
R1#ping 150.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

However, packets to any other subnets of the major 150.1.0.0/16 network will be sent to the Null0 interface because no specific route entries exist.

So far, everything appears to be in order. You can see that due to the more specific route entry of the major 150.1.0.0/16 network, R1 and R2 are able to ping each other. The problem, however, is connectivity between the major 10.0.0.0/8 subnets on R1 and R2. Router R1 displays the following specific route entries for its generated 10.0.0.0/8 summary address:

```
R1#show ip route 10.0.0.0 255.0.0.0 longer-prefixes
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, FastEthernet0/0
D       10.0.0.0/8 is a summary, 00:14:23, Null0
```

Similarly, router R2 displays the following specific entries for its generated 10.0.0.0/8 summary:

```
R2#show ip route 10.0.0.0 255.0.0.0 longer-prefixes
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
```

https://t.me/learningnets

```
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

```
C       10.2.2.0/24 is directly connected, FastEthernet0/0
D       10.0.0.0/8 is a summary, 00:15:11, Null0
```

Neither router has a route to the other router's 10.*x.x.x*/24 subnet. If, for example, R1 attempts to send packets to 10.2.2.0/24, the summary address will be used and the packets will be forwarded to the Null0 interface. This is illustrated in the following output:

```
R1#show ip route 10.2.2.0
Routing entry for 10.0.0.0/8
  Known via "eigrp 150", distance 5, metric 28160, type internal
  Redistributing via eigrp 150
  Routing Descriptor Blocks:
  * directly connected, via Null0
      Route metric is 28160, traffic share count is 1
      Total delay is 100 microseconds, minimum bandwidth is 100000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 0
```

R1 will be unable to ping the 10.*x.x.x*/24 subnet on R2 and vice-versa, as illustrated below:

```
R1#ping 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Two solutions to this issue are as follows:

- Manually configure static routes for the 10.*x.x.x*/24 subnets on both routers
- Disable EIGRP automatic classful network summarisation

The first option is very basic. However, static route configuration is not scalable and requires a great deal of configuration overhead in large networks. The second option, which is also the recommended option, is both scalable and requires less configuration overhead than the first. Automatic summarisation is disabled by issuing the `no auto-summary` command (disabled by default in newer IOS releases), as illustrated below:

```
R1(config)#router eigrp 150
R1(config-router)#no auto-summary
R1(config-router)#exit

R2(config)#router eigrp 150
R2(config-router)#no auto-summary
R2(config-router)#exit
```

The result of this configuration is that the specific subnets of the major network are advertised by both routers. A summary route is not generated, as illustrated below:

https://t.me/learningnets

```
R2#show ip route eigrp
```

```
     10.0.0.0/24 is subnetted, 2 subnets
D       10.1.1.0 [90/2172416] via 150.1.1.1, 00:01:17, Serial0/0
```

IP connectivity between the 10.*x.x.x*/24 subnets can be validated using a simple ping, as illustrated below:

```
R2#ping 10.1.1.1 source 10.2.2.2 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.2.2.2
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/3/4 ms
```

Before we go into the details pertaining to manual route summarisation, it is important to know that EIGRP will not automatically summarise external networks unless there is an internal network that will be included in the summary. To better understand this concept, refer to Figure 36.17 below, which illustrates a basic EIGRP network:

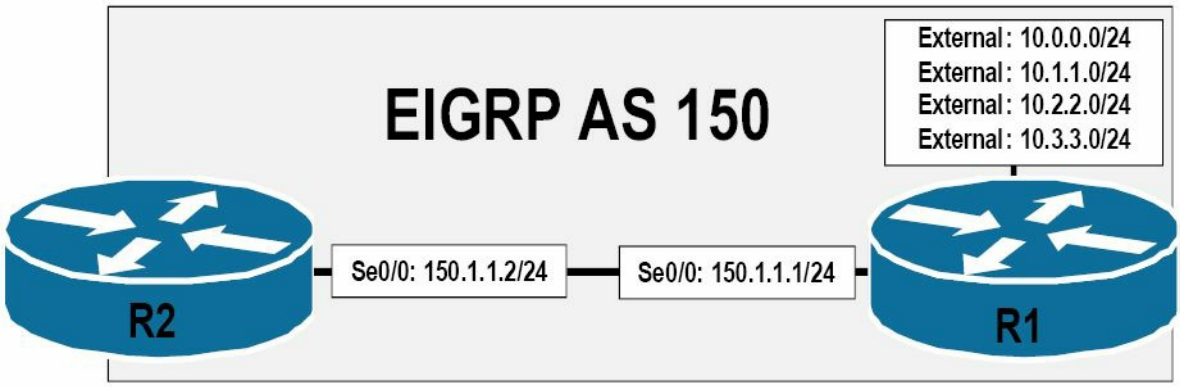


Figure 36.17 – Summarising External Networks

Referencing Figure 36.17, R1 is redistributing (which makes them external) and then advertising the 10.0.0.0/24, 10.1.1.0/24, 10.2.2.0/24, and 10.3.3.0/24 external networks via EIGRP. Automatic route summarisation is enabled on R1. The initial configuration on R1 is as follows:

```
R1(config)#router eigrp 150
R1(config-router)#redistribute connected metric 8000000 5000 255 1 1514
R1(config-router)#network 150.1.1.1 0.0.0.0
R1(config-router)#exit
```

The `show ip protocols` command shows that EIGRP is enabled for Serial0/0 and is redistributing connected networks. Automatic summarisation is also enabled, as illustrated below:

```
R1#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
```

https://t.me/learningnets

```
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: connected, eigrp 150
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    150.1.1.1/32
Routing Information Sources:
    Gateway         Distance      Last Update
    150.1.1.2             90      00:00:07
  Distance: internal 90 external 170
```

Because the 10.*x.x.x*/24 prefixes are all external routes, EIGRP will not automatically summarise these prefixes, as illustrated in the previous example. Therefore, EIGRP will not add a summary route to either the topology table or the IP routing table for these entries. This is illustrated in the following output:

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(150)/ID(10.3.3.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.0.0.0/24, 1 successors, FD is 1280256
        via Rconnected (1280256/0)
P 10.1.1.0/24, 1 successors, FD is 1280256
        via Rconnected (1280256/0)
P 10.2.2.0/24, 1 successors, FD is 1280256
        via Rconnected (1280256/0)
P 10.3.3.0/24, 1 successors, FD is 1280256
        via Rconnected (1280256/0)
...

[Truncated Output]
```

The specific route entries are advertised to R2 as external EIGRP routes, as illustrated below:

```
R2#show ip route eigrp
     10.0.0.0/24 is subnetted, 4 subnets
D EX    10.3.3.0 [170/3449856] via 150.1.1.1, 00:07:02, Serial0/0
D EX    10.2.2.0 [170/3449856] via 150.1.1.1, 00:07:02, Serial0/0
D EX    10.1.1.0 [170/3449856] via 150.1.1.1, 00:07:02, Serial0/0
D EX    10.0.0.0 [170/3449856] via 150.1.1.1, 00:07:02, Serial0/0
```

Now, assume that the 10.0.0.0/24 subnet is an internal network, while the 10.1.1.0/24, 10.2.2.0/24, and 10.3.3.0/24 subnets are external routes. Because one of the routes that will

https://t.me/learningnets

comprise the classful summary address 10.0.0.0/8 is an internal route, EIGRP will create a summary address and include that in the EIGRP topology table and the IP routing table. The `show ip protocols` command shows that the 10.0.0.0/24 network is now an internal EIGRP network, as illustrated below:

```
R1#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: connected, eigrp 150
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Automatic address summarization:
    150.1.0.0/16 for Loopback0
      Summarizing with metric 2169856
    10.0.0.0/8 for Serial0/0
      Summarizing with metric 128256
  Maximum path: 4
  Routing for Networks:
    10.0.0.1/32
    150.1.1.1/32
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)          90      00:00:05
    150.1.1.2              90      00:00:02
  Distance: internal 90 external 170
```

In the output above, EIGRP automatic summarisation has generated a summary address for 10.0.0.0/8 because the 10.0.0.0/24 internal subnet is a part of the aggregate address. The EIGRP topology table displays the external and internal entries, as well as the summary address, as illustrated below:

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(150)/ID(10.3.3.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.0.0.0/8, 1 successors, FD is 128256
         via Summary (128256/0), Null0
```

https://t.me/learningnets

```
P 10.0.0.0/24, 1 successors, FD is 128256
        via Connected, Loopback0
P 10.1.1.0/24, 1 successors, FD is 1280256
        via Rconnected (1280256/0)
P 10.2.2.0/24, 1 successors, FD is 1280256
        via Rconnected (1280256/0)
P 10.3.3.0/24, 1 successors, FD is 1280256
        via Rconnected (1280256/0)
...

[Truncated Output]
```

This time, only a single route is advertised to R2, as illustrated in the following output:

```
R2#show ip route eigrp
D    10.0.0.0/8 [90/2297856] via 150.1.1.1, 00:04:05, Serial0/0
```

From the perspective of R2, this is simply an internal EIGRP route. In other words, the router does not have any knowledge that the summary address is also comprised of external routes, as illustrated below:

```
R2#show ip route 10.0.0.0 255.0.0.0
Routing entry for 10.0.0.0/8
  Known via "eigrp 150", distance 90, metric 2297856, type internal
  Redistributing via eigrp 150
  Last update from 150.1.1.1 on Serial0/0, 00:05:34 ago
  Routing Descriptor Blocks:
  * 150.1.1.1, from 150.1.1.1, 00:05:34 ago, via Serial0/0
      Route metric is 2297856, traffic share count is 1
      Total delay is 25000 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

R2 is able to reach both the internal 10.0.0.0/24 network and the other external 10.*x.x.x*/24 networks via the received summary route, as illustrated below:

```
R2#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R2#ping 10.3.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.1, timeout is 2 seconds:
!!!!!
```

https://t.me/learningnets

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

Unlike EIGRP automatic summarisation, EIGRP manual route summarisation is configured and implemented at the interface level using the `ip summary-address eigrp [ASN] [network] [mask] [distance] [leak-map <name>]` interface configuration command. By default, an EIGRP summary address is assigned a default administrative distance value of 5. This default assignment can be changed by specifying the desired administrative distance value as specified by the `[distance]` keyword.

By default, when manual route summarisation is configured, EIGRP will not advertise the more specific route entries that fall within the summarised network entry. The [`leak-map <name>`] keyword can be configured to allow EIGRP route leaking, wherein EIGRP allows specified specific route entries to be advertised in conjunction with the summary address. Those entries that are not specified in the leak map are still suppressed.

When manually summarising routes, it is important to be as specific as possible. Otherwise, the configuration might result in a black-holing of traffic in a manner similar to the example pertaining to discontiguous networks that was described earlier. This concept is illustrated in Figure 36.18 below:

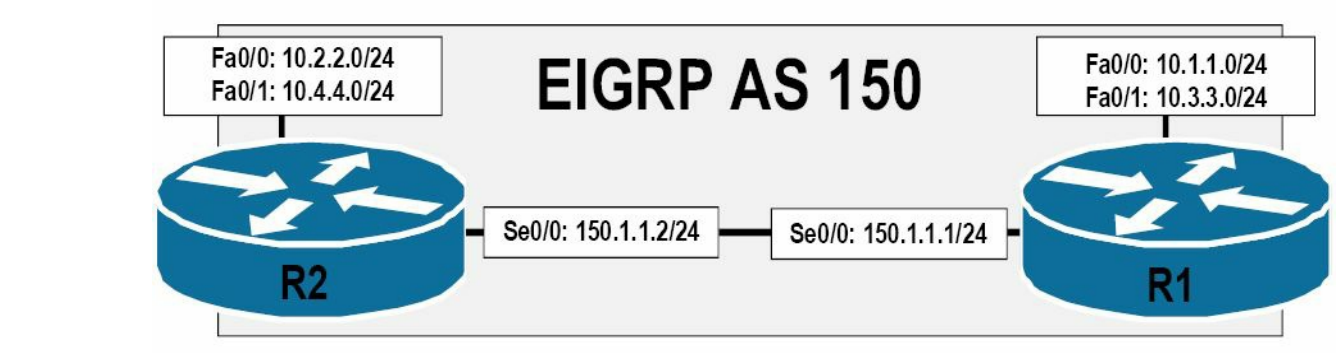


Figure 36.18 – Black-Holing Traffic with Poor Route Summarisation

Referencing Figure 36.18, if a manual summary address of 10.0.0.0/8 is configured on both of the routers, then the more specific prefixes are suppressed. Because EIGRP also installs a route to the summary address into both the EIGRP topology table and the IP routing table with a next-hop interface of Null0, the same issue experienced with automatic summarisation in discontiguous networks is experienced in this network, and the respective subnets on either router will be unable to communicate with each other.

Additionally, it is also important to understand that if poorly implemented within the network, route summarisation may result in suboptimal routing within the network. This concept is illustrated in Figure 36.19 below:

https://t.me/learningnets

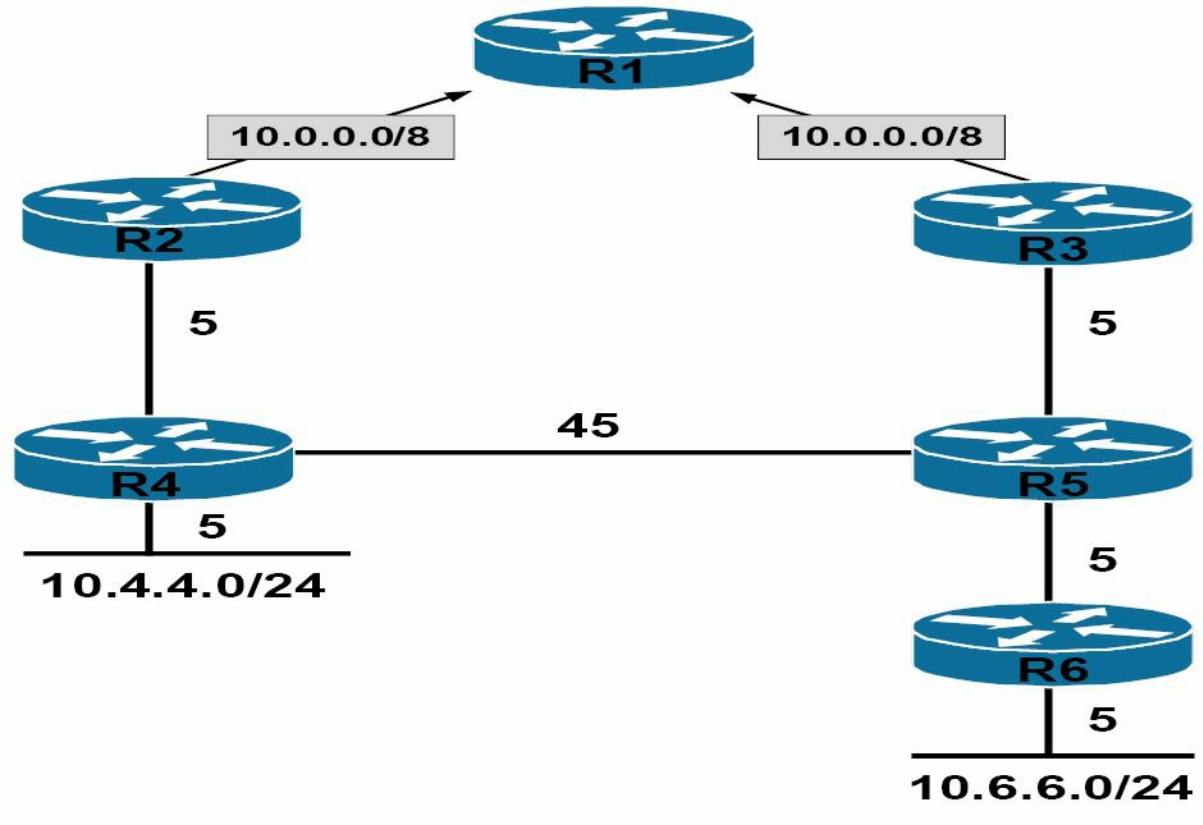


Figure 36.19 – Suboptimal Routing with Route Summarisation

By default, when a summary route is created for EIGRP, the router advertises the summary address with a metric equal to the minimum of all the more specific routes. In other words, the summary address will have the same metric as the lowest, most specific route included in the creation of the summary address.

Referencing the network topology illustrated in Figure 36.19, both R2 and R3 are advertising the summary address 10.0.0.0/8 to R1. This summary is comprised of the more specific 10.4.4.0/24 and 10.6.6.0/24 prefixes. The metric used by the summary address on both routers is calculated as illustrated below in Table 36.5:

Table 36.5 – Summary Route Metric Calculation

Starting Point (Router)	Metric To 10.4.4.0/24	Metric to 10.6.6.0/24
R2	5 + 5 = 10	5 + 45 + 5 + 5 = 60
R3	5 + 45 + 5 = 55	5 + 5 + 5 = 15

Based on the metric calculation in Table 36.5, R2 clearly has the lowest metric path to 10.4.4.0/24 for traffic originating from R1, while R3 has the lowest metric path to 10.6.6.0/24 for traffic originating from R1. However, when the 10.0.0.0/8 summary address is advertised to R1, the summary address uses the lowest minimum metric of all routes of which the summary is comprised. Based on this example, R2 advertises the summary address to R1 with a metric of 10. R3 follows the same logic and advertises the summary route to R1 with a metric of 15.

When R1 receives the summary routes from R2 and R3, it uses the one with the lowest metric to forward traffic destined to subnets contained within the 10.0.0.0/8 major classful network

https://t.me/learningnets

via R2. This is illustrated in Figure 36.20 below:

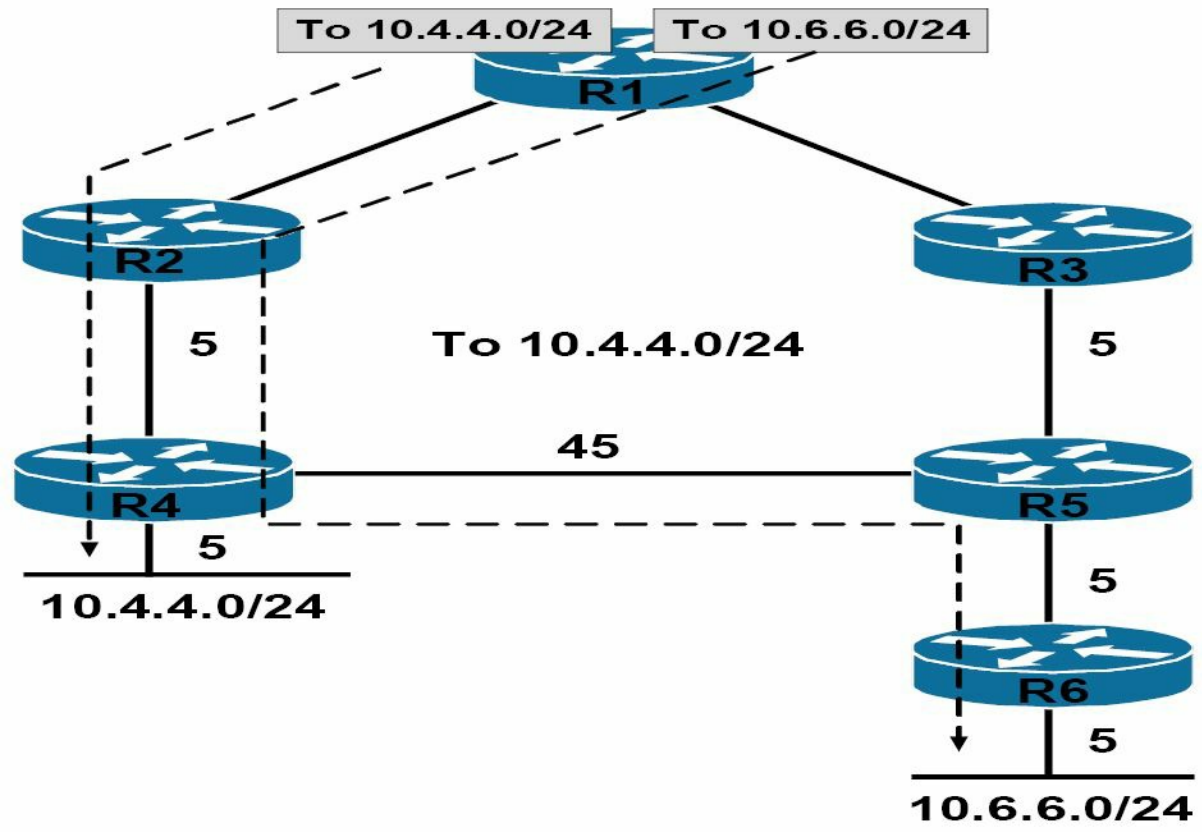


Figure 36.20 – Suboptimal Routing with Route Summarisation

Referencing Figure 36.20, you can clearly see that while this is the optimal path for the 10.4.4.0/24 subnet, it is a suboptimal path for the 10.6.6.0/24 subnet. It is therefore very important to understand the network topology before implementing route summarisation in the network.

Reverting back to the configuration of manual route summarisation when using EIGRP, the network topology illustrated in Figure 36.21 below will be used to demonstrate manual route summarisation and route leaking:

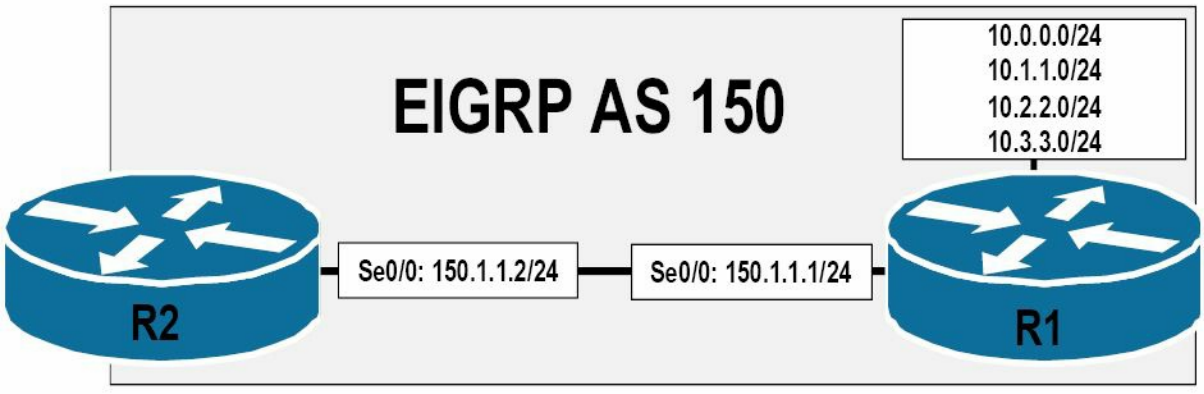


Figure 36.21 – Configuring EIGRP Manual Route Summarisation

Based on the interfaces configured on R1, the routing table on R2 displays the following entries:

```
R2#show ip route eigrp
     10.0.0.0/24 is subnetted, 4 subnets
```

https://t.me/learningnets

```
D       10.3.3.0 [90/2297856] via 150.1.1.1, 00:00:14, Serial0/0
D       10.2.2.0 [90/2297856] via 150.1.1.1, 00:00:14, Serial0/0
D       10.1.1.0 [90/2297856] via 150.1.1.1, 00:00:14, Serial0/0
D       10.0.0.0 [90/2297856] via 150.1.1.1, 00:00:14, Serial0/0
```

To summarise these entries on R1 and to advertise a single specific route, the following configuration is applied to the Serial0/0 interface of R1:

```
R1(config)#interface Serial0/0
R1(config-if)#ip summary-address eigrp 150 10.0.0.0 255.252.0.0
R1(config-if)#exit
```

Following this configuration, the summary entry 10.0.0.0/14 is installed into the EIGRP topology table and the IP routing table on R1. The EIGRP topology table entry is as follows:

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(150)/ID(10.3.3.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.0.0.0/14, 1 successors, FD is 128256
        via Summary (128256/0), Null0
P 10.3.3.0/24, 1 successors, FD is 128256
        via Connected, Loopback3
P 10.2.2.0/24, 1 successors, FD is 128256
        via Connected, Loopback2
P 10.0.0.0/24, 1 successors, FD is 128256
        via Connected, Loopback0
P 10.1.1.0/24, 1 successors, FD is 128256
        via Connected, Loopback1
...
[Truncated Output]
```

The routing table entry also reflects the summary route with a next-hop interface of Null0, as illustrated below:

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.3.3.0/24 is directly connected, Loopback3
```

https://t.me/learningnets

```
C       10.2.2.0/24 is directly connected, Loopback2
C       10.1.1.0/24 is directly connected, Loopback1
C       10.0.0.0/24 is directly connected, Loopback0
D*      10.0.0.0/14 is a summary, 00:02:37, Null0
     150.1.0.0/24 is subnetted, 1 subnets
C       150.1.1.0 is directly connected, Serial0/0
     150.2.0.0/24 is subnetted, 1 subnets
C       150.2.2.0 is directly connected, Serial0/1
```

Again, the `show ip route [address] [mask] longer-prefixes` command can be used to view the specific route entries that comprise the aggregate or summary route, as illustrated in the following output on R1:

```
R1#show ip route 10.0.0.0 255.252.0.0 longer-prefixes
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.3.3.0/24 is directly connected, Loopback3
C       10.2.2.0/24 is directly connected, Loopback2
C       10.1.1.0/24 is directly connected, Loopback1
C       10.0.0.0/24 is directly connected, Loopback0
D       10.0.0.0/14 is a summary, 00:04:03, Null0
```

On R2, a single route entry for the 10.0.0.0/14 summary address is received, as illustrated below:

```
R2#show ip route eigrp
     10.0.0.0/14 is subnetted, 1 subnets
D       10.0.0.0 [90/2297856] via 150.1.1.1, 00:06:22, Serial0/0
```

To reinforce the concept regarding the metric for the summary route, assume that the routes on R1 are all external EIGRP routes (i.e., they have been redistributed into EIGRP) with different metrics. The EIGRP topology table on R1 displays the following:

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(150)/ID(10.3.3.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.0.0.0/24, 1 successors, FD is 10127872
```

https://t.me/learningnets

```
        via Rconnected (10127872/0)
P 10.1.1.0/24, 1 successors, FD is 3461120
        via Rconnected (3461120/0)
P 10.2.2.0/24, 1 successors, FD is 2627840
        via Rconnected (2627840/0)
P 10.3.3.0/24, 1 successors, FD is 1377792
        via Rconnected (1377792/0)
...
[Truncated Output]
```

The same summary address configured on R1 in the previous example is configured again as follows:

```
R1(config)#int s0/0
R1(config-if)#ip summary-address eigrp 150 10.0.0.0 255.252.0.0
R1(config-if)#exit
```

Based on this configuration, the summary route is placed into the EIGRP topology table and the IP routing table with a metric equal to the lowest metric of all routes that it encompasses. Based on the output of the `show ip eigrp topology` command shown previously, the summary address will be assigned the same metric assigned to the 10.3.3.0/24 prefix, as illustrated below:

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(150)/ID(10.3.3.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.0.0.0/14, 1 successors, FD is 1377792
        via Summary (1377792/0), Null0
P 10.0.0.0/24, 1 successors, FD is 10127872
        via Rconnected (10127872/0)
P 10.1.1.0/24, 1 successors, FD is 3461120
        via Rconnected (3461120/0)
P 10.2.2.0/24, 1 successors, FD is 2627840
        via Rconnected (2627840/0)
P 10.3.3.0/24, 1 successors, FD is 1377792
        via Rconnected (1377792/0)
P 150.1.1.0/24, 1 successors, FD is 2169856
        via Connected, Serial0/0
```

Understanding Passive Interfaces

As stated earlier in this module, when EIGRP is enabled for a network, the router begins to send out Hello packets on all interfaces that fall within the specified network range. This allows EIGRP to discover neighbours dynamically and establish network relationships. This is desired

https://t.me/learningnets

on interfaces that are actually connected to physical media, such as Ethernet and Serial interfaces. However, this default behaviour also results in an unnecessary waste of router resources on logical interfaces, such as Loopback interfaces, that will never have any other device connected to them with which the router could ever establish an EIGRP neighbour relationship.

Cisco IOS software allows administrators to use the `passive-interface [name|default]` router configuration command to specify the named interface as passive, or all interfaces as passive. EIGRP packets are not sent out on passive interfaces; therefore, no neighbour relationship will ever be established between passive interfaces. The following output illustrates how to configure two EIGRP-enabled interfaces as passive on a router:

```
R1(config)#interface Loopback0
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface Loopback1
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface Serial0/0
R1(config-if)#ip address 150.1.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#router eigrp 150
R1(config-router)#no auto-summary
R1(config-router)#network 150.1.1.0 0.0.0.255
R1(config-router)#network 10.0.0.0 0.0.0.255
R1(config-router)#network 10.1.1.0 0.0.0.255
R1(config-router)#passive-interface Loopback0
R1(config-router)#passive-interface Loopback1
R1(config-router)#exit
```

Based on this configuration, Loopback0 and Loopback1 are enabled for EIGRP routing and the directly connected networks will be advertised to EIGRP neighbours. However, no EIGRP packets will be sent by R1 out of these interfaces. Serial0/0, on the other hand, is also configured for EIGRP routing, but EIGRP is allowed to send packets on this interface because it is not a passive interface. All three network entries are installed in the EIGRP topology table, as illustrated below:

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(150)/ID(10.3.3.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.1.1.0/24, 1 successors, FD is 128256
        via Connected, Loopback1
P 10.0.0.0/24, 1 successors, FD is 128256
```

https://t.me/learningnets

```
        via Connected, Loopback0
P 150.1.1.0/24, 1 successors, FD is 2169856
        via Connected, Serial0/0
```

However, the output of the `show ip eigrp interfaces` command shows that EIGRP routing is enabled only for the Serial0/0 interface, as illustrated below:

```
R1#show ip eigrp interfaces
IP-EIGRP interfaces for process 150
                      Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface      Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Se0/0            1        0/0        0       0/15           0           0
```

You can also view the interfaces configured as passive in the output of the `show ip protocols` command, as illustrated below:

```
R1#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 150
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0/24
    10.1.1.0/24
    150.1.1.0/24
  Passive Interface(s):
    Loopback0
    Loopback1
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

The `[default]` keyword makes all interfaces passive. Assume that a router is configured with 50 Loopback interfaces configured. If you wanted to make each Loopback interface passive, you would need to add 50 lines of code. The `passive-interface default` command can be used to make all interfaces passive. Those interfaces that you do want to send EIGRP packets to can then be configured with the `no passive-interface [name]` command. The following illustrates

https://t.me/learningnets

the use of the `passive-interface default` command:

```
R1(config)#interface Loopback0
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface Loopback1
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface Loopback3
R1(config-if)#ip address 10.3.3.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface Loopback2
R1(config-if)#ip address 10.2.2.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface Serial0/0
R1(config-if)#ip address 150.1.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#router eigrp 150
R1(config-router)#network 10.0.0.1 255.255.255.0
R1(config-router)#network 10.1.1.1 255.255.255.0
R1(config-router)#network 10.3.3.1 255.255.255.0
R1(config-router)#network 10.2.2.1 255.255.255.0
R1(config-router)#network 150.1.1.1 255.255.255.0
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface Serial0/0
R1(config-router)#exit
```

The `show ip protocols` can be used to view which interfaces are passive under EIGRP, as illustrated below:

```
R1#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 150
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
```

https://t.me/learningnets

```
  Routing for Networks:
    10.0.0.0/24
    10.1.1.0/24
    10.2.2.0/24
    10.3.3.0/24
    150.1.1.0/24
  Passive Interface(s):
    Loopback1
    Loopback2
    Loopback3
    Loopback4
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)          90      00:02:52
  Distance: internal 90 external 170
```

By using the `passive-interface default` command, the configuration of multiple passive interfaces is simplified and reduced. Used in conjunction with the `no passive-interface Serial0/0` command, EIGRP packets are still sent out on Serial0/0, allowing EIGRP neighbour relationships to be established across that interface, as illustrated below:

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 150
H   Address      Interface  Hold  Uptime    SRTT  RTO    Q     Seq
                            (sec)           (ms)         Cnt   Num
0   150.1.1.2    Se0/0      12    00:02:47  1     3000   0     69
```

Understanding the Use of the EIGRP Router ID

Unlike OSPF, which uses the router ID (RID) to identify the OSPF neighbour, the primary use of the EIGRP RID is to prevent routing loops. The RID is used to identify the originating router for external routes. If an external route is received with the same RID as the local router, the route is discarded. This feature is designed to reduce the possibility of routing loops in networks where route redistribution is being performed on more than one ASBR.

When determining the RID, EIGRP will select the highest IP address that is configured on the router. If Loopback interfaces are also configured on the router, those interfaces are preferred, since a Loopback interface is the most stable interface that can exist on a router. The RID will never change unless the EIGRP process is removed (i.e., if the RID is manually configured). The RID will always be listed in the EIGRP topology table, as illustrated below:

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(150)/ID(10.3.3.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
```

https://t.me/learningnets

```
P 10.2.2.0/24, 1 successors, FD is 128256
```

```
        via Connected, Loopback2
P 10.3.3.0/24, 1 successors, FD is 128256
        via Connected, Loopback3
P 10.1.1.0/24, 1 successors, FD is 128256
        via Connected, Loopback1
P 10.0.0.0/24, 1 successors, FD is 128256
        via Connected, Loopback0
P 150.1.1.0/24, 1 successors, FD is 2169856
        via Connected, Serial0/0
```

NOTE: It is important to understand that the RID and the neighbour ID will typically be different, although this may not be the case in routers with a single interface, for example.

The EIGRP RID is configured using the `eigrp router-id [address]` router configuration command. When this command is entered, the RID is automatically updated with the new address in the EIGRP topology table. To demonstrate this point, let's begin by looking at the current RID on the router, as stated in the topology table below:

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(150)/ID(10.3.3.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
...
[Truncated Output]
```

A RID of 1.1.1.1 is now configured on the router, as follows:

```
R1(config)#router eigrp 150
R1(config-router)#eigrp router-id 1.1.1.1
R1(config-router)#
*Mar  1 05:50:13.642: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 150: Neighbor 150.1.1.2 (Serial0/0)
is down: route configuration changed
*Mar  1 05:50:16.014: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 150: Neighbor 150.1.1.2 (Serial0/0)
is up: new adjacency
```

Following the change, the EIGRP neighbour relationship is reset and the new RID is reflected immediately in the EIGRP topology table, as illustrated below:

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(150)/ID(1.1.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
...
[Truncated Output]
```

When configuring the EIGRP RID, the following should be remembered:

https://t.me/learningnets

- You cannot configure the RID as 0.0.0.0
- You cannot configure the RID as 255.255.255.255

All external routes that are originated by the router now contain the EIGRP RID. This can be verified in the following output of neighbour router R2:

```
R2#show ip eigrp topology 192.168.254.0/24
IP-EIGRP (AS 150): Topology entry for 192.168.254.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 7289856
  Routing Descriptor Blocks:
  150.1.1.1 (Serial0/0), from 150.1.1.1, Send flag is 0x0
      Composite metric is (7289856/6777856), Route is External
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 220000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 1.1.1.1
        AS number of route is 0
        External protocol is Connected, external metric is 0
        Administrator tag is 0 (0x00000000)
```

The RID is not included for internal EIGRP routes, as illustrated in the following output:

```
R2#show ip eigrp topology 10.3.3.0/24
IP-EIGRP (AS 150): Topology entry for 10.3.3.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2297856
  Routing Descriptor Blocks:
  150.1.1.1 (Serial0/0), from 150.1.1.1, Send flag is 0x0
      Composite metric is (2297856/128256), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```

https://t.me/learningnets

Day 36 Questions

1. You can see the ASN with the `show ip` _____ command.
2. Every router you want to communicate with in your routing domain must have a different ASN. True or false?
3. What is the purpose of the EIGRP topology table?
4. By default, EIGRP uses the _____ bandwidth on the path to a destination network and the total _____ to compute routing metrics.
5. Dynamic neighbour discovery is performed by sending EIGRP Hello packets to the destination Multicast group address _____.
6. EIGRP packets are sent directly over IP using protocol number _____.
7. To populate the topology table, EIGRP runs the _____ algorithm.
8. The _____ _____ includes both the metric of a network as advertised by the connected neighbour, plus the cost of reaching that particular neighbour.
9. Cisco IOS software supports equal cost load sharing for a default of up to four paths for all routing protocols. True or false?
10. What EIGRP command can be used to enable unequal cost load sharing?

https://t.me/learningnets

Day 36 Answers

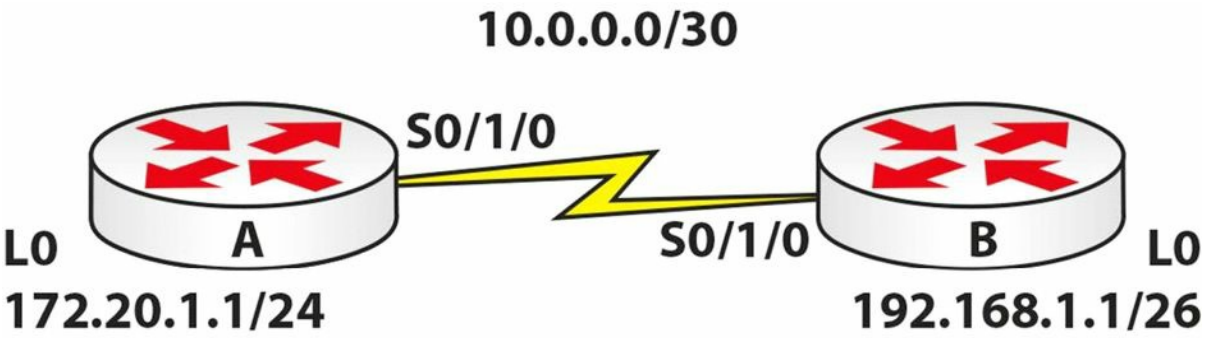
1. `protocols`.
2. False.
3. The topology table allows all EIGRP routers to have a consistent view of the entire network. All known destination networks and subnets that are advertised by neighbouring EIGRP routers are stored there.
4. Minimum, delay.
5. 224.0.0.10.
6. 88.
7. DUAL.
8. Feasible Distance.
9. True.
10. The `variance` command.

https://t.me/learningnets

Day 36 Lab

EIGRP Lab

Topology



Purpose

Learn how to configure basic EIGRP.

Walkthrough

1. Configure all IP addresses based on the topology above. Make sure you can ping across the Serial link.
2. Configure EIGRP with AS 30 on each router.

```
RouterA(config)#router eigrp 30
RouterA(config-router)#net 172.20.0.0
RouterA(config-router)#net 10.0.0.0
RouterA(config-router)#^Z
RouterA#
RouterB#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RouterB(config)#router eigrp 30
RouterB(config-router)#net 10.0.0.0
%DUAL-5-NBRCHANGE: IP-EIGRP 30: Neighbor 10.0.0.1 (Serial0/1/0) is up: new adjacency
RouterB(config-router)#net 192.168.1.0
```

3. Check the routing table on each router.

```
RouterA#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
```

https://t.me/learningnets

```
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:01:43, Null0
C       10.0.0.0/30 is directly connected, Serial0/1/0
     172.20.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.20.0.0/16 is a summary, 00:01:43, Null0
C       172.20.1.0/24 is directly connected, Loopback0
D    192.168.1.0/24 [90/20640000] via 10.0.0.2, 00:00:49, Serial0/1/0
RouterA
RouterB#show ip route
...
[Truncated Output]
...
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:01:21, Null0
C       10.0.0.0/30 is directly connected, Serial0/1/0
D    172.20.0.0/16 [90/20640000] via 10.0.0.1, 00:01:27, Serial0/1/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
D       192.168.1.0/24 is a summary, 00:01:21, Null0
C       192.168.1.0/26 is directly connected, Loopback0
RouterB#
```

4. Check to ensure that each router is auto-summarising each network. Then turn off auto-summary on Router B.

```
RouterB#show ip protocols
Routing Protocol is "eigrp  30"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 30
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.1.0/24 for Serial0/1/0
      Summarizing with metric 128256
    10.0.0.0/8 for Loopback0
      Summarizing with metric 20512000
  Maximum path: 4
  Routing for Networks:
```

https://t.me/learningnets

```
     10.0.0.0
     192.168.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.0.0.1        90            496078
  Distance: internal 90 external 170
RouterB(config)#router eigrp 30
RouterB(config-router)#no auto-summary
```

5. Check the routing table on Router A.

```
RouterA#show ip route
...
[Truncated Output]
...
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:00:04, Null0
C       10.0.0.0/30 is directly connected, Serial0/1/0
     172.20.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.20.0.0/16 is a summary, 00:00:04, Null0
C       172.20.1.0/24 is directly connected, Loopback0
     192.168.1.0/26 is subnetted, 1 subnets
D       192.168.1.0 [90/20640000] via 10.0.0.2, 00:00:04, Serial0/1/0
RouterA#
```

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 37 – Troubleshooting EIGRP

Day 37 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes

Enhanced Interior Gateway Routing Protocol is a Cisco-proprietary advanced Distance Vector routing protocol. As a CCNA network engineer, it is important that you understand how to support EIGRP, as it is a very commonly implemented routing protocol. As with the previous technologies described thus far in this guide, in order to troubleshoot and support networks running EIGRP, you must have a solid understanding of the inner workings of the protocol itself.

While it is not possible to delve into all potential EIGRP problem scenarios, this module will discuss some of the most common problem scenarios when EIGRP is implemented as the Interior Gateway Protocol (IGP) of choice.

Today you will learn about the following:

- Troubleshooting neighbour relationships
- Troubleshooting route installation
- Troubleshooting route advertisement
- Debugging EIGRP routing issues

This lesson maps to the following CCNA syllabus requirement:

- Troubleshoot and resolve EIGRP problems
    - Neighbour adjancies
    - AS number
    - Load balancing
    - Split horizon

Troubleshooting Neighbour Relationships

It is important to understand that simply enabling EIGRP between two or more routers does not guarantee that a neighbour relationship will be established. In addition to certain parameters-matching, additional factors can also result in a failure of EIGRP neighbour relationship establishment. The EIGRP neighbour relationship may not establish due to any of the following:

- The neighbour routers are not on a common subnet
- Mismatched primary and secondary subnets
- Mismatched K values

https://t.me/learningnets

- ☐ Mismatched ASN
- ☐ Access control lists are filtering EIGRP packets
- ☐ Physical Layer issues
- ☐ Data Link Layer issues
- ☐ Mismatched authentication parameters

Uncommon subnet issues are one of the most common problems experienced when attempting to establish EIGRP neighbour relationships. When EIGRP cannot establish a neighbour relationship because of an uncommon subnet, the following error message will be printed on the console, or will be logged by the router or switch:

```
*Mar  2 22:12:46.589 CST: IP-EIGRP(Default-IP-Routing-Table:1): Neighbor 150.1.1.2 not on common subnet for FastEthernet0/0
*Mar  2 22:12:50.977 CST: IP-EIGRP(Default-IP-Routing-Table:1): Neighbor 150.1.1.2 not on common subnet for FastEthernet0/0
```

The most common reason for the neighbour routers being on an uncommon subnet is a misconfiguration issue. It may be that the router interfaces have been accidentally configured on two different subnets. However, if the neighbours are connected via a VLAN, it is possible that Multicast packets could be leaking between VLANs, resulting in this error. The first troubleshooting step, however, simply would be to verify the interface configuration on the devices. Following this, additional troubleshooting steps, such as VLAN troubleshooting (if applicable) could be undertaken to isolate and resolve the issue.

Another common reason for this error message is using secondary addresses when attempting to establish EIGRP neighbour relationships. Again, the simplest way to troubleshoot such issues is to verify the router or switch configurations. For example, assume the error message above was being printed on the console of the local router. The first troubleshooting step would be to validate the IP addresses configured on the interface, as follows:

```
R1#show running-config interface FastEthernet0/0
Building configuration...
Current configuration : 140 bytes
!
interface FastEthernet0/0
ip address 150.2.2.1 255.255.255.0
duplex auto
speed auto
end
```

Next, validate that the configuration is the same on the device with the IP address 150.1.1.2, as follows:

```
R2#show running-config interface FastEthernet0/0
Building configuration...
Current configuration : 140 bytes
```

https://t.me/learningnets

```
!
interface FastEthernet0/0
ip address 150.2.2.2 255.255.255.0 secondary
ip address 150.1.1.2 255.255.255.0
duplex auto
speed auto
end
```

From the output above, you can see that the primary subnet on R1 is the secondary subnet on the local router. EIGRP will not establish neighbour relationships using a secondary address. The resolution for this issue simply would be to correct the IP addressing configuration under the FastEthernet0/0 interface of R2, as follows:

```
R2#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface FastEthernet0/0
R2(config-if)#ip address 150.2.2.2 255.255.255.0
R2(config-if)#ip address 150.1.1.2 255.255.255.0 secondary
R2(config-if)#end
*Oct 20 03:10:27.185 CST: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 150.2.2.1
(FastEthernet0/0) is up: new adjacency
```

EIGRP K values are constants that are used to distribute weight to different path aspects, which may be included in the composite EIGRP metric. Once again, the default values for the K values are K1 = K3 = 1 and K2 = K4 = K5 = 0. If changed on one router or switch, then these values must be adjusted for all other routers or switches within the autonomous system. The default EIGRP K values can be viewed using the `show ip protocols` command, as illustrated below:

```
R1#show ip protocols
Routing Protocol is "eigrp 150"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is 1
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 150, ospf 1
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    10.1.0.0/24
    172.16.1.0/30
```

https://t.me/learningnets

```
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      15:59:19
    172.16.0.2            90      12:51:56
    172.16.1.2            90      00:27:17
  Distance: internal 90 external 170
```

When K values are reset on a router, all neighbour relationships for the local router will be reset. If the values are not consistent on all routers following the reset, the following error message will be printed on the console, and the EIGRP neighbour relationship(s) will not be established:

```
*Oct 20 03:19:14.140 CST: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 150.2.2.1
(FastEthernet0/0) is down: Interface Goodbye received
*Oct 20 03:19:18.732 CST: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 150.2.2.1
(FastEthernet0/0) is down: K-value mismatch
```

NOTE: While EIGRP K values can be adjusted using the `metric-weights` command, this is not recommended without assistance from seasoned network engineers or the Technical Assistance Centre (TAC).

Unlike OSPF, which uses a locally significant process ID, EIGRP requires the same ASN (among other variables) when establishing neighbour relationships with other routers. Troubleshoot such issues by comparing configurations of devices and ensuring that the ASN (among other variables) is consistent between routers that should establish neighbour relationships. A good indicator that neighbours are in a different AS would be a lack of bidirectional Hellos, even in the presence of basic IP connectivity between the routers. This can be validated using the `show ip eigrp traffic` command, the output of which is illustrated in the section that follows.

ACLs and other filters are also common causes for routers failing to establish EIGRP neighbour relationships. Check router configurations and those of intermediate devices to ensure that EIGRP or Multicast packets are not filtered. A very useful troubleshooting command to use is the `show ip eigrp traffic` command. This command provides statistics on all EIGRP packets. Assume, for example, that you have verified basic connectivity and configurations between two devices, but the EIGRP neighbour relationship is still not up. In that case, you could use this command to check to see whether the routers are exchanging Hello packets, before enabling debugging on the local device, as illustrated below:

```
R2#show ip eigrp traffic
IP-EIGRP Traffic Statistics for AS 2
  Hellos sent/received: 144/0
  Updates sent/received: 0/0
  Queries sent/received: 0/0
  Replies sent/received: 0/0
  Acks sent/received: 0/0
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
```

https://t.me/learningnets

```
  Hello Process ID: 149
  PDM Process ID: 120
  IP Socket queue:   0/2000/0/0 (current/max/highest/drops)
  Eigrp input queue: 0/2000/0/0 (current/max/highest/drops)
```

In the output above, notice that the local router has not received any Hello packets, although it has sent out 144 Hellos. Assuming that you have verified IP connectivity between the two devices, as well as the configuration, you could also check ACL configurations on the local routers, as well as intermediate devices (if applicable), to ensure that EIGRP or Multicast traffic is not being filtered. For example, you might find an ACL that is configured to deny Class D and Class E traffic, while allowing all other traffic, such as the following ACL:

```
R2#show ip access-lists
Extended IP access list 100
    10 deny ip 224.0.0.0 15.255.255.255 any
    20 deny ip any 224.0.0.0 15.255.255.255 (47 matches)
    30 permit ip any any (27 matches)
```

Physical and Data Link Layer issues, and ways in which these can affect routing protocols and other traffic, have been described in detail in previous modules. You can troubleshoot these issues using the `show interfaces`, `show interfaces counters`, `show vlan`, and `show spanning-tree` commands, among other commands described in those modules. To avoid being redundant, we will not restate the Physical and Data Link Layer troubleshooting steps.

Finally, common authentication configuration mistakes include using different key IDs when configuring key chains and specifying different or mismatched passwords. When authentication is enabled under an interface, the EIGRP neighbour relationships are reset and reinitialised. If previously established neighbour relationships do not come up following authentication implementation, verify the authentication configuration parameters by looking at the running configuration or using the `show key chain` and `show ip eigrp interfaces detail [name]` commands on the router. Following is a sample output of the information that is printed by the `show key chain` command:

```
R2#show key chain
Key-chain EIGRP-1:
    key 1 -- text "eigrp-1"
      accept lifetime (always valid) - (always valid) [valid now]
      send lifetime (always valid) - (always valid) [valid now]
Key-chain EIGRP-2:
    key 1 -- text "eigrp-2"
      accept lifetime (00:00:01 UTC Nov 1 2010) - (infinite)
      send lifetime (00:00:01 UTC Nov 1 2010) - (infinite)
Key-chain EIGRP-3:
    key 1 -- text "eigrp-3"
      accept lifetime (00:00:01 UTC Dec 1 2010) - (00:00:01 UTC Dec 31 2010)
```

https://t.me/learningnets

```
      send lifetime (00:00:01 UTC Dec 1 2010) - (00:00:01 UTC Dec 31 2010)
```

The following is a sample output of the information that is printed by the `show ip eigrp interfaces detail [name]` command:

```
R2#show ip eigrp interfaces detail Serial0/0
IP-EIGRP interfaces for process 1
                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Se0/0              0        0/0        0        0/1            0           0
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/0  Un/reliable ucasts: 0/0
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
  Retransmissions sent: 0  Out-of-sequence rcvd: 0
  Authentication mode is md5,  key-chain is "EIGRP-1"
  Use unicast
```

When troubleshooting in general, it is recommended that you use `show` commands in Cisco IOS software instead of enabling `debug` commands. While debugging provides real-time information, it is very processor intensive, and it could result in high CPU utilisation of the device and, in some cases, even crashing the device. In addition to `show` commands, you should also pay attention to the various error messages that are printed by the software, as these provide useful information that can be used to troubleshoot and isolate the root cause of the problem.

Troubleshooting Route Installation

There are instances where you might notice that EIGRP is not installing certain routes into the routing table. For the most part, this is typically due to some misconfigurations versus a protocol failure. Some common reasons for route installation failure include the following:

- The same route is received via another protocol with a lower administrative distance
- EIGRP summarisation
- Duplicate router IDs are present within the EIGRP domain
- The routes do not meet the Feasibility Condition

The administrative distance (AD) concept is used to determine how reliable the route source is. The lower the AD, the more reliable the route source is. If the same route is received from three different protocols, the route with the lowest AD will be installed into the routing table. When using EIGRP, keep in mind that EIGRP uses different AD values for summary, internal, and external routes. If you are running multiple routing protocols, it is important to ensure that you understand AD values and how they impact routing table population. This is especially of concern when you are redistributing routes between multiple routing protocols.

By default, EIGRP automatically summarises at classful boundaries and creates a summary route pointing to the Null0 interface. Because the summary is installed with a default AD value

https://timelearningnets

of 5, any other similar dynamically received routes will not be installed into the routing table. Consider the topology illustrated in Figure 37.1 below, for example:

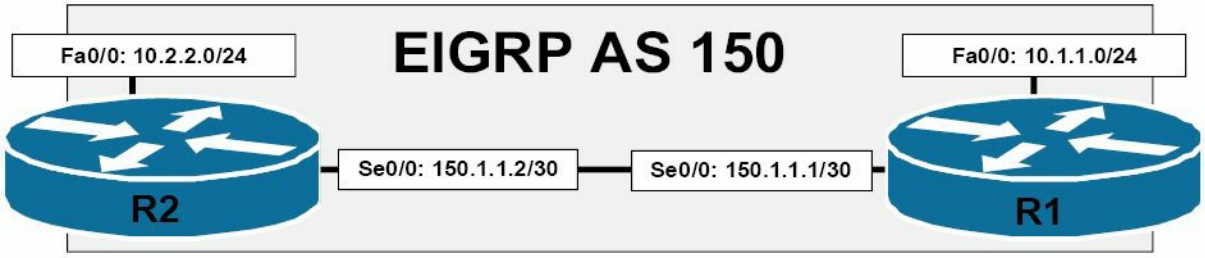


Figure 37.1 – EIGRP Automatic Summarisation

Referencing the diagram illustrated in Figure 37.1, the 150.1.1.0./30 subnet separates 10.1.1.0/24 and 10.2.2.0/24. When automatic summarisation is enabled, both R1 and R2 will summarise the 10.1.1.0/24 and 10.2.2.0/24 subnets, respectively, to 10.0.0.0/8. This summary route will be installed into the routing table with an AD of 5 and a next-hop interface of Null0. This lower administrative distance value will prevent either router from accepting or installing the 10.0.0.0/8 summary from the other router, as illustrated in the following output:

```
R2#debug eigrp fsm

EIGRP FSM Events/Actions debugging is on

R2#

R2#

*Mar 13 03:24:31.983: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 150.1.1.1
(FastEthernet0/0) is up: new adjacency

*Mar 13 03:24:33.995: DUAL: dest(10.0.0.0/8) not active

*Mar 13 03:24:33.995: DUAL: rcvupdate: 10.0.0.0/8 via 150.1.1.1 metric 156160/128256

*Mar 13 03:24:33.995: DUAL: Find FS for dest 10.0.0.0/8. FD is 128256, RD is 128256

*Mar 13 03:24:33.995: DUAL:     0.0.0.0 metric 128256/0

*Mar 13 03:24:33.995: DUAL:     150.1.1.1 metric 156160/128256 found Dmin is 128256

*Mar 13 03:24:33.999: DUAL: RT installed 10.0.0.0/8 via 0.0.0.0
```

In the debug output above, the local router receives the 10.0.0.0/8 route from neighbour 150.1.1.1 with a route metric of 156160/128256. However, DUAL also has the same route locally, due to summarisation, and this route has a route metric of 128256/0. The local route is therefore installed into the routing table instead because it has the better metric. The same would also be applicable on R1, which would install its local 10.0.0.0/8 route into the RIB instead. The result is that neither router would be able to ping the 10.x.x.x subnet of the other router. To resolve this issue, automatic summarisation should be disabled using the `no auto-summary` command on both of the routers, allowing the specific route entries to be advertised instead.

The primary use of the EIGRP router ID (RID) is to prevent routing loops. The RID is used to identify the originating router for external routes. If an external route is received with the same RID as the local router, the route will be discarded. However, duplicate RIDs do not affect any internal EIGRP routes. This feature is designed to reduce the possibility of routing loops in networks where route redistribution is being performed on more than one ASBR. The

https://t.me/learningnets

originating RID can be viewed in the output of the `show ip eigrp topology` command, as illustrated below:

```
R1#show ip eigrp topology 2.2.2.2 255.255.255.255
IP-EIGRP (AS 1): Topology entry for 2.2.2.2/32
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 156160
  Routing Descriptor Blocks:
  150.1.1.2 (FastEthernet0/0), from 150.1.1.2, Send flag is 0x0
      Composite metric is (156160/128256), Route is External
      Vector metric:
        Minimum bandwidth is 100000 Kbit
        Total delay is 5100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 2.2.2.2
        AS number of route is 0
        External protocol is Connected, external metric is 0
        Administrator tag is 0 (0x00000000)
```

If you suspect a potential duplicate RID issue, you can check the events in the EIGRP event log to see if any routes have been rejected because of a duplicate RID. The following illustrates a sample output of the EIGRP event log, showing routes that have been rejected because they were received from a router with the same RID as the local router:

```
R2#show ip eigrp events
Event information for AS 1:
...
[Truncated Output]
21   03:05:39.747 Ignored route, neighbor info: 10.0.0.1 Serial0/0
22   03:05:39.747 Ignored route, dup router: 150.1.1.254
23   03:05:06.659 Ignored route, metric: 192.168.2.0 284160
24   03:05:06.659 Ignored route, neighbor info: 10.0.0.1 Serial0/0
25   03:05:06.659 Ignored route, dup router: 150.1.1.254
26   03:04:33.311 Ignored route, metric: 192.168.1.0 284160
27   03:04:33.311 Ignored route, neighbor info: 10.0.0.1 Serial0/0
28   03:04:33.311 Ignored route, dup router: 150.1.1.254
...
[Truncated Output]
```

The resolution for the solution above would be to change the RID on neighbour router 10.0.0.1 or on the local router, depending upon which one of the two has been incorrectly configured.

https://t.me/learningnets

Finally, it is important to remember that EIGRP will not install routes into the routing table if they do not meet the Feasibility Condition. This is true even if the `variance` command has been configured on the local router. It is a common misconception that issuing the `variance` command will allow EIGRP to load share over any paths whose route metric is *x* times that of the successor metric. Consider the topology illustrated in Figure 37.2 below, for example:

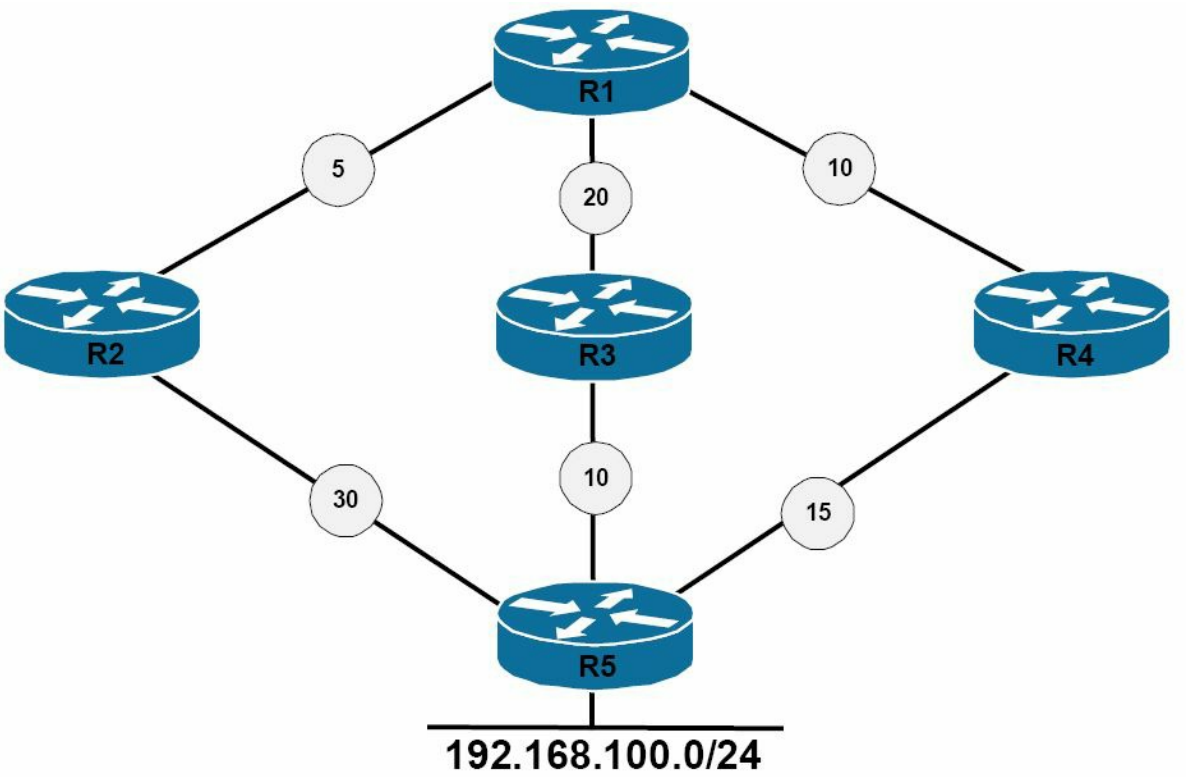


Figure 37.2 – Understanding the Feasibility Condition

Figure 37.2 shows a basic network that includes metrics from R1 to the 192.168.100.0/24 subnet. Referencing Figure 37.2, Table 37.1 below displays the Reported Distance and Feasible Distance values as seen on R1 for the 192.168.100.0/24 network:

Table 37.1 – R1 Paths and Distances

Network Path	R1 Neighbour	Neighbour Metric (RD)	R1 Feasible Distance
R1 – R2 – R5	R2	30	35
R1 – R3 – R5	R3	10	30
R1 – R4 – R5	R4	15	25

R1 has been configured to load share across all paths and the `variance 2` command is added to the router configuration. This allows EIGRP to load share across paths with up to twice the metric of the Successor route, which would include all three paths based on the default metric calculation. However, despite this configuration, only two paths will be installed and used.

First, R1 will select the path through R4 as the Successor route based on the FD for the route, which is 25. This route will be placed into the IP routing table as well as the EIGRP topology table. The metric for neighbour R3 to the 192.168.100.0/24 network, also referred to as the Reported Distance or Advertised Distance, is 10. This is less than the FD, and so this route meets the FC and is placed into the EIGRP topology table.

https://t.me/learningnets

The metric for neighbour R2 to the 192.168.100.0/24 network is 30. This value is higher than the FD of 25. This route does not meet the FC and is not considered a Feasible Successor. The route, however, is still placed into the EIGRP topology table. However, the path will not be used for load sharing, even though the metric falls within the range specified by the configuration of the `variance 2` EIGRP router configuration command. In such situations, consider using EIGRP offset lists to ensure that all routes are considered.

Troubleshooting Route Advertisement

There are times when it may seem that EIGRP is either not advertising the networks that it has been configured to advertise or is advertising networks that it has not been configured to advertise. For the most part, such issues are typically due to router and switch misconfigurations. There are several reasons why EIGRP might not advertise a network that it has been configured to advertise. Some of these reasons include the following:

- Distribute lists (outside CCNA syllabus)
- Split horizon
- Summarisation

Incorrectly configured distribute lists are one reason why EIGRP might not advertise a network that it has been configured to advertise. When configuring distribute lists, ensure that all networks that should be advertised are permitted by the referenced IP ACL or IP Prefix List.

Another common issue pertaining to network advertisement when using EIGRP is the default behaviour of split horizon. Split horizon is a Distance Vector protocol feature that mandates that routing information cannot be sent back out of the same interface through which it was received. This prevents the re-advertising of information back to the source from which it was learned, effectively preventing routing loops. This concept is illustrated in Figure 37.3 below:

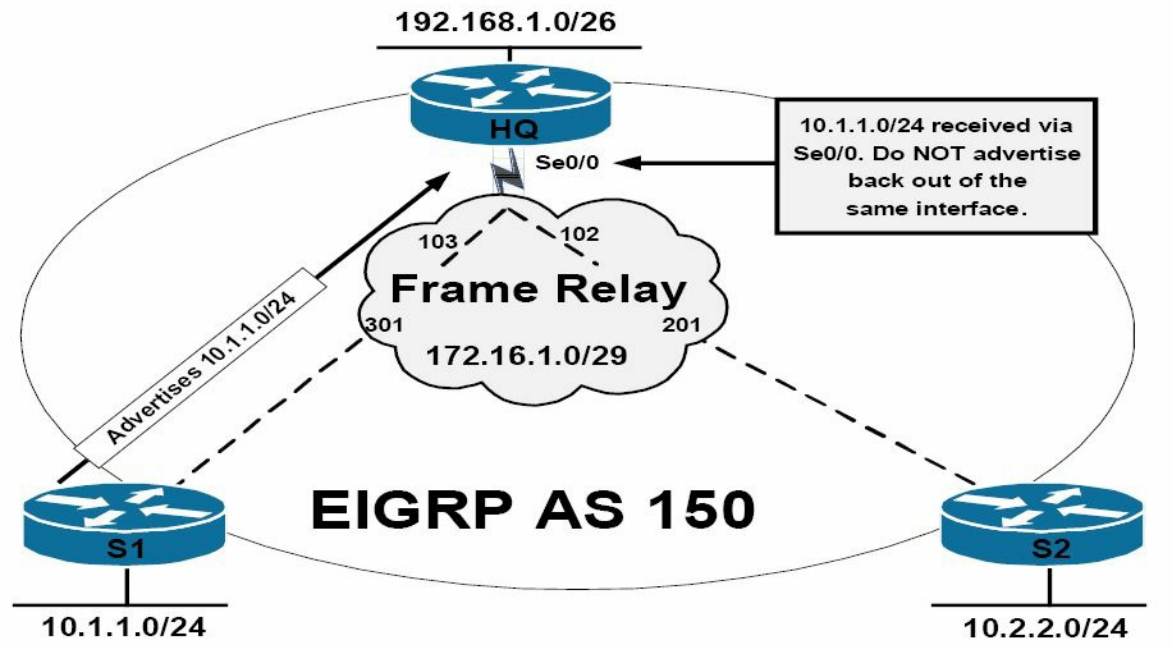


Figure 37.3 – EIGRP Split Horizon

The topology in Figure 37.3 illustrates a classic hub-and-spoke network, with router HQ as the

https://t.me/learningnets

hub router and routers S1 and S2 as the two spoke routers. On the Frame Relay WAN, each spoke router has a single DLCI provisioned between itself and the HQ router in a partial-mesh topology. By default, EIGRP split horizon is enabled for WAN interfaces connected to packet-switched networks, such as Frame Relay. This means that the HQ router will not advertise routing information learned on Serial0/0 out of the same interface.

The effect of this default behaviour is that the HQ router will not advertise the 10.1.1.0/24 prefix received from S1 to S2 because the route is received via the Serial0/0 interface, and the split horizon feature prevents the router from advertising information learned on that interface back out of the same interface. The same is also applicable for the 10.2.2.0/24 prefix the HQ router receives from S2. The recommended solution for this problem would be to disable the split horizon feature on the WAN interface using the `no ip split-horizon eigrp [asn]` interface configuration command on the HQ router.

By default, automatic summarisation at the classful boundary is enabled for EIGRP. This can be validated using the `show ip protocols` command. In addition to automatic summarisation, EIGRP also supports manual summarisation at the interface level. Regardless of the method implemented, summarisation prevents the more specific route entries that are encompassed by the summary from being advertised to neighbour routers. If route summarisation is configured incorrectly, it may appear that EIGRP is not advertising certain networks. For example, consider the basic network topology that is illustrated in Figure 37.4 below:

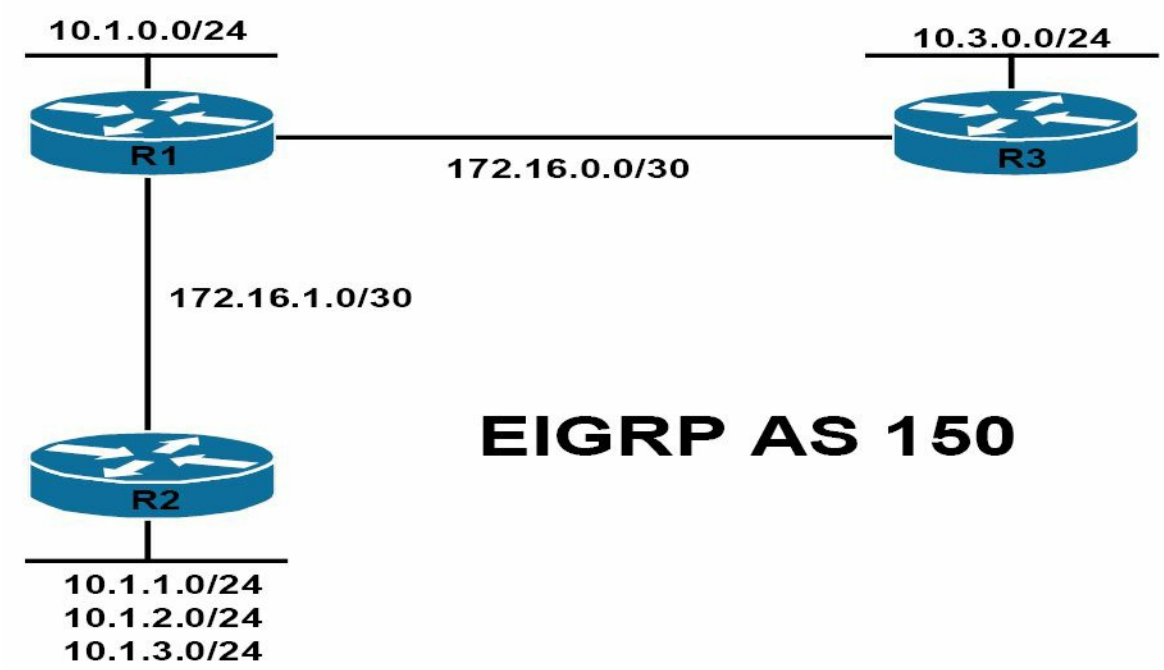


Figure 37.4 – EIGRP Summarisation

Referencing Figure 37.4, all routers reside in EIGRP Autonomous System 150. R2 is advertising the 10.1.1.0/24, 10.1.2.0/24, and 10.1.3.0/24 subnets to R1 via EIGRP. R1, which also has an interface assigned to the 10.1.0.0/24 subnet, should in turn advertise these subnets to R3. The EIGRP configuration on router R2 has been implemented as follows:

```
R2(config)#router eigrp 150
R2(config-router)#network 10.1.1.0 0.0.0.255
R2(config-router)#network 10.1.2.0 0.0.0.255
```

https://t.me/learningnets

```
R2(config-router)#network 10.1.3.0 0.0.0.255
R2(config-router)#network 172.16.1.0 0.0.0.3
R2(config-router)#no auto-summary
R2(config-router)#exit
```

The EIGRP configuration on R1 has been implemented as follows:

```
R1(config)#router eigrp 150
R1(config-router)#network 10.1.0.0 0.0.0.255
R1(config-router)#network 172.16.0.0 0.0.0.3
R1(config-router)#network 172.16.1.0 0.0.0.3
R1(config-router)#exit
```

Finally, the EIGRP configuration on R3 has been implemented as follows:

```
R3(config)#router eigrp 150
R3(config-router)#network 172.16.0.0 0.0.0.3
R3(config-router)#no auto-summary
R3(config-router)#exit
```

After this configuration, the routing table on R2 displays the following entries:

```
R2#show ip route eigrp
     172.16.0.0/30 is subnetted, 2 subnets
D       172.16.0.0 [90/2172416] via 172.16.1.1, 00:02:38, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
D       10.0.0.0/8 [90/156160] via 172.16.1.1, 00:00:36, FastEthernet0/0
```

The routing table on R1 displays the following entries:

```
R1#show ip route eigrp
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:01:01, Null0
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
D       10.1.3.0/24 [90/156160] via 172.16.1.2, 00:21:01, FastEthernet0/0
D       10.3.0.0/24 [90/2297856] via 172.16.0.2, 00:00:39, Serial0/0
D       10.1.2.0/24 [90/156160] via 172.16.1.2, 00:21:01, FastEthernet0/0
D       10.1.1.0/24 [90/156160] via 172.16.1.2, 00:21:01, FastEthernet0/0
D       10.0.0.0/8 is a summary, 00:01:01, Null0
```

Finally, the routing table on R3 displays the following entries:

```
R3#show ip route eigrp
     172.16.0.0/30 is subnetted, 2 subnets
D       172.16.1.0 [90/2172416] via 172.16.0.1, 00:21:21, Serial0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.0.0.0/8 [90/2297856] via 172.16.0.1, 00:01:15, Serial0/0
```

https://t.me/learningnets

Because summarisation is enabled on R1, it appears that the EIGRP is no longer advertising the

specific subnets encompassed by the 10.0.0.0/8 summary. To allow the specific subnets to be advertised via EIGRP, automatic summarisation should be disabled on R1, as illustrated below:

```
R1(config)#router eigrp 150
R1(config-router)#no auto-summary
R1(config-router)#exit
```

After this, the routing table on R3 would display the following route entries:

```
R3#show ip route eigrp
     172.16.0.0/30 is subnetted, 2 subnets
D       172.16.1.0 [90/2172416] via 172.16.0.1, 00:00:09, Serial0/0
     10.0.0.0/24 is subnetted, 5 subnets
D       10.1.3.0 [90/2300416] via 172.16.0.1, 00:00:09, Serial0/0
D       10.1.2.0 [90/2300416] via 172.16.0.1, 00:00:09, Serial0/0
D       10.1.1.0 [90/2300416] via 172.16.0.1, 00:00:09, Serial0/0
D       10.1.0.0 [90/2297856] via 172.16.0.1, 00:00:09, Serial0/0
```

The same would also be applicable to R2, which would now display the specific entries for the 10.1.0.0/24 and 10.3.0.0/24 subnets, as follows:

```
R2#show ip route eigrp
     172.16.0.0/30 is subnetted, 2 subnets
D       172.16.0.0 [90/2172416] via 172.16.1.1, 00:00:10, FastEthernet0/0
     10.0.0.0/24 is subnetted, 5 subnets
D       10.3.0.0 [90/2300416] via 172.16.1.1, 00:00:10, FastEthernet0/0
D       10.1.0.0 [90/156160] via 172.16.1.1, 00:00:10, FastEthernet0/0
```

Debugging EIGRP Routing Issues

While primary emphasis has been placed on the use of `show` commands in the previous sections, this final section describes some of the debugging commands that can also be used to troubleshoot EIGRP. Keep in mind, however, that debugging is very processor intensive and should be used only as a last resort (i.e., after all `show` commands and other troubleshooting methods and tools have been applied or attempted).

The `debug ip routing [acl|static]` command is a powerful troubleshooting tool and command. It should be noted, however, that while this command is not EIGRP-specific, it provides useful and detailed information on routing table events. Following is a sample of the information that is printed by this command:

```
R1#debug ip routing
IP routing debugging is on
R1#
*Mar  3 23:03:35.673: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
*Mar  3 23:03:35.673: RT: is_up: FastEthernet0/0 0 state: 4 sub state: 1 line: 0
has_route: True
```

https://t.me/learningnets

```
*Mar  3 23:03:35.677: RT: interface FastEthernet0/0 removed from routing table
```

```
*Mar  3 23:03:35.677: RT: del 172.16.1.0/30 via 0.0.0.0, connected metric [0/0]
*Mar  3 23:03:35.677: RT: delete subnet route to 172.16.1.0/30
*Mar  3 23:03:35.677: RT: NET-RED 172.16.1.0/30
*Mar  3 23:03:35.677: RT: Pruning routes for FastEthernet0/0 (3)
*Mar  3 23:03:35.689: RT: delete route to 10.1.3.0 via 172.16.1.2, FastEthernet0/0
*Mar  3 23:03:35.689: RT: no routes to 10.1.3.0, flushing
*Mar  3 23:03:35.689: RT: NET-RED 10.1.3.0/24
*Mar  3 23:03:35.689: RT: delete route to 10.1.2.0 via 172.16.1.2, FastEthernet0/0
*Mar  3 23:03:35.689: RT: no routes to 10.1.2.0, flushing
*Mar  3 23:03:35.689: RT: NET-RED 10.1.2.0/24
*Mar  3 23:03:35.689: RT: delete route to 10.1.1.0 via 172.16.1.2, FastEthernet0/0
*Mar  3 23:03:35.689: RT: no routes to 10.1.1.0, flushing
*Mar  3 23:03:35.693: RT: NET-RED 10.1.1.0/24
*Mar  3 23:03:35.693: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 150: Neighbor 172.16.1.2
(FastEthernet0/0) is down: interface down
*Mar  3 23:03:39.599: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 150: Neighbor 172.16.1.2
(FastEthernet0/0) is up: new adjacency
*Mar  3 23:03:40.601: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
*Mar  3 23:03:40.601: RT: is_up: FastEthernet0/0 1 state: 4 sub state: 1 line: 1
has_route: False
*Mar  3 23:03:40.605: RT: SET_LAST_RDB for 172.16.1.0/30
  NEW rdb: is directly connected
*Mar  3 23:03:40.605: RT: add 172.16.1.0/30 via 0.0.0.0, connected metric [0/0]
*Mar  3 23:03:40.605: RT: NET-RED 172.16.1.0/30
*Mar  3 23:03:40.605: RT: interface FastEthernet0/0 added to routing table
*Mar  3 23:03:49.119: RT: SET_LAST_RDB for 10.1.1.0/24
  NEW rdb: via 172.16.1.2
*Mar  3 23:03:49.119: RT: add 10.1.1.0/24 via 172.16.1.2, eigrp metric [90/156160]
```

You can use this command in conjunction with an ACL to view information about the route or routes referenced in the ACL. Additionally, the same command can also be used for troubleshooting static route events on the local device. As a side note, instead of using this command, if you are running EIGRP, consider using the `show ip eigrp events` command instead, as it provides a history of EIGRP internal events and can be used to troubleshoot SIA issues, as well as route flaps and other events. Following is a sample of the information that is printed by this command:

```
R1#show ip eigrp events
Event information for AS 150:
1    23:03:49.135 Ignored route, metric: 192.168.3.0 28160
2    23:03:49.135 Ignored route, metric: 192.168.2.0 28160
3    23:03:49.135 Ignored route, metric: 192.168.1.0 28160
```

https://t.me/learningnets

```
4    23:03:49.131 Rcv EOT update src/seq: 172.16.1.2 85
5    23:03:49.127 Change queue emptied, entries: 3
6    23:03:49.127 Ignored route, metric: 192.168.3.0 28160
7    23:03:49.127 Ignored route, metric: 192.168.2.0 28160
8    23:03:49.127 Ignored route, metric: 192.168.1.0 28160
9    23:03:49.127 Metric set: 10.1.3.0/24 156160
10   23:03:49.127 Update reason, delay: new if 4294967295
11   23:03:49.127 Update sent, RD: 10.1.3.0/24 4294967295
12   23:03:49.127 Update reason, delay: metric chg 4294967295
13   23:03:49.127 Update sent, RD: 10.1.3.0/24 4294967295
14   23:03:49.123 Route install: 10.1.3.0/24 172.16.1.2
15   23:03:49.123 Find FS: 10.1.3.0/24 4294967295
16   23:03:49.123 Rcv update met/succmet: 156160 128256
17   23:03:49.123 Rcv update dest/nh: 10.1.3.0/24 172.16.1.2
18   23:03:49.123 Metric set: 10.1.3.0/24 4294967295
19   23:03:49.123 Metric set: 10.1.2.0/24 156160
20   23:03:49.123 Update reason, delay: new if 4294967295
21   23:03:49.123 Update sent, RD: 10.1.2.0/24 4294967295
22   23:03:49.123 Update reason, delay: metric chg 4294967295
...
[Truncated Output]
```

In addition to the `debug ip routing` command, two additional EIGRP-specific debugging commands are also available in Cisco IOS software. The `debug eigrp` command can be used to provide real-time information on the DUAL Finite State Machine, EIGRP neighbour relationships, Non-Stop Forwarding events, packets, and transmission events. The options that are available with this command are illustrated below:

```
R1#debug eigrp ?
  fsm        EIGRP Dual Finite State Machine events/actions
  neighbors  EIGRP neighbors
  nsf        EIGRP Non-Stop Forwarding events/actions
  packets    EIGRP packets
  transmit   EIGRP transmission events
```

In addition to the `debug eigrp` command, the `debug ip eigrp` command prints detailed information on EIGRP route events, such as how EIGRP processes incoming updates. The additional keywords that can be used in conjunction with this command are illustrated below:

```
R1#debug ip eigrp ?
  <1-65535>      Autonomous System
  neighbor       IP-EIGRP neighbor debugging
  notifications  IP-EIGRP event notifications
  summary        IP-EIGRP summary route processing
```

https://t.me/learningnets

```
  vrf            Select a VPN Routing/Forwarding instance
  <cr>
```

In conclusion, the following is a sample output of the `debug ip eigrp` command:

```
R1#debug ip eigrp
IP-EIGRP Route Events debugging is on
R1#
*Mar  3 23:49:47.028: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 150: Neighbor 172.16.1.2
(FastEthernet0/0) is up: new adjacency
*Mar  3 23:49:47.044: IP-EIGRP(Default-IP-Routing-Table:150): 10.1.0.0/24 - do advertise
out FastEthernet0/0
*Mar  3 23:49:47.044: IP-EIGRP(Default-IP-Routing-Table:150): Int 10.1.0.0/24 metric
128256 - 256 128000
*Mar  3 23:49:48.030: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
*Mar  3 23:49:56.179: IP-EIGRP(Default-IP-Routing-Table:150): Processing incoming UPDATE
packet
*Mar  3 23:49:56.544: IP-EIGRP(Default-IP-Routing-Table:150): Processing incoming UPDATE
packet
*Mar  3 23:49:56.544: IP-EIGRP(Default-IP-Routing-Table:150): Int 10.1.1.0/24 M 156160 -
25600 130560 SM 128256 - 256 128000
*Mar  3 23:49:56.544: IP-EIGRP(Default-IP-Routing-Table:150): route installed for
10.1.1.0  ()
*Mar  3 23:49:56.544: IP-EIGRP(Default-IP-Routing-Table:150): Int 10.1.2.0/24 M 156160 -
25600 130560 SM 128256 - 256 128000
*Mar  3 23:49:56.548: IP-EIGRP(Default-IP-Routing-Table:150): route installed for
10.1.2.0  ()
*Mar  3 23:49:56.548: IP-EIGRP(Default-IP-Routing-Table:150): Int 10.1.3.0/24 M 156160 -
25600 130560 SM 128256 - 256 128000
...
[Truncated Output]
```

https://t.me/learningnets

Day 37 Questions

1. Name at least three reasons for EIGRP neighbour relationships not forming.
2. Which command can you use to verify EIGRP K values?
3. Which command can you use to verify EIGRP packets statistics?
4. Name at least two common reasons for EIGRP route installation failures.
5. The administrative distance concept is used to determine how reliable the route source is. True or false?
6. By default, EIGRP automatically summarises at classful boundaries and creates a summary route pointing to the Null0 interface. True or false?
7. Which command can you can use to debug FSM events?
8. Which command can you use to see the originating router ID of a specific prefix?
9. Which command can you use to show the EIGRP event log?
10. What is the best command to use when debugging various routing issues?

https://t.me/learningnets

Day 37 Answers

1. The neighbour routers are not on a common subnet; mismatched primary and secondary subnets; mismatched K values; mismatched ASN; ACLs are filtering EIGRP packets; Physical Layer issues; Data Link Layer issues; and mismatched authentication parameters.
2. The `show ip protocols` command.
3. The `show ip eigrp traffic` command.
4. The same route is received via another protocol with a lower administrative distance;EIGRP summarisation; duplicate router IDs are present within the EIGRP domain; and the routes do not meet the Feasibility Condition.
5. True.
6. True.
7. The `debug eigrp fsm` command.
8. The `show ip eigrp topology x.x.x.x y.y.y.y` command.
9. The `show ip eigrp events` command.
10. The `debug ip routing` command.

https://t.me/learningnets

Day 37 Lab

Repeat the EIGRP lab from the previous day. In addition, test the EIGRP troubleshooting commands presented in this lesson:

- ☐ See the EIGRP parameters using the `show ip protocol` command
- ☐ Modify K values on both routers and issue the command again
- ☐ Notice that different configured K values lead to EIGRP neighbour relationships being lost
- ☐ Verify the Hello packets being transmited by issuing the `show ip eigrp traffic` command
- ☐ Test the `debug eigrp fsm` command
- ☐ Test the `show ip eigrp topology` command for the advertised route and notice the originating RID; change the RID on the remote router and issue the command again
- ☐ Verify the `show ip eigrp events` command
- ☐ Start the debug IP routing before advertising the network into EIGRP; notice the generated debug updates

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 38 – EIGRP For IPv6

Day 38 Tasks

- Read today's lesson notes (below)
- Review the EIGRP module
- Review the EIGRP Troubleshooting module

Although EIGRP for IPv6 is not specifically listed in the new CCNA exam syllabus, it will be covered in this module for a number of reasons. First, the CCNA topics have a great focus on EIGRP and IPv6 technologies and EIGRPv6 topics may appear in the exam, even though this is not very likely. Second, the topic is relatively easy and straightforward, so it should not take long to understand it, especially considering that the explanations will not be in-depth.

In addition to open standard protocols, the Cisco-proprietary EIGRP has also been modified to support IPv6. This modified version of EIGRP is sometimes referred to as EIGRPv6 because of its support for IPv6, not because it is revision 6 of the EIGRP routing protocol. Similarly, EIGRP for IPv4 is also sometimes referred to as EIGRPv4 to differentiate between the routing protocol versions supported by either version.

Today you will learn about the following:

- Cisco EIGRP for IPv6 overview and fundamentals
- EIGRP for IPv6 configuration fundamentals

This lesson maps to the following CCNA syllabus requirement:

- Configure and verify EIGRP (single AS)

For the most part, EIGRPv6 retains the same basic core functions as EIGRPv4. For example, both versions still use DUAL to ensure loop-free paths, and both protocols use Multicast packets to send updates – although EIGRPv6 uses IPv6 Multicast address FF02::A instead of the 224.0.0.10 group address used by EIGRPv4. While the same core fundamentals are retained, there are some differences between these versions. Table 38.1 below lists the differences between EIGRPv4 and EIGRPv6, or simply and more commonly between EIGRP for IPv4 and EIGRP for IPv6:

Table 38.1 – EIGRPv4 and EIGRPv6 Differences

Protocol Characteristic	EIGRP for IPv4	EIGRP for IPv6
Automatic Summarisation	Yes	Not Applicable
Authentication or Security	MD5	Built into IPv6
Common Subnet for Peers	Yes	No
Advertisement Contents	Subnet/Mask	Prefix/Length
Packet Encapsulation	IPv4	IPv6

https://t.me/learningnets

NOTE: Because EIGRPv6 uses the Link-Local address of the neighbour as the next-hop address, the global IPv6 Unicast subnets do not need to be the same for a neighbour relationship to be established between two routers that reside within the same autonomous system and are on a common network segment. This is one of the most significant differences between EIGRPv4, which requires neighbours to be on a common subnet, and EIGRPv6, which negates this need by using the Link-Local addresses for neighbour relationships instead.

Cisco IOS Software EIGRPv4 and EIGRPv6 Configuration Differences

There are some notable differences in the configuration of EIGRPv4 and EIGRPv6 in Cisco IOS software. The first notable difference is the way in which the routing protocol is enabled. For EIGRPv4, the `router eigrp [ASN]` global configuration command is required to enable EIGRPv4 routing and to specify the EIGRPv4 autonomous system number (ASN). When configuring EIGRPv6, the `ipv6 router eigrp [ASN]` global configuration command is used instead to enable EIGRPv6 and to specify the local router ASN.

While enabling EIGRPv4 and EIGRPv6 is somewhat similar, there is a very notable and significant difference in the protocol states once the routing process has been enabled. By default, when EIGRPv4 is enabled, the protocol automatically starts and, assuming correct configuration, begins sending Hello packets on all specified operational interfaces. When enabling EIGRPv6 in Cisco IOS software, by default, after the protocol has been enabled, it remains in the shutdown state. This means that even if enabled under specified interfaces, the EIGRP process will not be operational until the `no shutdown` router configuration command is issued.

Yet another configuration difference between EIGRPv4 and EIGRPv6 is that with EIGRPv6, the router ID is mandatory and must be specified in IPv4 dotted-decimal notation. When assigning the RID, keep in mind that the address does not have to be a routable or reachable address.

NOTE: If there are any interfaces with IPv4 addresses configured on the local router, then the router will select the router ID from these interfaces – preferring Loopback interfaces, and then using physical interfaces if no Loopback interfaces are configured or operational on the router. The highest IP address of the Loopback interface(s), if up, will be selected. If not, the RID will be selected from the highest IP address of the physical interfaces, if up. If neither is configured on the router, the `eigrp router-id [IPv4 Address]` command must be used.

Configuring and Verifying EIGRPv6 in Cisco IOS Software

Continuing from the previous section, which highlighted the configuration differences between EIGRPv4 and EIGRPv6, this section goes through the sequence of steps required to enable and verify EIGRPv6 functionality and routing in Cisco IOS software, as follows:

1. Globally enable IPv6 routing using the `ipv6 unicast-routing` global configuration command. By default, IPv6 routing is disabled in Cisco IOS software.
2. Configure one or more EIGRPv6 processes using the `ipv6 router eigrp [ASN]` global configuration command.
3. If there are no operational interfaces with an IPv4 address configured on the router, then

https://t.me/learningnets

configure the EIGRPv6 RID manually using the `eigrp router-id [IPv4 Address]` router configuration command.

4. Enable the EIGRPv6 process(es) using the `no shutdown` router configuration command.
5. Enable IPv6 on the desired interfaces using the `ipv6 address` and `ipv6 enable` interface configuration commands.
6. Enable one or more EIGRPv6 processes under the interface using the `ipv6 eigrp [ASN]` interface configuration command.

Because automatic summarisation is not applicable to EIGRPv6, there is no need to disable this behaviour. To solidify the configuration of EIGRPv6, consider the topology illustrated in Figure 38.1 below, which illustrates a network comprised of two routers. Both routers will be running EIGRPv6 using AS 1. Router R3 will be advertising two additional prefixes via EIGRPv6:

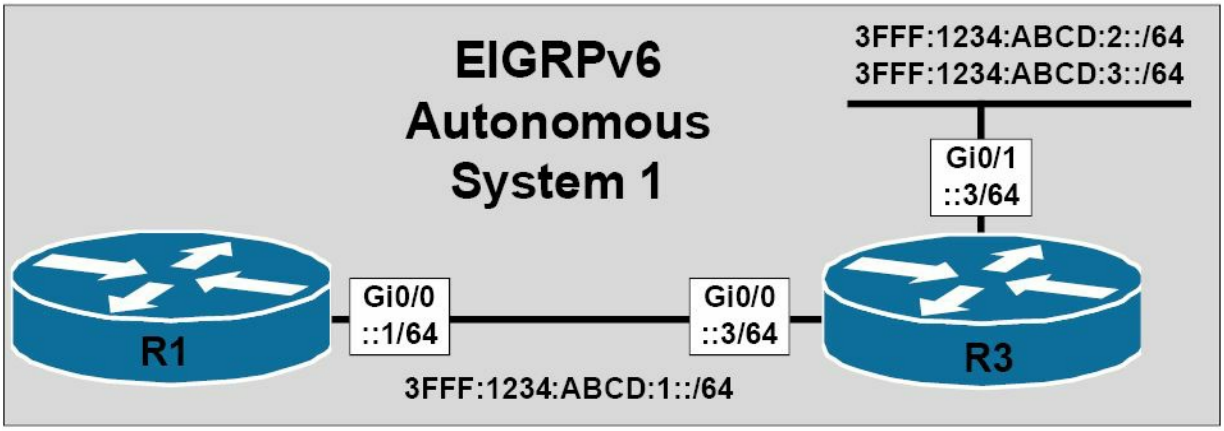


Figure 38.1 – Configuring EIGRPv6 in Cisco IOS Software

Following the sequence of configuration steps described above, EIGRPv6 will be configured on router R1 as follows:

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router eigrp 1
R1(config-rtr)#eigrp router-id 1.1.1.1
R1(config-rtr)#no shutdown
R1(config-rtr)#exit
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ipv6 address 3fff:1234:abcd:1::1/64
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 eigrp 1
R1(config-if)#exit
```

Following the same sequence of steps, EIGRPv6 routing is configured on router R3 as follows:

```
R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router eigrp 1
R3(config-rtr)#eigrp router-id 3.3.3.3
R3(config-rtr)#no shutdown
R3(config-rtr)#exit
```

https://t.me/learningnets

```
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ipv6 address 3fff:1234:abcd:1::3/64
R3(config-if)#ipv6 enable
R3(config-if)#ipv6 eigrp 1
R3(config-if)#exit
R3(config)#interface GigabitEthernet0/1
R3(config-if)#ipv6 address 3fff:1234:abcd:2::3/64
R3(config-if)#ipv6 address 3fff:1234:abcd:3::3/64
R3(config-if)#ipv6 enable
R3(config-if)#ipv6 eigrp 1
R3(config-if)#exit
```

The verification process for EIGRPv6 follows the same as that for EIGRPv4. First, verify that the EIGRP neighbour relationships have been established successfully. For EIGRPv6, this is performed using the `show ipv6 eigrp neighbors` command, as illustrated below:

```
R1#show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(1)
H   Address                 Interface Hold Uptime    SRTT   RTO Q   Seq
                                      (sec)          (ms)       Cnt Num
0   Link-local address:  Gi0/0      13  00:01:37  1200       0   3
    FE80::1AEF:63FF:FE63:1B00
```

As was stated earlier, notice that the next-hop address (i.e., EIGRP neighbour address) is specified as the Link-Local address, rather than the global Unicast address. All of the other information printed by this command is the same as that printed for the `show ip eigrp neighbors` command. To view detailed neighbour information, you can simply append the `[detail]` keyword to the end of the `show ipv6 eigrp neighbors` command. Using this option prints information on the EIGRP version, as well as the number of prefixes received from that particular EIGRP neighbour, as illustrated below:

```
R1#show ipv6 eigrp neighbors detail
EIGRP-IPv6 Neighbors for AS(1)
H   Address                 Interface Hold Uptime   SRTT   RTO Q   Seq
                                      (sec)          (ms)       Cnt Num
0   Link-local address:   Gi0/0     12   00:01:52 1200       0   3
    FE80::1AEF:63FF:FE63:1B00
   Version 5.0/3.0, Retrans: 1, Retries: 0, Prefixes: 3
   Topology-ids from peer - 0
```

Following the verification of the EIGRPv6 neighbour relationships, you can then verify routing information. For example, to view the IPv6 prefixes received from EIGRPv6 neighbours, you would use the `show ipv6 route` command, as illustrated in the following output:

```
R1#show ipv6 route eigrp
IPv6 Routing Table - default - 6 entries
```

https://t.me/learningnets

```
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS inter area, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery
D   3FFF:1234:ABCD:2::/64 [90/3072]
     via FE80::1AEF:63FF:FE63:1B00, GigabitEthernet0/0
D   3FFF:1234:ABCD:3::/64 [90/3072]
     via FE80::1AEF:63FF:FE63:1B00, GigabitEthernet0/0
```

Again, notice that the received prefixes all contain the Link-Local address of the neighbour as the next-hop IPv6 address for all received prefixes. To view the EIGRPv6 topology table, the `show ipv6 eigrp topology` command should be used. This command supports the same options as those available with the `show ip eigrp topology` command used to view the EIGRPv4 topology table. Based on the implemented configuration, the topology table on R1 displays the following IPv6 prefix information:

```
R1#show ipv6 eigrp topology
EIGRP-IPv6 Topology Table for AS(1)/ID(1.1.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 3FFF:1234:ABCD:2::/64, 1 successors, FD is 3072
        via FE80::1AEF:63FF:FE63:1B00 (3072/2816), GigabitEthernet0/0
P 3FFF:1234:ABCD:1::/64, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/0
P 3FFF:1234:ABCD:3::/64, 1 successors, FD is 3072
        via FE80::1AEF:63FF:FE63:1B00 (3072/2816), GigabitEthernet0/0
```

As is the case with EIGRPv4, you can append a prefix to the end of this command in order to view the detailed information on that prefix or subnet. For example, to view detailed information on the 3FFF:1234:ABCD:2::/64 subnet, you would simply enter the `show ipv6 eigrp topology 3FFF:1234:ABCD:2::/64` command, as illustrated below:

```
R1#show ipv6 eigrp topology 3FFF:1234:ABCD:2::/64
EIGRP-IPv6 Topology Entry for AS(1)/ID(1.1.1.1) for 3FFF:1234:ABCD:2::/64
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 3072
  Descriptor Blocks:
  FE80::1AEF:63FF:FE63:1B00 (GigabitEthernet0/0), from FE80::1AEF:63FF:FE63:1B00, Send
flag is 0x0
      Composite metric is (3072/2816), route is Internal
      Vector metric:
        Minimum bandwidth is 1000000 Kbit
        Total delay is 20 microseconds
        Reliability is 255/255
        Load is 1/255
```

https://t.me/learningnets

```
        Minimum MTU is 1500
        Hop count is 1
        Originating router is 3.3.3.3
```

Finally, a simple ping can and should be used to verify connectivity between subnets. The following is a ping from R1 to the `3FFF:1234:ABCD:2::3` address on R3:

```
R1#ping 3FFF:1234:ABCD:2::3 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 3FFF:1234:ABCD:2::3, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 0/0/4 ms
```

As is the case with EIGRPv4, the default protocol values for EIGRPv6 can be validated using the `show ipv6 protocols` command, the output of which is printed below. This command includes the interfaces enabled for the EIGRP instance, the route redistribution information (if applicable), and the manually specified or configured dotted-decimal EIGRPv6 router ID.

```
R1#show ipv6 protocols
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  NSF-aware route hold timer is 240
  Router-ID: 1.1.1.1
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1
  Interfaces:
    GigabitEthernet0/0
  Redistribution:
```

https://t.me/learningnets

Day 38 Questions

1. IPv6 security for EIGRPv6 is built-in. True or false?
2. Because EIGRPv6 uses the Link-Local address of the neighbour as the next-hop address, the global IPv6 Unicast subnets do not need to be the same in order for a neighbour relationship to be established between two routers that reside within the same autonomous system and are on a common network segment. True or false?
3. Which command do you use to enter EIGRP for IPv6 Router Configuration mode?
4. Which state is the EIGRP for IPv6 initially in (active or shutdown)?
5. How do you enable EIGRP for IPv6 on a router interface?

https://t.me/learningnets

Day 38 Answers

1. True.
2. True.
3. The `ipv6 router eigrp [ASN]` command.
4. The shutdown state.
5. Issue the `ipv6 eigrp [ASN]` command.

https://t.me/learningnets

Day 38 Lab

Repeat the EIGRP lab from Day 36, this time using IPv6 addresses and activating EIGRP for IPv6:

- ☐ Enable IPv6 Unicast routing on both routers
- ☐ Configure IPv6 addresses on the interfaces
- ☐ Configure the EIGRP process using the `ipv6 router eigrp 100` command
- ☐ Configure a RID using the `eigrp router-id 10.10.10.10` command
- ☐ Activate the process using the `no shutdown` command
- ☐ Enable EIGRP on the IPv6 interfaces using the `ipv6 eigrp 10` command
- ☐ Verify the neighbour relationships using the `show ipv6 eigrp neighbors [detail]` command
- ☐ Verify the advertised route(s) using the `show ipv6 route eigrp` command
- ☐ Verify the EIGRP topology using the `show ipv6 eigrp topology` command

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 39 – OSPF

Day 39 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's lab
- Read the ICND2 cram guide
- Spend 15 minutes on the subnetting.org website

As with EIGRP, we could discuss OSPF over several days, but we need to stick to what you need to know for your exam. Even CCNA-level OSPF knowledge wouldn't be sufficient to design and deploy it on most networks.

Today you will learn about the following:

- OSPF operations
- DR and BDR
- Configuring OSPF
- Troubleshooting OSPF

This lesson maps to the following CCNA syllabus requirements:

- Configure and verify OSPF (single area)
- Neighbour adjacencies
- OSPF states
- Discuss multi-area
- Configure OSPFv2
- Router ID
- LSA types

Designated and Backup Designated Routers

As stated in the Day 12 module, OSPF elects a Designated Router (DR) and/or a Backup Designated Router (BDR) on Broadcast and Non-Broadcast network types. It is important to understand that the BDR is not a mandatory component on these network types. In fact, OSPF will work just as well when only a DR is elected and there is no BDR; however, there will be no redundancy if the DR fails and the OSPF routers need to go through the election process again to elect a new DR.

On the segment (on Broadcast and Non-Broadcast network types), each individual non-DR/BDR router establishes an adjacency with the DR and, if one has also been elected, the BDR, but not

with any other non-DR/BDR routers on the segment. The DR and BDR routers are fully adjacent with each other and all other routers on the segment. The non-DR/BDR routers send messages and updates to the AllDRRouters Multicast group address 224.0.0.6. Only the DR/BDR routers listen to Multicast messages sent to this group address. The DR then advertises messages to the AllSPFRouters Multicast group address 224.0.0.5. This allows all other OSPF routers on the segment to receive the updates.

It is important to understand the sequence of message exchanges when a DR and/or a BDR router have been elected. As an example, imagine a Broadcast network with four routers, which are R1, R2, R3, and R4. Assume that R4 has been elected DR, and R3 has been elected BDR. R2 and R1 are neither DR nor BDR and are therefore referred to as DROther routers in Cisco OSPF terminology. A configuration change is made on R1, and R1 then sends an update to the AllDRRouters Multicast group address 224.0.0.6. R4, the DR, receives this update and sends an acknowledgement back to the AllSPFRouters Multicast group address 224.0.0.5. R4 then sends this update to all other non-DR/BDR routers using the AllSPFRouters Multicast group address. This update is received by the other DROther router, R2, and R2 sends an acknowledgement to the AllDRRouters Multicast group 224.0.0.6. This is illustrated in Figure 39.1 below:

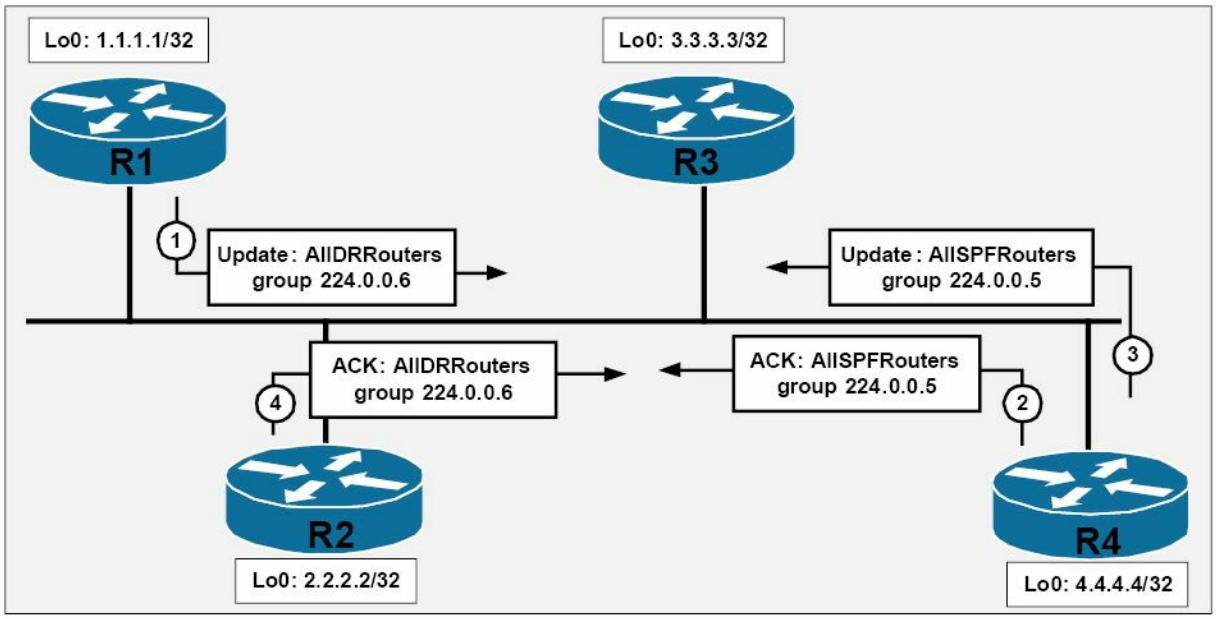


Figure 39.1 – OSPF DR and BDR Advertisements

NOTE: The BDR simply listens to the packets sent to both Multicast groups.

In order for a router to be the DR or the BDR for the segment, the router must be elected. This election is based on the following:

- The highest router priority value
- The highest router ID

By default, all routers have a default priority value of 1. This value can be adjusted using the `ip ospf priority <0-255>` interface configuration command. The higher the priority, the greater the likelihood the router will be elected DR for the segment. The router with the second-highest priority will then be elected BDR. If a priority value of 0 is configured, the router will not

https://t.me/learningnets

participate in the DR/BDR election process. The highest router priority and router ID are important only if OSPF processes loads at the same time on all routers participating in the DR/BDR election process. Otherwise the router that finishes loading the OSPF process first will become the DR on the segment.

When determining the OSPF router ID, Cisco IOS selects the highest IP address of configured Loopback interfaces. If no Loopback interfaces are configured, the software uses the highest IP address of all configured physical interfaces as the OSPF router ID. Cisco IOS software also allows administrators to specify the router ID manually using the `router-id [address]` router configuration command.

It is important to remember that with OSPF, once the DR and the BDR have been elected, they will remain as DR/BDR routers until a new election is held. For example, if a DR and a BDR exist on a Multi-Access network and a router with a higher priority or IP address is added to the same segment, the existing DR and BDR routers will not change. If the DR fails, the BDR will assume the role of the DR, not the new router with the higher priority or IP address. Instead, a new election will be held and that router will most likely be elected BDR. In order for that router to become the DR, the BDR must be removed or the OSPF process must be reset using the `clear ip ospf` command, forcing a new DR/BDR election. Once elected, OSPF uses the DR and the BDR routers as follows:

- To reduce the number of adjacencies required on the segment
- To advertise the routers on the Multi-Access segment
- To ensure that updates are sent to all routers on the segment

To better understand these fundamental concepts, reference the basic OSPF network topology illustrated in Figure 39.2 below:

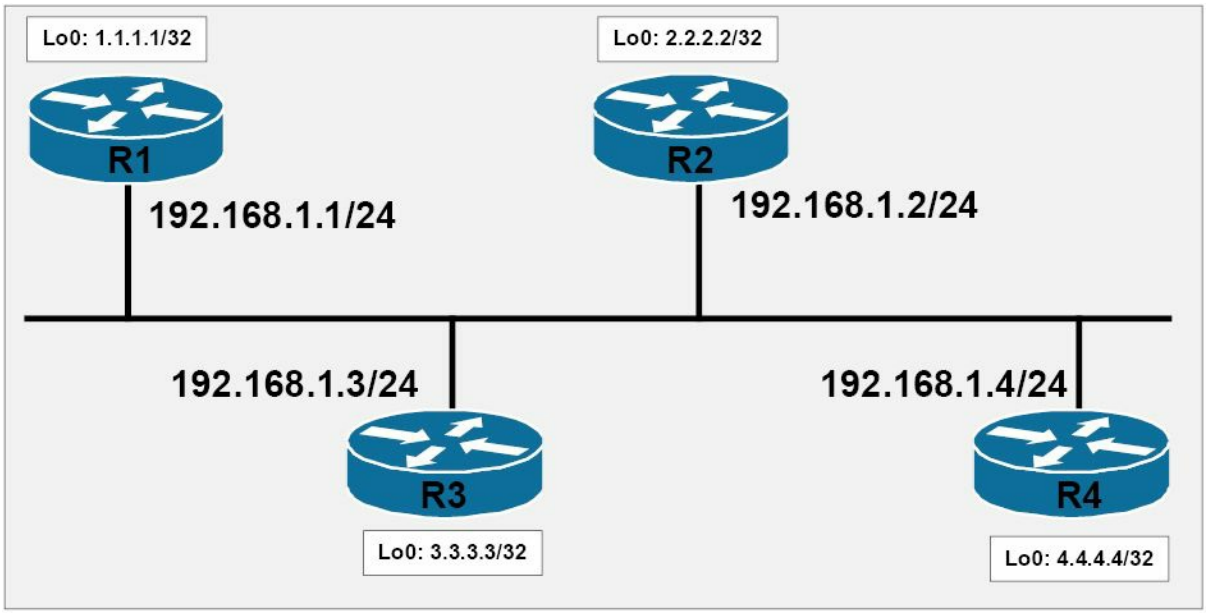


Figure 39.2 – OSPF DR and BDR Fundamentals

Referencing Figure 39.2, each router on the segment establishes an adjacency with the DR and the BDR but not with each other. In other words, non-DR/BDR routers do not establish an adjacency with each other. This prevents the routers on the segment from forming N(N-1)

https://www.learningnets

adjacencies with each other, which reduces excessive OSPF packet flooding on the segment.

For example, without the concept of a DR/BDR on the segment, each individual router would need to establish an adjacency with every other router on the segment. This would result in 4(4-1) or 12 adjacencies on the segment. However, with the DR/BDR, each individual router needs to establish an adjacency with only these two routers and no other non-DR and BDR routers. The DR and the BDR also establish an adjacency between themselves. This reduces the number of adjacencies required on the segment and on each individual OSPF router, which in turn reduces resources consumption (e.g., memory and processor utilisation) on the routers.

Regarding the second point, OSPF views a link as a connection between two routers or nodes. In Multi-Access networks, such as Ethernet, multiple routers can reside on the same segment, as illustrated in Figure 39.2. On such networks, OSPF uses the Network Link State Advertisement (Type 2 LSA) to advertise the routers on the Multi-Access segment. This LSA is generated by the DR and is flooded only within the area. Because the other non-DR/BDR routers do not establish adjacencies with each other, this LSA allows those routers to know about the other routers on the Multi-Access segment.

To further clarify this point, referencing Figure 39.2, assuming that all routers on the segment have the default OSPF priority value of 1 (and load the OSPF process at the same time), R4 is elected as the DR for the segment because it has the highest router ID. R3 is elected as the BDR for the segment because it has the second-highest router ID. Because R2 and R1 are neither the DR nor the BDR, they are referred to as DROther routers in Cisco terminology. This can be validated using the `show ip ospf neighbor` command on all routers, as follows:

```
R1#show ip ospf neighbor
Neighbor ID   Pri   State           Dead Time   Address         Interface
2.2.2.2         1   2WAY/DROTHER    00:00:38    192.168.1.2     Ethernet0/0
3.3.3.3         1   FULL/BDR        00:00:39    192.168.1.3     Ethernet0/0
4.4.4.4         1   FULL/DR         00:00:38    192.168.1.4     Ethernet0/0

R2#show ip ospf neighbor
Neighbor ID  Pri   State           Dead Time   Address         Interface
1.1.1.1        1   2WAY/DROTHER    00:00:32    192.168.1.1     FastEthernet0/0
3.3.3.3        1   FULL/BDR        00:00:33    192.168.1.3     FastEthernet0/0
4.4.4.4        1   FULL/DR         00:00:32    192.168.1.4     FastEthernet0/0

R3#show ip ospf neighbor
Neighbor ID  Pri   State           Dead Time   Address         Interface
1.1.1.1        1   FULL/DROTHER    00:00:36    192.168.1.1     FastEthernet0/0
2.2.2.2        1   FULL/DROTHER    00:00:36    192.168.1.2     FastEthernet0/0
4.4.4.4        1   FULL/DR         00:00:35    192.168.1.4     FastEthernet0/0

R4#show ip ospf neighbor
```

https://t.me/learningnets

```
Neighbor ID  Pri   State           Dead Time   Address         Interface
1.1.1.1        1   FULL/DROTHER    00:00:39    192.168.1.1     FastEthernet0/0
2.2.2.2        1   FULL/DROTHER    00:00:39    192.168.1.2     FastEthernet0/0
3.3.3.3        1   FULL/BDR        00:00:30    192.168.1.3     FastEthernet0/0
```

NOTE: The DROther routers remain in the 2WAY/DROTHER state because they exchange their databases only with the DR and BDR routers. Therefore, because there is no full database exchange between the DROther routers, they will never reach the OSPF FULL adjacency state.

Because R4 has been elected DR, it generates the Network LSA, which advertises the other routers on the Multi-Access segment. This can be verified using the `show ip ospf database network [link state ID]` command on any router on the segment or the `show ip ospf database network self-originate` command on the DR only. The following illustrates the output of the `show ip ospf database network self-originate` command on the DR (R4):

```
R4#show ip ospf database network self-originate

            OSPF Router with ID (4.4.4.4) (Process ID 4)

                Net Link States (Area 0)

  Routing Bit Set on this LSA
  LS age: 429
  Options: (No TOS-capability, DC)
  LS Type: Network Links
  Link State ID: 192.168.1.4 (address of Designated Router)
  Advertising Router: 4.4.4.4
  LS Seq Number: 80000006
  Checksum: 0x7E08
  Length: 40
  Network Mask: /24
        Attached Router: 4.4.4.4
        Attached Router: 1.1.1.1
        Attached Router: 2.2.2.2
        Attached Router: 3.3.3.3
```

Referencing the output above, the DR (R4) originates the Type 2 (Network) LSA representing the 192.168.1.0/24 subnet. Because multiple routers exist on this subnet, this 192.168.1.0/24 subnet is referred to as a transit link in OSPF terminology. The Advertising Router field shows the router that originated this LSA. The Network Mask field shows the subnet mask of the transit network, which is 24-bit or 255.255.255.0.

The Attached Router field lists the router IDs of all routers that are on the network segment. This allows all of the routers on the segment to know what other routers also reside on the segment. The output of the `show ip ospf database network [link state ID]` command on R1, R2, and R3 reflects the same information, as illustrated in the following outputs:

```
R2#show ip ospf database network
```

https://t.me/learningnets

```
            OSPF Router with ID (2.2.2.2) (Process ID 2)
                Net Link States (Area 0)
  Routing Bit Set on this LSA
  LS age: 923
  Options: (No TOS-capability, DC)
  LS Type: Network Links
  Link State ID: 192.168.1.4 (address of Designated Router)
  Advertising Router: 4.4.4.4
  LS Seq Number: 80000006
  Checksum: 0x7E08
  Length: 40
  Network Mask: /24
        Attached Router: 4.4.4.4
        Attached Router: 1.1.1.1
        Attached Router: 2.2.2.2
        Attached Router: 3.3.3.3

R1#show ip ospf database network
            OSPF Router with ID (1.1.1.1) (Process ID 1)
                Net Link States (Area 0)
  Routing Bit Set on this LSA
  LS age: 951
  Options: (No TOS-capability, DC)
  LS Type: Network Links
  Link State ID: 192.168.1.4 (address of Designated Router)
  Advertising Router: 4.4.4.4
  LS Seq Number: 80000006
  Checksum: 0x7E08
  Length: 40
  Network Mask: /24
        Attached Router: 4.4.4.4
        Attached Router: 1.1.1.1
        Attached Router: 2.2.2.2
        Attached Router: 3.3.3.3
            OSPF Router with ID (4.4.4.4) (Process ID 4)

R3#show ip ospf database network
            OSPF Router with ID (3.3.3.3) (Process ID 3)
                Net Link States (Area 0)
  Routing Bit Set on this LSA
```

https://t.me/learningnets

```
LS age: 988
Options: (No TOS-capability, DC)
LS Type: Network Links
Link State ID: 192.168.1.4 (address of Designated Router)
Advertising Router: 4.4.4.4
LS Seq Number: 80000006
Checksum: 0x7E08
Length: 40
Network Mask: /24
      Attached Router: 4.4.4.4
      Attached Router: 1.1.1.1
      Attached Router: 2.2.2.2
      Attached Router: 3.3.3.3
```

The functionality of the Network LSA and how it is correlated to another LSA, specifically the Router LSA (Type 1), will be described in detail later in this module. For this section, primary emphasis should be placed on understanding that the DR generates and advertises the Network LSA on the Multi-Access segment to advertise other routers that reside on the same segment. This is because routers on the segment establish an adjacency only with the DR and BDR routers and not with each other. Without an adjacency with each other, the routers will never know about other non-DR/BDR routers on the Multi-Access segment.

Finally, regarding the third point made on DR/BDR routers, the DR/BDR routers ensure that all routers on the segment have complete databases. Non-DR/BDR routers send updates to the Multicast group address 224.0.0.6 (AllDRRouters). The DR then advertises these updates to other non-DR/BDR routers by sending the update to the Multicast group address 224.0.0.5 (AllSPFRouters). Figure 39.3 below illustrates an update from R1 (a DROther) to the DR group address referencing the routers illustrated in Figure 39.2:

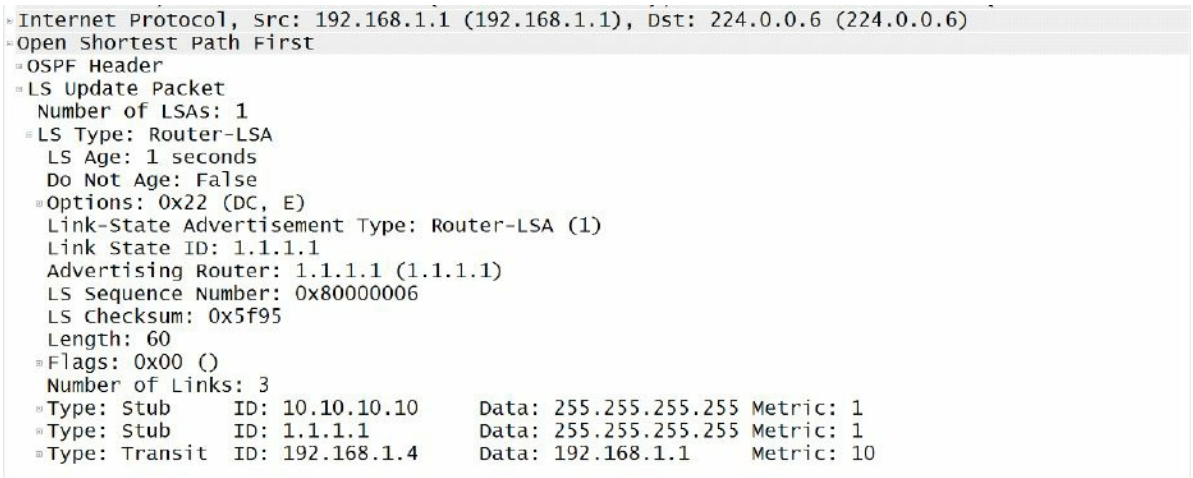


Figure 39.3 – DROther Update to DR/BDR Group Address

R4 (DR) receives this update and in turn sends the same to Multicast group address 224.0.0.5. This group address is used by all OSPF routers, ensuring that all other routers on the segment receive this update. This update from the DR (R4) is illustrated in Figure 39.4 below:

https://t.me/learningnets

```
Internet Protocol, Src: 192.168.1.4 (192.168.1.4), Dst: 224.0.0.5 (224.0.0.5)
Open Shortest Path First
 OSPF Header
 LS Update Packet
   Number of LSAs: 1
  LS Type: Router-LSA
    LS Age: 2 seconds
    Do Not Age: False
   Options: 0x22 (DC, E)
    Link-State Advertisement Type: Router-LSA (1)
    Link State ID: 1.1.1.1
    Advertising Router: 1.1.1.1 (1.1.1.1)
    LS Sequence Number: 0x80000006
    LS Checksum: 0x5f95
    Length: 60
   Flags: 0x00 ()
    Number of Links: 3
   Type: Stub     ID: 10.10.10.10     Data: 255.255.255.255 Metric: 1
   Type: Stub     ID: 1.1.1.1         Data: 255.255.255.255 Metric: 1
   Type: Transit  ID: 192.168.1.4     Data: 192.168.1.1     Metric: 10
```

Figure 39.4 – DR Update to OSPF Group Address

NOTE: You can see that this is the Update from R1 because the Advertising Router field in both Figures 39.3 and 39.4 contains the router ID (RID) of R1, which is 1.1.1.1.

NOTE: The other LSAs used by OSPF will be described in detail later in this module.

Additional Router Types

In addition to the Designated Router and the Backup Designated Router on Multi-Access segments, OSPF routers are also described based on their location and function within the OSPF network. The additional router types that are commonly found within the OSPF network include the following:

- Area Border Routers
- Autonomous System Boundary Routers
- Internal routers
- Backbone routers

Figure 39.5 below illustrates a basic OSPF network comprised of two areas, the OSPF backbone area (Area 0) and an additional normal OSPF area (Area 2). R2 has an external BGP neighbour relationship with R1. This diagram will be used to describe the different OSPF router types within this network.

https://t.me/learningnets

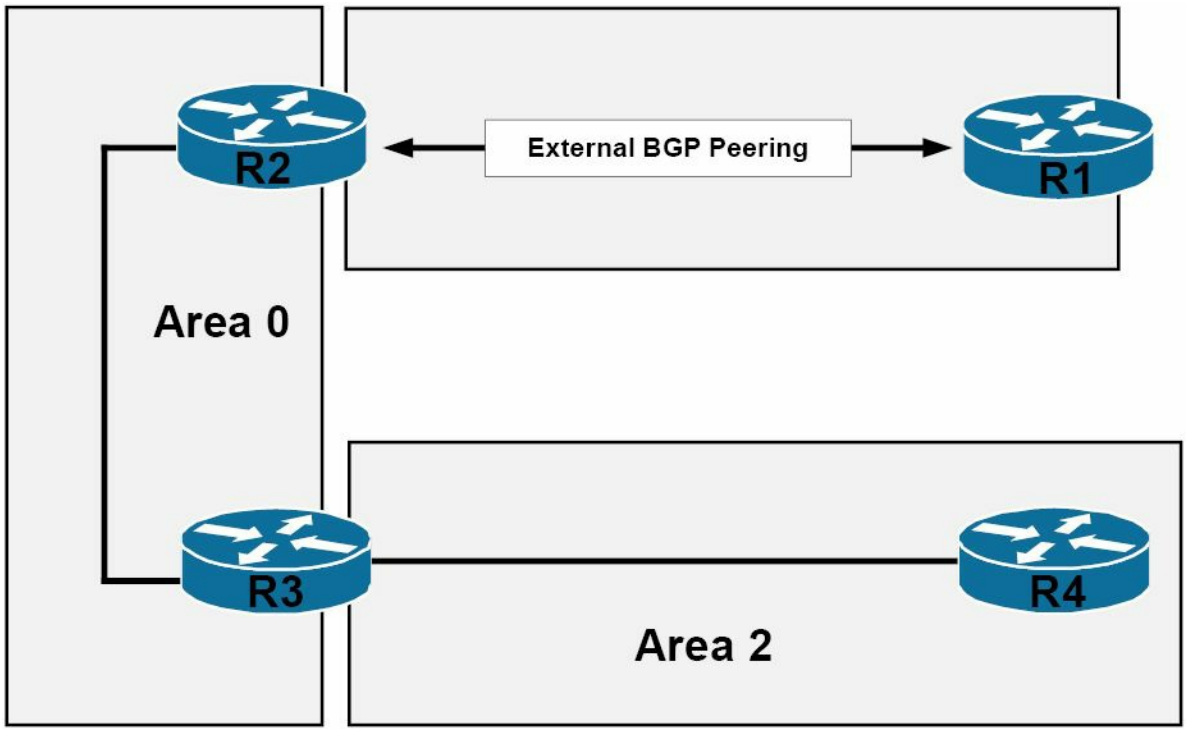


Figure 39.5 Additional OSPF Router Types

An Area Border Router (ABR) is an OSPF router that connects one or more OSPF areas to the OSPF backbone. This means that it must have at least one interface in Area 0 and another interface, or interfaces, within a different OSPF area. ABRs are members of all areas to which they belong, and they keep a separate Link State Database for every area to which they belong. Referencing Figure 39.5, R3 would be considered an ABR, as it connects Area 2 to the OSPF backbone, or Area 0.

An Autonomous System Boundary Router (ASBR), in the traditional sense, resides at the edge of the routing domain and defines the boundary between the internal and the external networks. Referencing Figure 39.5, R2 would be considered an ASBR. In addition to injecting routing information from other protocols (e.g., BGP), a router can also be classified as an ASBR if it injects static routes or connected subnets into the OSPF domain.

Internal routers maintain all operational interfaces within a single OSPF area. Based on the network topology illustrated in Figure 39.5, R4 would be considered an internal router because its only interface resides within a single OSPF area.

Backbone routers are routers that have an interface in the OSPF backbone. Backbone routers can include routers that have interfaces only in the OSPF backbone area, or routers that have an interface in the OSPF backbone area as well as interfaces in other areas (ABRs). Based on the topology illustrated in Figure 39.5, both R2 and R3 would be considered backbone routers.

NOTE: OSPF routers can have multiple roles. For example, R2 is both an ASBR and a backbone router, while R3 is both a backbone router and an ABR. Throughout this module, we will take a detailed look at these types of routers and their roles and functions within the OSPF domain.

OSPF Packet Types

https://t.me/learningnets

The different types of packets sent by OSPF routers are contained in the common 24-byte OSPF

header. While delving into the specifics of the OSPF header is beyond the scope of the CCNA exam requirements, it is still important to have a basic understanding of the fields contained within this header and what they are used for. Figure 39.6 below illustrates the common 24-octet OSPF header:

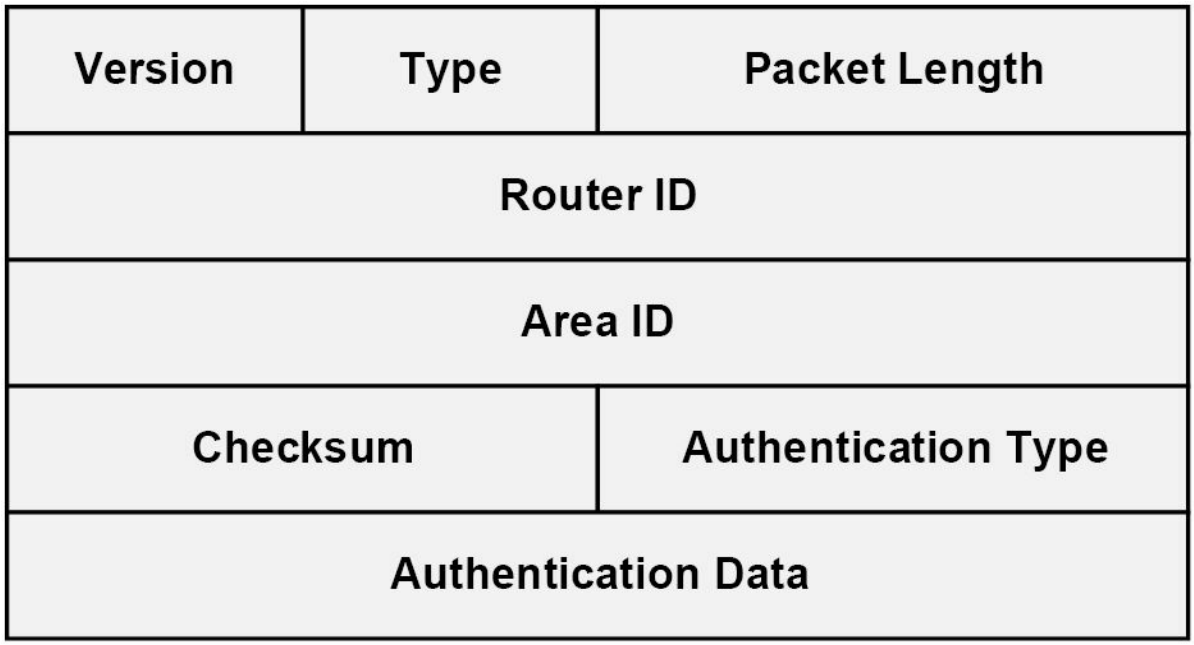


Figure 39.6 – The OSPF Packet Header

The 8-bit Version field specifies the OSPF version. The default value for this field is 2. However, when OSPFv3 is enabled, this field is also set to 3. OSPFv3 was described in detail in the Day 13 module.

The 8-bit Type field is used to specify the OSPF packet type. The five main OSPF packet types, which are described in detail later in this module, are as follows:

- Type 1 = Hello packet
- Type 2 = Database Description packet
- Type 3 = Link State Request packet
- Type 4 = Link State Update packet
- Type 5 = Link State Acknowledgement packet

The 16-bit Packet Length field is used to specify the length of the protocol packet. This length includes the standard OSPF header.

The 32-bit Router ID field is used to specify the IP address of the router from which the packet originated. On Cisco IOS devices, this field will contain the highest IP address of all physical interfaces configured on the device running OSPF. If Loopback interfaces are configured on the device, the field will contain the highest IP address of all configured Loopback interfaces. Alternatively, this field can also contain a manually configured router ID if one has been explicitly configured or specified by the administrator.

NOTE: When the router ID has been selected, it will never change unless the router is reloaded, the interface that the IP address is derived from is removed or removed, or the OSPF process is reset using the `clear ip ospf process`

https://lmelearning.ets

privileged EXEC command on the router.

The 32-bit Area ID field is used to identify the OSPF area of the packet. A packet can belong only to a single OSPF area. If the packet is received via a virtual link, then the Area ID will be the OSPF backbone, or Area 0. Virtual links are described in detail later in this module.

The Checksum field is 16-bits long and indicates the standard IP checksum of the entire contents of the packet, starting with the OSPF packet header but excluding the 64-bit Authentication Data field. If the packet's length is not an integral number of 16-bit words, the packet is padded with a byte of zero before being checksummed.

The 16-bit Authentication (Auth) Type field identifies the type of authentication used. This field is valid only for OSPFv2 and may contain one of the following three codes:

- Code 0 – This means that there is null (no) authentication; this is the default
- Code 1 – This means that the authentication type is plain text
- Code 2 – This means that the authentication type is Message Digest 5 (MD5)

Finally, the 64-bit Authentication Data field is for the actual authentication information or data, if authentication has been enabled. It is important to remember that this field is valid only for OSPFv2. If plain text authentication is being used, this field contains the authentication key. However, if MD5 authentication is being used, this field is redefined into several other fields, which are beyond the scope of the CCNA exam requirements. Figure 39.7 below shows the different fields as they appear in a wire capture of an OSPF packet:

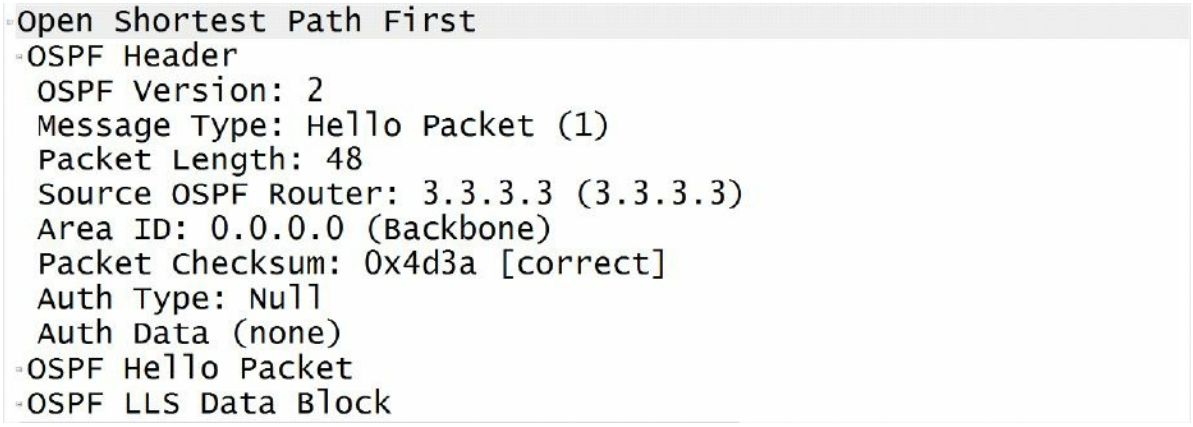


Figure 39.7 – OSPF Packet Header Wire Capture

Within the OSPF packet header, the 8-bit Type field is used to specify the OSPF packet type. Again, the five OSPF packet types are as follows:

- Type 1 = Hello packet
- Type 2 = Database Description packet
- Type 3 = Link State Request packet
- Type 4 = Link State Update packet
- Type 5 = Link State Acknowledgement packet

https://t.me/learningnets

OSPF Hello Packets

Hello packets are used to discover other directly connected OSPF routers and to establish OSPF adjacencies between OSPF routers. OSPF uses Multicast to send Hello packets for Broadcast and Point-to-Point network types. These packets are addressed to the AllSPFRouters Multicast group address 224.0.0.5. For Non-Broadcast links (e.g., Frame Relay), OSPF uses Unicast to send Hello packets directly to statically configured neighbours.

NOTE: By default, all OSPF packets (i.e., Multicast and Unicast) are sent with an IP TTL of 1. This limits these packets to the local link. In other words, you cannot establish an OSPF adjacency with another router that is more than one hop away. This is also applicable to EIGRP.

OSPF Hello packets are also used on Broadcast links to elect a DR and a BDR. The DR listens specifically to the Multicast address 224.0.0.6 (AllDRRouters). The DR and the BDR were described in detail previously in this module. Figure 39.8 below illustrates the fields contained within the OSPF Hello packet:

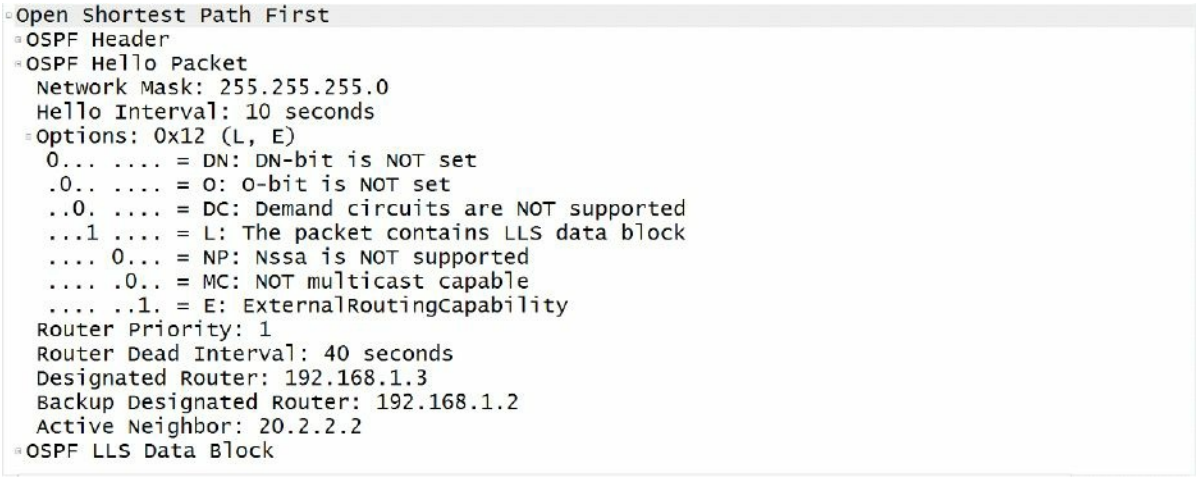


Figure 39.8 – OSPF Hello Packet

The 4-byte Network Mask field contains the subnet mask of the advertising OSPF interface. The network mask is checked only on Broadcast media. Unnumbered Point-to-Point interfaces and virtual links, both of which will be described later in this module, set this value to 0.0.0.0.

The 2-byte Hello field displays the value of the Hello interval, which is the number of seconds between two Hello packets, requested by the advertising router. Possible values range from 1 to 255. By default, the Hello interval is 10 seconds on Broadcast and Point-to-Point media and 30 seconds on all other media.

The 1-byte Options field is used by the local router to advertise optional capabilities. Each bit in the Options field represents a different function. Going into them is outside the scope of the CCNA exam requirements.

The 1-byte Router Priority field contains the priority of the local router. By default, this field has a value of 1. The value is used in the election of the DR and the BDR. Possible values range from 0 to 255. The higher the priority, the higher the chances the local router will become the DR. A priority value of 0 means that the local router will not participate in the DR or the BDR election.

https://t.me/learningnets

The 4-byte Router Dead Interval field shows the value of the dead interval. The dead interval is the time (seconds) before a neighbour router is declared dead. This value is requested by the advertising router. The default value for the dead interval is four times the value of the Hello interval, which would be a default of 40 seconds on Broadcast and Point-to-Point interfaces and 120 seconds on all other types of media.

The 4-byte Designated Router field lists the IP address of the DR. A value of 0.0.0.0 is used when no DR has been elected, for example, on a Point-to-Point link or when a router has been explicitly configured not to participate in this election.

The 4-byte Backup Designated Router field identifies the BDR and lists the interface address of the current BDR. A value of 0.0.0.0 is used when no BDR has been elected.

Finally, the (Active) Neighbor field is a variable length field that displays the router ID of all OSPF routers for which a Hello packet has been received on the network segment.

Database Description Packets

Database Description packets are used during the database exchange when each OSPF router advertises its local database information. These packets are commonly referred to as DBD packets or as DD packets. The first DBD packet is used for the Master and Slave election for database exchange. The DBD packet also contains the initial sequence number selected by the Master. The router with the highest router ID becomes the Master and initiates database synchronisation. This is the only router that can increment the sequence number. The Master router begins the database exchange and polls the Slave for information. The Master and Slave election is held on a per-neighbour basis.

It is important to understand that the Master and Slave election process is not the same as the DR and BDR election process. This is commonly incorrectly assumed. The Master and Slave election process is based solely on the router with the highest IP address; however, the DR/BDR election process may be determined using either the IP address or the priority value.

Assume, for example, two routers named R1 and R2 are beginning the adjacency establishment process. R1 has a RID of 1.1.1.1, while R2 has a RID of 2.2.2.2. The network administrator has configured R1 with an OSPF priority value of 255 to ensure that this router will be elected the DR. During the Master and Slave determination process, R2 will be elected master by virtue of the higher RID. However, the priority value configured on R1 results in R1 being elected the DR. In essence, the DR (R1) can be the Slave during the Master and Slave election process.

After the Master and Slave have been elected, DBD packets are used to summarise the local database by sending LSA headers to the remote router. The remote router analyses these headers to determine whether it lacks any information within its own copy of the LSDB. The OSPF Database Description packet is illustrated in Figure 39.9 below:

https://t.me/learningnets

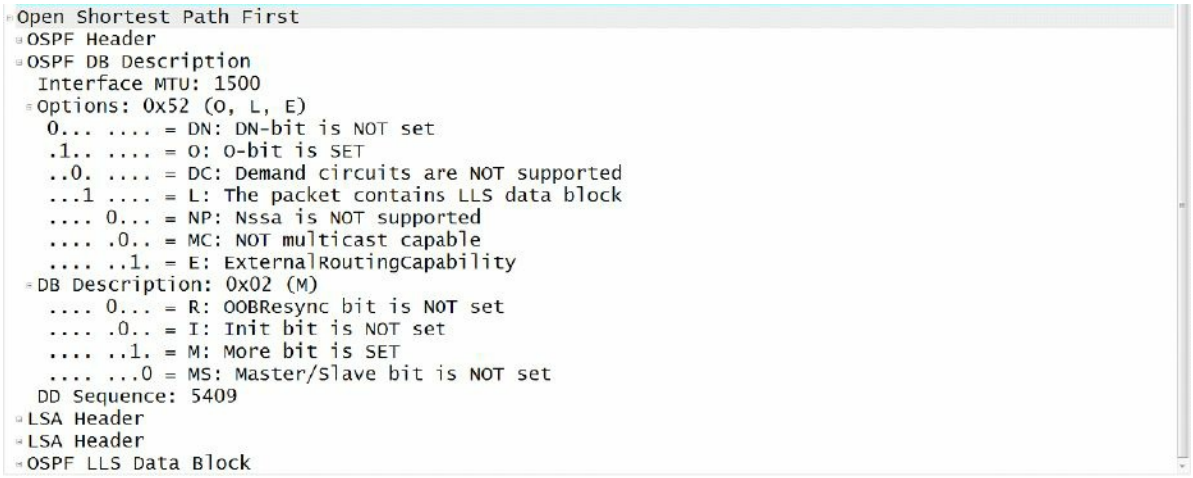


Figure 39.9 – OSPF Database Description Packet

Within the DBD packet, the 2-byte Interface MTU field contains the MTU value, in octets, of the outgoing interface. In other words, this field contains the largest data size that can be sent through the associated interface (in bytes). When the interface is used on a virtual link, the field is set to a value of 0x0000. In order for an OSPF neighbour adjacency to be established successfully, the MTU must be the same on all routers. If you change this value on one router, you must configure the same value on all other routers on the same subnet (or use the `ip ospf mtu-ignore` command).

NOTE: The interface MTU values for EIGRP do not have to be the same in order for an EIGRP neighbour relationship to be established successfully.

The 1-byte Options field contains the same options contained within the OSPF Hello packet. For brevity, these options will not be described again.

The Database Description or Flags field is a 1-byte field that provides an OSPF router with the capability to exchange multiple DBD packets with a neighbour during an adjacency formation.

The 4-byte DBD Sequence Number field is used to guarantee that all DBD packets are received and processed during the synchronisation process through the use of a sequence number. The Master router initialises this field to a unique value in the first DBD packet, with each subsequent packet being incremented by 1. The sequence number is incremented only by the Master.

Finally, the variable length LSA Header field carries the LSA headers describing the local router's database information. Each header is 20 octets in length and uniquely identifies each LSA in the database. Each DBD packet may contain multiple LSA headers.

Link State Request Packets

Link State Request (LSR) packets are sent by OSPF routers to request missing or out-of-date database information. These packets contain identifiers that uniquely describe the requested Link State Advertisement. An individual LSR packet may contain a single set of identifiers or multiple sets of identifiers to request multiple LSAs. LSR packets are also used after database exchange to request LSAs that were seen during the database exchange that the local router does not have. Figure 39.10 below illustrates the format of the OSPF LSR packet:

https://t.me/learningnets

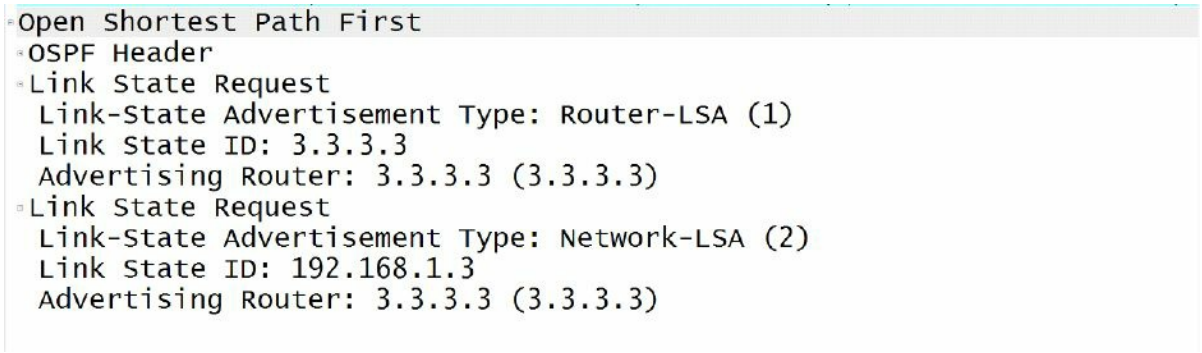


Fig. 39.10 – OSPF Link State Request Packet

The 4-byte Link State Advertisement Type field contains the type of LSA being requested. It may contain one of the following fields:

- Type 1 = Router Link State Advertisement
- Type 2 = Network Link State Advertisement
- Type 3 = Network Summary Link State Advertisement
- Type 4 = ASBR Summary Link State Advertisement
- Type 5 = AS External Link State Advertisement
- Type 6 = Multicast Link State Advertisement
- Type 7 = NSSA External Link State Advertisement
- Type 8 = External Attributes Link State Advertisement
- Type 9 = Opaque Link State Advertisement – Link Local
- Type 10 = Opaque Link State Advertisement – Area
- Type 11 = Opaque Link State Advertisement – Autonomous System

NOTE: Some of the LSAs listed above are described in detail in the following sections.

The 4-byte Link State ID field encodes information specific to the LSA. The information that is contained in this field depends upon the type of LSA. Finally, the 4-byte Advertising Router field contains the RID of the router that first originated the LSA.

Link State Update Packets

Link State Update (LSU) packets are used by the router to advertise LSAs. LSU packets may be Unicast to an OSPF neighbour in response to a received LSR from that neighbour. Most commonly, however, they are reliably flooded throughout the network to the AllSPFRouters Multicast group address 224.0.0.5 until each router has a copy. The flooded updates are then acknowledged in the LSA Acknowledgement packet. If the LSA is not acknowledged, it will be retransmitted every five seconds, by default. Figure 39.11 below shows an LSU sent to a neighbour in response to an LSR:

https://t.me/learningnets

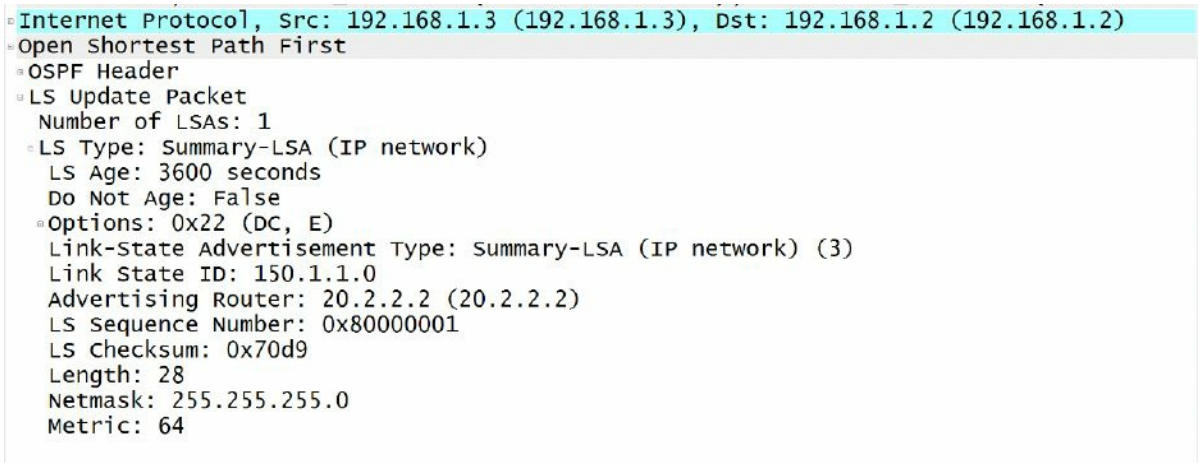


Figure 39.11 – Unicast LSU Packet

Figure 39.12 below illustrates an LSU that is reliably flooded to the Multicast group address 224.0.0.5:

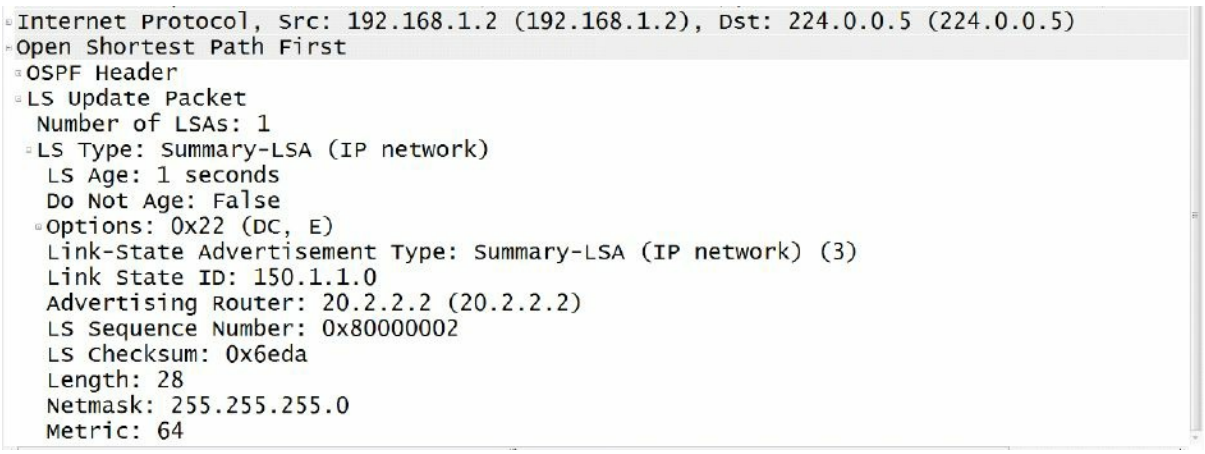


Figure 39.12 – Multicast LSU Packet

The LSU is comprised of two parts. The first part is the 4-byte Number of LSAs field. This field displays the number of LSAs carried within the LSU packet. The second part is one or more Link State Advertisements. This variable-length field contains the complete LSA. Each type of LSA has a common header format along with specific data fields to describe its information. An LSU packet may contain a single LSA or multiple LSAs.

Link State Acknowledgement Packets

The Link State Acknowledgement (LSAck) packet is used to acknowledge each LSA and is sent in response to LSU packets. By explicitly acknowledging packets with LSAcks, the flooding mechanism used by OSPF is considered reliable.

The LSAck contains the common OSPF header followed by a list of LSA headers. This variable-length field allows the local router to acknowledge multiple LSAs using a single packet. LSAcks are sent using Multicast. On Multi-Access networks, if the router sending the LSAck is a DR or a BDR, then LSAcks are sent to the Multicast group address 224.0.0.5 (AllSPFRouters). However, if the router sending the LSAcks is not a DR or a BDR device, then LSAck packets are sent to the Multicast group address 224.0.0.6 (AllDRRouters). Figure 39.13 below illustrates the format of the LSAck:

https://t.me/learningnets

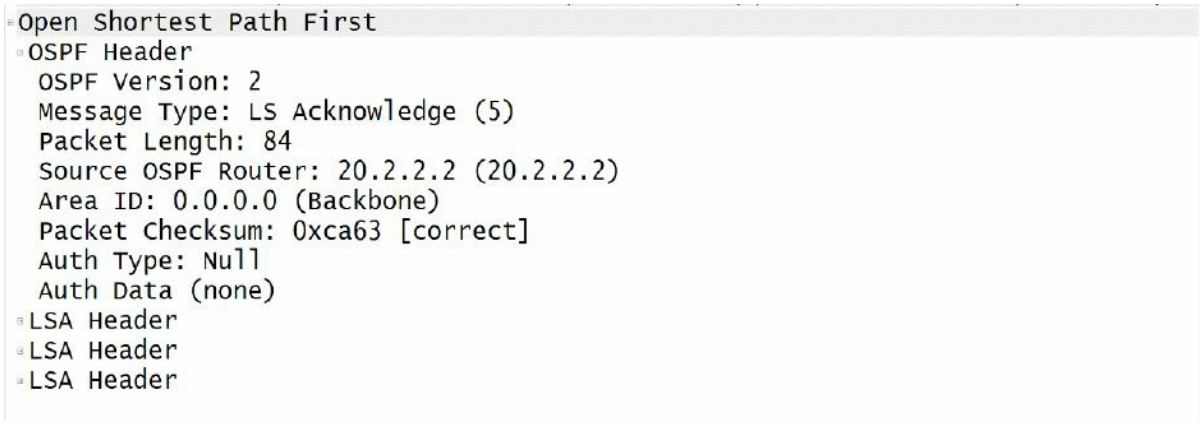


Figure 39.13 – Link State Acknowledgement Packet

In conclusion, it is important to remember the different OSPF packet types and what information they contain. This not only will benefit you in the exam but also will aid you in understanding the overall operation of OSPF as a protocol.

In Cisco IOS software, you can use the `show ip ospf traffic` command to view OSPF packet statistics. This command shows the total count for the sent and received OSPF packets, and then segments this further to the individual OSPF process and, finally, to the interfaces enabled for OSPF routing under that process. This command can also be used to troubleshoot OSPF adjacency establishment and is not as processor intensive as debugging. The information printed by this command is illustrated in the following output:

```
R4#show ip ospf traffic
OSPF statistics:
  Rcvd: 702 total, 0 checksum errors
        682 hello, 3 database desc, 0 link state req
        12 link state updates, 5 link state acks
  Sent: 1378 total
        1364 hello, 2 database desc, 1 link state req
        5 link state updates, 6 link state acks
            OSPF Router with ID (4.4.4.4) (Process ID 4)
OSPF queue statistics for process ID 4:
                    InputQ     UpdateQ    OutputQ
  Limit             0          200        0
  Drops             0          0          0
  Max delay [msec]  4          0          0
  Max size          2          2          2
    Invalid         0          0          0
    Hello           0          0          1
    DB des          2          2          1
    LS req          0          0          0
    LS upd          0          0          0
    LS ack          0          0          0
  Current size      0          0          0
```

https://t.me/learningnets

```
    Invalid       0          0          0
    Hello         0          0          0
    DB des        0          0          0
    LS req        0          0          0
    LS upd        0          0          0
    LS ack        0          0          0
Interface statistics:
    Interface Serial0/0
OSPF packets received/sent
    Invalid  Hellos   DB-des   LS-req   LS-upd   LS-ack   Total
Rx: 0        683      3        0        12       5        703
Tx: 0        684      2        1        5        6        698
OSPF header errors
  Length 0, Auth Type 0, Checksum 0, Version 0,
  Bad Source 0, No Virtual Link 0, Area Mismatch 0,
  No Sham Link 0, Self Originated 0, Duplicate ID 0,
  Hello 0, MTU Mismatch 0, Nbr Ignored 0,
  LLS 0, Unknown Neighbor 0, Authentication 0,
  TTL Check Fail 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
    Interface FastEthernet0/0
OSPF packets received/sent
    Invalid  Hellos   DB-des   LS-req   LS-upd   LS-ack   Total
Rx: 0        0        0        0        0        0        0
Tx: 0        682      0        0        0        0        682
OSPF header errors
  Length 0, Auth Type 0, Checksum 0, Version 0,
  Bad Source 0, No Virtual Link 0, Area Mismatch 0,
  No Sham Link 0, Self Originated 0, Duplicate ID 0,
  Hello 0, MTU Mismatch 0, Nbr Ignored 0,
  LLS 0, Unknown Neighbor 0, Authentication 0,
  TTL Check Fail 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
Summary traffic statistics for process ID 4:
  Rcvd: 703 total, 0 errors
        683 hello, 3 database desc, 0 link state req
        12 link state upds, 5 link state acks, 0 invalid
  Sent: 1380 total
```

https://t.me/learningnets

```
1366 hello, 2 database desc, 1 link state req
5 link state upds, 6 link state acks, 0 invalid
```

Establishing Adjacencies

Routers running OSPF transition through several states before establishing an adjacency. The routers exchange different types of packets during these states. This exchange of messages allows all routers that establish an adjacency to have a consistent view of the network. Additional changes to the current network are simply sent out as incremental updates. The different states are the Down, Attempt, Init, 2-Way, Exstart, Exchange, Loading, and Full states, as described below:

- The Down state is the starting state for all OSPF routers. However, the local router may also show a neighbour in this state when no Hello packets have been received within the specified router dead interval for that interface.
- The Attempt state is valid only for OSPF neighbours on NBMA networks. In this state, a Hello has been sent but no information has been received from the statically configured neighbour within the dead interval; however, some effort is being made to establish an adjacency with this neighbour.
- The Init state is reached when an OSPF router receives a Hello packet from a neighbour but the local RID is not listed in the received Neighbor field. If OSPF Hello parameters, such as timer values, do not match, then OSPF routers will never progress beyond this state.
- The 2-Way state indicates bidirectional communication (each router has seen the other's Hello packet) with the OSPF neighbour(s). In this state, the local router has received a Hello packet with its own RID in the Neighbor field and Hello packet parameters are identical on the two routers. At this state, a router decides whether to become adjacent with this neighbour. On Multi-Access networks, the DR and the BDR are elected during this phase.
- The Exstart state is used for the initialisation of the database synchronisation process. It is at this stage that the local router and its neighbour establish which router is in charge of the database synchronisation process. The Master and Slave are elected in this state, and the first sequence number for DBD exchange is decided by the Master in this stage.
- The Exchange state is where routers describe the contents of their databases using DBD packets. Each DBD sequence is explicitly acknowledged, and only one outstanding DBD is allowed at a time. During this phase, LSR packets are also sent to request a new instance of the LSA. The M (More) bit is used to request missing information during this stage. When both routers have exchanged their complete databases, they will both set the M bit to 0.
- In the Loading state, OSPF routers build an LSR and Link State Retransmission list. LSR packets are sent to request the more recent instance of an LSA that has not been received

https://t.me/learningnets

during the Exchange process. Updates that are sent during this phase are placed on the Link State Retransmission list until the local router receives an acknowledgement. If the local router also receives an LSR during this phase, it will respond with a Link State Update that contains the requested information.

- The Full state indicates that the OSPF neighbours have exchanged their entire databases and both agree (i.e., have the same view of the network). Both neighbouring routers in this state add the adjacency to their local database and advertise the relationship in a Link State Update packet. At this point, the routing tables are calculated, or recalculated if the adjacency was reset. Full is the normal state for an OSPF router. If a router is stuck in another state, it's an indication that there are problems in forming adjacencies. The only exception to this is the 2-Way state, which is normal in Broadcast and Non-Broadcast Multi-Access networks where routers achieve the Full state with their DR and BDR only. Other neighbours always see each other as 2-Way.

In order for an OSPF adjacency to be established successfully, certain parameters on both routers must match. These parameters include the following:

- The interface MTU values (can be configured to be ignored)
- The Hello and Dead timers
- The Area ID
- The Authentication type and password
- The Stub Area flag
- Compatible network types

These parameters will be described as we progress through this module. If these parameters do not match, the OSPF adjacency will never fully establish.

NOTE: In addition to mismatched parameters, it is also important to remember that on a Multi-Access network, if both routers are configured with a priority value of 0, then the adjacency will not be established. The DR must be present on such network types.

OSPF LSAs and the Link State Database (LSDB)

As stated in the previous section, OSPF uses several types of Link State Advertisements. Each LSA begins with a standard 20-byte LSA header. This header contains the following fields:

- Link State Age
- Options
- Link State Type
- Link State ID
- Advertising Router

https://t.me/learningnets

- Link State Sequence Number
- Link State Checksum
- Length

The 2-byte Link State Age field states the time (in seconds) since the LSA was originated. The maximum age of the LSA is 3600 seconds, which means that if the age reaches 3600 seconds, the LSA is removed from the database. To avoid this, the LSA is refreshed every 1800 seconds.

The 1-byte Options field contains the same options as those in the OSPF Hello packet.

The 1-byte Link State Type field represents the types of LSAs. These different LSA packet types are described in detail in the following sections.

The 4-byte Link State ID field identifies the portion of the network that is being described by the LSA. The contents of this field depend upon the advertisement's LS type.

The 4-byte Advertising Router field represents the router ID of the router originating the LSA.

The 1-byte Link State Sequence Number field detects old or duplicate Link State Advertisements. Successive instances of an LSA are given successive Link State Sequence Numbers. The first sequence number 0x80000000 is reserved; therefore, the actual first sequence number is always 0x80000001. This value is incremented as packets are sent. The maximum sequence number is 0x7FFFFFFF.

The 2-byte Link State Checksum field performs the Fletcher checksum of the complete contents of the LSA, including the LSA header. The Link State Age field is not included in the checksum. The checksum is performed because Link State Advertisements can be corrupted while being stored in memory due to router software or hardware issues or during flooding due to Physical Layer errors, for example.

NOTE: The checksum is performed at the time the LSA is generated or is received. In addition, the checksum is performed at every CheckAge interval, which is 10 minutes. If this field has a value of 0, then it means that the checksum has not been performed.

The 2-byte Length field is the final field and includes the length (in bytes) of the LSA. This includes the 20-byte LSA header. Figure 39.13 below illustrates the LSA header:

```
Open Shortest Path First
OSPF Header
LSA Header
  LS Age: 3600 seconds
  Do Not Age: False
  Options: 0x22 (DC, E)
  Link-State Advertisement Type: Router-LSA (1)
  Link State ID: 20.2.2.2
  Advertising Router: 20.2.2.2 (20.2.2.2)
  LS Sequence Number: 0x80000005
  LS Checksum: 0xcb54
  Length: 36
LSA Header
LSA Header
```

https://t.me/learningnets

Figure 39.13 – Link State Advertisement Header

While OSPF supports 11 different types of Link State Advertisements, only LSA Types 1, 2, and 3, which are used to calculate internal routes, and LSA Types 4, 5, and 7, which are used to calculate external routes, are within the scope of the CCNA exam requirements. Because there is really no need to go into great detail on the other LSAs for the CCNA exam, these LSAs will not be described further in this guide. However, a brief outline and a printable guide are provided at www.in60days.com.

In Cisco IOS software, the `show ip ospf database` command is used to view the contents of the Link State Database. This command, when used without any keywords, prints out a summary of LSAs in all areas to which the router is connected. The command supports several keywords that provide greater granularity in allowing network administrators to restrict output only to specific types of LSAs, LSAs advertised by the local router, or even LSAs advertised by other routers within the OSPF domain.

While illustrating the output of the usage of each keyword is unrealistic, the following section describes the different LSAs and the common keywords used in conjunction with the `show ip ospf database` command to view detailed information on these LSAs. The keywords supported by this command are illustrated in the following output:

```
R3#show ip ospf database ?
  adv-router         Advertising Router link states
  asbr-summary       ASBR Summary link states
  database-summary   Summary of database
  external           External link states
  network            Network link states
  nssa-external      NSSA External link states
  opaque-area        Opaque Area link states
  opaque-as          Opaque AS link states
  opaque-link        Opaque Link-Local link states
  router             Router link states
  self-originate     Self-originated link states
  summary            Network Summary link states
  |                  Output modifiers
  <cr>
```

Router Link State Advertisements (Type 1)

Type 1 LSAs are generated by each router for each area to which it belongs. The Router LSA lists the originating router's router ID (RID). Each individual router will generate a Type 1 LSA for the area in which it resides. The Router LSAs are the first LSA types printed in the output of the `show ip ospf database` command.

Network Link State Advertisements (Type 2)

OSPF uses the Network Link State Advertisement (Type 2 LSA) to advertise the routers on the

https://t.me/learningnets

Multi-Access segment. This LSA is generated by the DR and is flooded only within the area. Because the other non-DR/BDRs do not establish adjacencies with each other, the Network LSA allows those routers to know about the other routers on the Multi-Access segment.

Network Summary Link State Advertisements (Type 3)

The Network (Type 3) LSA is a summary of destinations outside of the local area but within the OSPF domain. In other words, this LSA advertises both inter-area and intra-area routing information. The Network Summary LSA does not carry any topological information. Instead, the only information contained in the LSA is an IP prefix. Type 3 LSAs are generated by ABRs and are flooded to all adjacent areas. By default, each Type 3 LSA matches a single Router or Network LSA on a one-for-one basis. In other words, a Type 3 LSA exists for each individual Type 1 and Type 2 LSA. Special attention must be paid to how these LSAs are propagated in relation to the OSPF backbone. This propagation or flooding is performed as follows:

- Network Summary (Type 3) LSAs are advertised from a non-backbone area to the OSPF backbone for intra-area routes (i.e., for Type 1 and Type 2 LSAs).
- Network Summary (Type 3) LSAs are advertised from the OSPF backbone to other non-backbone areas for both intra-area (i.e., Area 0 Type 1 and Type 2 LSAs) and inter-area routes (i.e., for the Type 3 LSAs flooded into the backbone by other ABRs).

The next three Link State Advertisements, Type 4, Type 5, and Type 7, are used in external route calculation. Type 4 and Type 5 LSAs will be described in the following sections. Type 7 LSAs will be described later in this module when we discuss the different types of OSPF areas.

ASBR Summary Link State Advertisements (Type 4)

The Type 4 LSA describes information regarding the Autonomous System Boundary Router (ASBR). This LSA contains the same packet format as the Type 3 LSA and performs the same basic functionality, with some notable differences. Like the Type 3 LSA, the Type 4 LSA is generated by the ABR. For both LSAs, the Advertising Router field contains the RID of the ABR that generated the Summary LSA. However, the Type 4 LSA is created by the ABR for each ASBR reachable by a Router LSA. The ABR then injects the Type 4 LSA into the appropriate area. This LSA provides reachability information on the ASBR itself. The key differences between the Type 3 and Type 4 LSAs that you should be familiar with are listed below in Table 39.2:

Table 39.2 – Type 3 and Type 4 Summary LSAs

Type 3 Summary LSA	Type 4 Summary LSA
Provides information about the network link.	Provides information about the ASBR.
The Network Mask field contains the subnet mask value of the network.	The Network Mask field will always contain a value of 0.0.0.0, or simply just 0.
The Link State ID field contains the actual network number.	The Link State ID field contains the router ID of the ASBR.

AS External Link State Advertisements (Type 5)

The External Link State Advertisement is used to describe destinations that are external to the

https://t.me/learningnets

autonomous system. In other words, Type 5 LSAs provide the network information necessary to reach the external networks. In addition to external routes, the default route for an OSPF routing domain can also be injected as a Type 5 Link State Advertisement.

OSPF Areas

In addition to the backbone (Area 0) and other non-backbone areas described and used in the examples in previous sections of this module, the OSPF specification also defines several “special” types of areas. The configuration of these areas is used primarily to reduce the size of the Link State Database on routers residing within those areas by preventing the injection of different types of LSAs (primarily Type 5 LSAs) into certain areas, which include the following:

- Not-so-stubby Areas
- Totally Not-so-stubby Areas
- Stub Areas
- Totally Stubby Areas

Not-so-stubby Areas (NSSAs)

Not-so-stubby Areas (NSSAs) are a type of OSPF Stub Area that allows the injection of external routing information by an ASBR using an NSSA External LSA (Type 7). As stated in the previous section, Type 4, Type 5, and Type 7 LSAs are used for external route calculation. We will not examine Type 7 LSAs in detail or how they are used in NSSAs.

Totally Not-so-stubby Areas (TNSSAs)

Totally Not-so-stubby Areas (TNSSAs) are an extension of NSSAs. Like NSSAs, Type 5 LSAs are not allowed into a TNSSA; unlike NSSAs, Summary LSAs are also not allowed into a TNSSA. In addition, when a TNSSA is configured, the default route is injected into the area as a Type 7 LSA. TNSSAs have the following characteristics:

- Type 7 LSAs are converted into Type 5 LSAs at the NSSA ABR
- They do not allow Network Summary LSAs
- They do not allow External LSAs
- The default route is injected as a Summary LSA

Stub Areas

Stub areas are somewhat similar to NSSAs, with the major exception being that external routes (Type 5 or Type 7) are not allowed into Stub Areas. It is important to understand that Stub functionality in OSPF and EIGRP is not at all similar. In OSPF, the configuration of an area as a Stub Area reduces the size of the routing table and the OSPF database for the routers within the Stub Area by preventing external LSAs from being advertised into such areas without any further configuration. Stub Areas have the following characteristics:

- The default route is injected into the Stub Area by the ABR as a Type 3 LSA

https://t.me/learningnets

- Type 3 LSAs from other areas are permitted into these areas
- External route LSAs (i.e., Type 4 and Type 5 LSAs) are not allowed

Totally Stubby Areas

Totally Stubby Areas (TSAs) are an extension of Stub Areas. However, unlike Stub Areas, TSAs further reduce the size of the LSDB on routers in the TSA by restricting Type 3 LSAs, in addition to the external LSAs. TSAs are typically configured on routers that have a single ingress and egress point into the network, for example in a traditional hub-and-spoke network. The area routers forward all external traffic to the ABR. The ABR is also the exit point for all backbone and inter-area traffic to the TSA, which has the following characteristics:

- The default route is injected into Stub Areas as a Type 3 Network Summary LSA
- Type 3, Type 4, and Type 5 LSAs from other areas are not permitted into these areas

Route Metrics and Best Route Selection

In the following sections, you will learn about the OSPF metric and how it is calculated.

Calculating the OSPF Metric

The OSPF metric is commonly referred to as the cost. The cost is derived from the bandwidth of a link using the formula 10^8 / bandwidth (in bps). This means that different links are assigned different cost values, depending on their bandwidth. Using this formula, the OSPF cost of a 10Mbps Ethernet interface would be calculated as follows:

- Cost = 10^8 / bandwidth (bps)
- Cost = 100 000 000 / 10 000 000
- Cost = 10

Using the same formula, the OSPF cost of a T1 link would be calculated as follows:

- Cost = 10^8 / bandwidth (bps)
- Cost = 100 000 000 / 1 544 000
- Cost = 64.77

NOTE: When calculating the OSPF metric, point math is not used. Therefore, any such values are always rounded down to the nearest integer. Regarding the previous example, the actual cost for a T1 link would be rounded down to 64.

The OSPF cost of an interface can be viewed using the `show ip ospf interface [name]` command, as was illustrated previously. The default reference bandwidth used in metric calculation can be viewed in the output of the `show ip protocols` command, as is illustrated in the following output:

```
R4#show ip protocols

Routing Protocol is "ospf 4"
```

https://t.me/learningnets

```
  Outgoing update filter list for all interfaces is not set
```

```
  Incoming update filter list for all interfaces is not set
  Router ID 4.4.4.4
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    0.0.0.0 255.255.255.255 Area 2
Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:00:03
  Distance: (default is 110)
```

The default reference bandwidth used in OSPF cost calculation can be adjusted using the `auto-cost reference-bandwidth <1-4294967>` router configuration command and specifying the reference bandwidth value in Mbps. This is particularly important in networks that have links that have a bandwidth value over 100Mbps, for example, GigabitEthernet links. In such networks, the default value assigned to the GigabitEthernet link would be the same as that of a FastEthernet link. In most cases, this is certainly not desirable, especially if OSPF attempts to load balance across both links.

To prevent this skewed calculation of cost value, the `auto-cost reference-bandwidth 1000` router configuration command should be issued on the router. This results in a recalculation of cost values on the router using the new reference bandwidth value. For example, following this configuration, the cost of a T1 link would be recalculated as follows:

- Cost = 10^9 / bandwidth (bps)
- Cost = 1 000 000 000 / 1 544 000
- Cost = 647.66

NOTE: Again, because the OSPF metric does not support point values, this would be rounded down to a metric value of simply 647, as illustrated in the following output:

```
R4#show ip ospf interface Serial0/0
Serial0/0 is up, line protocol is up
  Internet Address 10.0.2.4/24, Area 2
  Process ID 4, Router ID 4.4.4.4, Network Type POINT_TO_POINT, Cost: 647
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 60, Wait 60, Retransmit 5
    oob-resync timeout 60
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
```

https://t.me/learningnets

```
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress Hello for 0 neighbor(s)
```

When the `auto-cost reference-bandwidth 1000` router configuration command is issued, Cisco IOS software prints the following message indicating that this same value should be applied to all routers within the OSPF domain. This is illustrated in the following output:

```
R4(config)#router ospf 4
R4(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
```

While this may seem like an important warning, keep in mind that the use of this command simply affects the local router. It is not mandatory to configure it on all routers; however, for exam purposes, ensure that a consistent configuration is implemented on all routers.

Influencing OSPF Metric Calculation

The calculation of the OSPF metric can be directly influenced by performing the following:

- Adjusting the interface bandwidth using the `bandwidth` command
- Manually specifying a cost using the `ip ospf cost` command

The use of the `bandwidth` command was described in a previous module when we discussed EIGRP metric calculation. As stated earlier, the default OSPF cost is calculated by dividing the link bandwidth by a reference bandwidth of 10^8, or 100 Mbps. Either incrementing or decrementing the link bandwidth directly affects the OSPF cost for the particular link. This is typically a path control mechanism used to ensure that one path is preferred over another.

However, as was described in the previous module, the `bandwidth` command affects more than just the routing protocol. It is for this reason that the second method, manually specifying a cost value, is the recommended method for influencing OSPF metric calculation.

The `ip ospf cost <1-65535>` interface configuration command is used to manually specify the cost of a link. The lower the value, the greater the probability that the link will be preferred over other links to the same destination network but with higher cost values. The following example illustrates how to configure an OSPF cost of 5 for a Serial (T1) link:

```
R1(config)#interface Serial0/0
R1(config-if)#ip ospf cost 5
R1(config-if)#exit
```

This configuration can be validated using the `show ip ospf interface [name]` command, as illustrated in the following output:

```
R1#show ip ospf interface Serial0/0
Serial0/0 is up, line protocol is up
  Internet Address 10.0.0.1/24, Area 0
```

https://t.me/learningnets

```
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 5
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 4
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress Hello for 0 neighbor(s)
```

OSPF Default Routing

Unlike EIGRP, which supports several different ways of generating and advertising the default route, OSPF uses only the `default-information originate [always] [metric <value>] [metric-type <1|2>] [route-map <name>]` router configuration command to advertise dynamically the default route.

The `default-information originate` command used by itself will configure the router to advertise a default route only if a default route is already present in the routing table. However, the `[always]` keyword can be appended to this command to force the router to generate a default route, even when one does not exist in the routing table. This keyword should be used with caution, as it may result in the black-holing of traffic within the OSPF domain or the forwarding of packets for all unknown destinations to the configured router.

The `[metric <value>]` keyword is used to specify the route metric for the generated default route. The `[metric-type <1|2>]` keyword can be used to change the metric type for the default route. Finally, the `[route-map <name>]` keyword configures the router to generate a default route only if the conditions specified in the named route map are met.

The following configuration example illustrates how to configure an OSPF-enabled router to generate and advertise a default route if one already exists in the routing table. The existing default route can be a static route or even a default route from another routing protocol if multiple routing protocols have been configured on the router. The output below illustrates this configuration based on a configured static default route:

```
R4(config)#ip route 0.0.0.0 0.0.0.0 FastEthernet0/0 172.16.4.254
R4(config)#router ospf 4
R4(config-router)#network 172.16.4.0 0.0.0.255 Area 2
R4(config-router)#default-information originate
R4(config-router)#exit
```

By default, the default route is advertised as a Type 5 LSA.

https://t.me/learningnets

Configuring OSPF

Basic OSPF can be enabled on the router with one line of configuration, and then by adding the network statement that specifies on which interfaces you want to run OSPF, not necessarily networks you wish to advertise:

1. `Router ospf 9` ← locally significant number
2. `network 10.0.0.0 0.255.255.255 area 0`

OSPF won't become active until at least one interface is up/up, and remember that at least one area must be Area 0. A Sample OSPF network is illustrated in Figure 39.14 below:

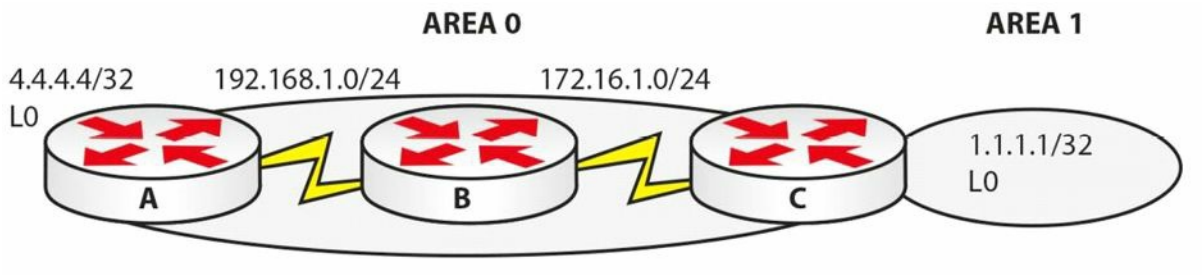


Figure 39.14 – A Sample OSPF Network

Router A configuration:

```
router ospf 20
network 4.4.4.4 0.0.0.0 area 0
network 192.168.1.0 0.0.0.255 area 0
router-id 4.4.4.4
```

Router B configuration:

```
router ospf 22
network 172.16.1.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
router-id 192.168.1.2
```

Router C configuration:

```
router ospf 44
network 1.1.1.1 0.0.0.0 area 1
network 172.16.1.0 0.0.0.255 area 0
router-id 1.1.1.1
RouterC#show ip route
Gateway of last resort is not set
     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/129] via 172.16.1.1, 00:10:39, Serial0/0/0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial0/0/0
```

https://t.me/learningnets

```
O     192.168.1.0/24 [110/128] via 172.16.1.1, 00:10:39, Serial0/0/0
```

Troubleshooting OSPF

Once again, Open Shortest Path First is an open-standard Link State routing protocol that advertises the state of its links. When a Link State router begins operating on a network link, information associated with that logical network is added to its local Link State Database (LSDB). The local router then sends Hello messages on its operational links to determine whether other Link State routers are operating on the interfaces as well. OSPF runs directly over Internet Protocol using IP number 89.

While it is not possible to delve into all potential OSPF problem scenarios, the sections to follow discuss some of the most common problem scenarios when OSPF is implemented as the IGP of choice.

Troubleshooting Neighbour Relationships

Routers running OSPF transition through several states before establishing an adjacency. These different states are the Down, Attempt, Init, 2-Way, Exstart, Exchange, Loading, and Full states. The preferred state for an OSPF adjacency is the Full state. This state indicates that the neighbours have exchanged their entire databases and both have the same view of the network. While the Full state is the preferred adjacency state, it is possible that during the adjacency establishment process, the neighbours get “stuck” in one of the other states. For this reason, it is important to understand what to look for in order to troubleshoot the issue.

The Neighbour Table Is Empty

There are several reasons why the OSPF neighbour table may be empty (i.e., why the output of the `show ip ospf neighbor` command might not yield any results). Common reasons are as follows:

- Basic OSPF misconfigurations
- Layer 1 and Layer 2 issues
- ACL filtering
- Interface misconfigurations

Basic OSPF misconfigurations span a broad number of things. These could include mismatched timers, area IDs, authentication parameters, and stub configuration, for example. A plethora of tools is available in Cisco IOS software to troubleshoot basic OSPF misconfigurations. For example, you could use the `show ip protocols` command to determine information (e.g., about OSPF-enabled networks); the `show ip ospf` command to determine area configuration and the interfaces per area; and the `show ip ospf interface brief` command to determine which interfaces reside in which area, and for which OSPF process IDs those interfaces have been enabled, assuming that OSPF has been enabled for the interface.

Another common misconfiguration is specifying the interface as passive. If this is so, then the interface will not send out Hello packets, and a neighbour relationship will not be established using that interface. You can verify which interfaces have been configured or specified as

https://t.me/learningnets

passive using either the `show ip protocols` or the `show ip ospf interface` commands. The following is a sample output of the latter command on a passive interface:

```
R1#show ip ospf interface Serial0/0
Serial0/0 is up, line protocol is up
  Internet Address 172.16.0.1/30, Area 0
  Process ID 1, Router ID 10.1.0.1, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-Local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Finally, when enabling OSPF over NBMA technologies such as Frame Relay, remember that the neighbours must be defined statically, as OSPF does not use Multicast transmission for neighbour discovery for the default Non-Broadcast network type. This is a common reason for empty neighbour tables when implementing OSPF.

Layer 1 and Layer 2 issues can also result in no formation of OSPF neighbour relationships. Layer 1 and Layer 2 troubleshooting was described in detail in previous modules. Use commands such as the `show interfaces` command to check for interface status (i.e., line protocol), as well as any received errors on the interface. If the OSPF-enabled routers reside in a VLAN that spans multiple switches, verify that there is end-to-end connectivity within the VLAN and that all ports or interfaces are in the correct Spanning Tree states, for example.

ACL filtering is another common cause for adjacencies failing to establish. It is important to be familiar with the topology in order to troubleshoot such issues. For example, if the routers failing to establish an adjacency are connected via different physical switches, it may be that the ACL filtering is being implemented in the form of a VACL that has been configured on the switches for security purposes. A useful troubleshooting tool that may indicate that OSPF packets are being either blocked or discarded is the `show ip ospf traffic` command, which prints information on transmitted and sent OSPF packets as illustrated in the output below:

```
R1#show ip ospf traffic Serial0/0
    Interface Serial0/0
OSPF packets received/sent
    Invalid  Hellos   DB-des   LS-req   LS-upd   LS-ack   Total
Rx: 0        0        0        0        0        0        0
Tx: 0        4        0        0        0        0        6
```

https://t.me/learningnets

```
OSPF header errors
  Length 0, Auth Type 0, Checksum 0, Version 0,
  Bad Source 0, No Virtual Link 0, Area Mismatch 0,
  No Sham Link 0, Self Originated 0, Duplicate ID 0,
  Hello 0, MTU Mismatch 0, Nbr Ignored 0,
  LLS 0, Unknown Neighbor 0, Authentication 0,
  TTL Check Fail 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

In the output above, notice that the local router is sending OSPF Hello packets but is not receiving any. If the configuration on the routers is correct, check ACLs on the routers or intermediate devices to ensure that OSPF packets are not being filtered or discarded.

Another common reason for an empty neighbour table is interface misconfigurations. Similar to EIGRP, OSPF will not establish a neighbour relationship using secondary interface addresses. However, unlike EIGRP, OSPF will also not establish a neighbour relationship if interface subnet masks are not consistent.

EIGRP-enabled routers will establish neighbour relationships even if the interface subnet masks are different. For example, if two routers, one with an interface using the address 10.1.1.1/24 and another with an interface using the address 10.1.1.2/30 are configured in back-to-back EIGRP implementation, they will successfully establish a neighbour relationship. However, it should be noted that such implementations could cause routing loops between the routers. In addition to mismatched subnet masks, EIGRP-enabled routers also ignore Maximum Transmission Unit (MTU) configurations and establish neighbour relationships even if the interface MTU values are different. Use the `show ip interfaces` and `show interfaces` commands to verify IP address and mask configuration.

Troubleshooting Route Advertisement

As is the case with EIGRP, there may be times when you notice that OSPF is not advertising certain routes. For the most part, this is typically due to some misconfigurations versus a protocol failure. Some common reasons for this include the following:

- OSPF is not enabled on the interface(s)
- The interface(s) is/are down
- Interface addresses are in a different area
- OSPF misconfigurations

A common reason why OSPF does not advertise routes is that the network is not advertised via OSPF. In current Cisco IOS versions, networks can be advertised using the `network` router configuration command or the `ip ospf` interface configuration command. Regardless of the method used, the `show ip protocols` command can be used to view which networks OSPF is configured to advertise, as can be seen in the following output:

https://t.me/learningnets

```
R2#show ip protocols
```

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.2.2.0 0.0.0.128 Area 1
    20.2.2.0 0.0.0.255 Area 1
  Routing on Interfaces Configured Explicitly (Area 1):
    Loopback0
Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:00:17
Distance: (default is 110)
```

Additionally, keep in mind that you can also use the `show ip ospf interfaces` command to find out for which interfaces OSPF has been enabled, among other things. In addition to network configuration, if the interface is down, OSPF will not advertise the route. You can use the `show ip ospf interface` command to determine the interface state, as follows:

```
R1#show ip ospf interface brief
Interface    PID   Area     IP Address/Mask   Cost  State  Nbrs F/C
Lo100        1     0        100.1.1.1/24      1     DOWN   0/0
Fa0/0        1     0        10.0.0.1/24       1     BDR    1/1
```

Referencing the output above, you can see that Loopback100 is in a DOWN state. Taking a closer look, you can see that the issue is because the interface has been administratively shut, as illustrated in the following output:

```
R1#show ip ospf interface Loopback100
Loopback100 is administratively down, line protocol is down
  Internet Address 100.1.1.1/24, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type LOOPBACK, Cost: 1
  Enabled by interface config, including secondary ip addresses
  Loopback interface is treated as a stub Host
```

If you debugged IP routing events using the `debug ip routing` command and then issued the `no shutdown` command under the Loopback100 interface, then you would see the following:

```
R1#debug ip routing
IP routing debugging is on
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface Loopback100
```

https://t.me/learningnets

```
R1(config-if)#no shutdown
R1(config-if)#end
R1#
*Mar 18 20:03:34.687: RT: is_up: Loopback100 1 state: 4 sub state: 1 line: 0 has_route:
False
*Mar 18 20:03:34.687: RT: SET_LAST_RDB for 100.1.1.0/24
  NEW rdb: is directly connected
*Mar 18 20:03:34.687: RT: add 100.1.1.0/24 via 0.0.0.0, connected metric [0/0]
*Mar 18 20:03:34.687: RT: NET-RED 100.1.1.0/24
*Mar 18 20:03:34.687: RT: interface Loopback100 added to routing table
...
[Truncated Output]
```

When multiple addresses are configured under an interface, all secondary addresses must be in the same area as the primary address; otherwise, OSPF will not advertise these networks. As an example, consider the network topology illustrated in Figure 39.15 below:

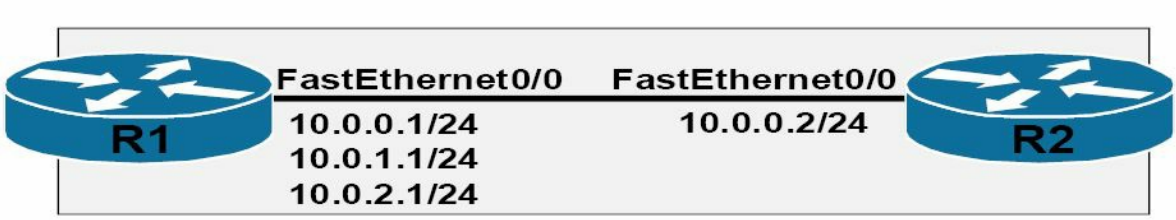


Figure 39.15 – OSPF Secondary Subnet Advertisement

Referencing Figure 39.15, routers R1 and R2 are connected via a back-to-back connection. These two routers share the 10.0.0.0/24 subnet. However, in addition, R1 has been configured with some additional (secondary) subnets under its FastEthernet0/0 interface so that the interface configuration on R1 is printed as follows:

```
R1#show running-config interface FastEthernet0/0
Building configuration...
Current configuration : 183 bytes
!
interface FastEthernet0/0
ip address 10.0.1.1 255.255.255.0 secondary
ip address 10.0.2.1 255.255.255.0 secondary
ip address 10.0.0.1 255.255.255.0
duplex auto
speed auto
end
```

OSPF is enabled on both R1 and R2. The configuration implemented on R1 is as follows:

```
R1#show running-config | section ospf
router ospf 1
router-id 1.1.1.1
```

https://t.me/learningnets

```
log-adjacency-changes
network 10.0.0.1 0.0.0.0 Area 0
network 10.0.1.1 0.0.0.0 Area 1
network 10.0.2.1 0.0.0.0 Area 1
```

The configuration implemented on R2 is as follows:

```
R2#show running-config | section ospf
router ospf 2
router-id 2.2.2.2
log-adjacency-changes
network 10.0.0.2 0.0.0.0 Area 0
```

By default, because the secondary subnets have been placed into a different OSPF area on R1, they will not be advertised by the router. This can be seen on R2, which displays the following when the `show ip route` command is issued:

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, FastEthernet0/0
```

To resolve this issue, the secondary subnets must also be assigned to Area 0, as follows:

```
R1(config)#router ospf 1
R1(config-router)#network 10.0.1.1 0.0.0.0 Area 0
*Mar 18 20:20:37.491: %OSPF-6-AREACHG: 10.0.1.1/32 changed from Area 1 to Area 0
R1(config-router)#network 10.0.2.1 0.0.0.0 Area 0
*Mar 18 20:20:42.211: %OSPF-6-AREACHG: 10.0.2.1/32 changed from Area 1 to Area 0
R1(config-router)#end
```

After this configuration change, the networks are now advertised to router R2, as follows:

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
```

https://t.me/learningnets

```
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/24 is subnetted, 3 subnets
O       10.0.2.0 [110/2] via 10.0.0.1, 00:01:08, FastEthernet0/0
C       10.0.0.0 is directly connected, FastEthernet0/0
O       10.0.1.0 [110/2] via 10.0.0.1, 00:01:08, FastEthernet0/0
```

In addition to the three common causes described above, poor design, implementation, and misconfigurations are another reason OSPF may not advertise networks as expected. Common design issues that cause such issues include a discontiguous or partitioned backbone and area type misconfigurations, such as configuring areas as Totally Stubby, for example. For this reason, it is important to have a solid understanding of how the protocol works and how it has been implemented in your environment. This understanding will greatly simplify the troubleshooting process, as half the battle is already won before you even start troubleshooting the problem or issue.

Debugging OSPF Routing Issues

In the final section of this module, we will look at some of the more commonly used OSPF debugging commands. OSPF debugging is enabled using the `debug ip ospf` command. This command can be used in conjunction with the following additional keywords:

```
R1#debug ip ospf ?
  adj              OSPF adjacency events
  database-timer   OSPF database timer
  events           OSPF events
  flood            OSPF flooding
  hello            OSPF hello events
  lsa-generation   OSPF lsa generation
  mpls             OSPF MPLS
  nsf              OSPF non-stop forwarding events
  packet           OSPF packets
  retransmission   OSPF retransmission events
  spf              OSPF spf
  tree             OSPF database tree
```

The `debug ip ospf adj` command prints real-time information on adjacency events. This is a useful troubleshooting tool when troubleshooting OSPF neighbour adjacency problems. Following is a sample of the information that is printed by this command. The example below illustrates how this command can be used to determine that an MTU mismatch is preventing the neighbour adjacency from reaching the Full state:

```
R1#debug ip ospf adj
OSPF adjacency events debugging is on
R1#
*Mar 1 00:12:12.199: OSPF: DR/BDR election on FastEthernet0/0
```

https://t.me/learningnets

```
*Mar 18 23:13:21.279: OSPF: Elect BDR 2.2.2.2

*Mar 18 23:13:21.279: OSPF: Elect DR 1.1.1.1

*Mar 18 23:13:21.279:        DR: 1.1.1.1 (Id)   BDR: 2.2.2.2 (Id)

*Mar 18 23:13:21.283: OSPF: Neighbor change Event on interface FastEthernet0/0

*Mar 18 23:13:21.283: OSPF: DR/BDR election on FastEthernet0/0

*Mar 18 23:13:21.283: OSPF: Elect BDR 2.2.2.2

*Mar 18 23:13:21.283: OSPF: Elect DR 1.1.1.1

*Mar 18 23:13:21.283:        DR: 1.1.1.1 (Id)   BDR: 2.2.2.2 (Id)

*Mar 18 23:13:21.283: OSPF: Rcv DBD from 2.2.2.2 on FastEthernet0/0 seq 0xA65 opt 0x52
flag 0x7 len 32  mtu 1480 state EXSTART

*Mar 18 23:13:21.283: OSPF: Nbr 2.2.2.2 has smaller interface MTU

*Mar 18 23:13:21.283: OSPF: NBR Negotiation Done. We are the SLAVE

*Mar 18 23:13:21.287: OSPF: Send DBD to 2.2.2.2 on FastEthernet0/0 seq 0xA65 opt 0x52
flag 0x2 len 192

*Mar 18 23:13:26.275: OSPF: Rcv DBD from 2.2.2.2 on FastEthernet0/0 seq 0xA65 opt 0x52
flag 0x7 len 32  mtu 1480 state EXCHANGE

*Mar 18 23:13:26.279: OSPF: Nbr 2.2.2.2 has smaller interface MTU

*Mar 18 23:13:26.279: OSPF: Send DBD to 2.2.2.2 on FastEthernet0/0 seq 0xA65 opt 0x52
flag 0x2 len 192

...

[Truncated Output]
```

From the output above, you can conclude that the MTU on the local router is larger than 1480 bytes because the debug output shows that the neighbour has the smaller MTU value. The recommended solution would be to adjust the smaller MTU value so that both neighbours have the same interface MTU values. This will allow the adjacency to reach the Full state.

The `debug ip ospf lsa-generation` command prints information on OSPF LSAs. This command can be used to troubleshoot route advertisement when using OSPF. Following is a sample output of the information that is printed by this command:

```
R1#debug ip ospf lsa-generation

OSPF summary lsa generation debugging is on

R1#

R1#

*Mar 18 23:25:59.447: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthernet0/0 from FULL
to DOWN, Neighbor Down: Interface down or detached

*Mar 18 23:25:59.511: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthernet0/0 from
LOADING to FULL, Loading Done

*Mar 18 23:26:00.491: OSPF: Start redist-scanning

*Mar 18 23:26:00.491: OSPF: Scan the RIB for both redistribution and translation

*Mar 18 23:26:00.499: OSPF: max-aged external LSA for summary 150.0.0.0 255.255.0.0,
scope: Translation

*Mar 18 23:26:00.499: OSPF: End scanning, Elapsed time 8ms

*Mar 18 23:26:00.499: OSPF: Generate external LSA 192.168.4.0, mask 255.255.255.0, type
```

https://t.me/learningnets

```
5, age 0, metric 20, tag 0, metric-type 2, seq 0x80000001

*Mar 18 23:26:00.503: OSPF: Generate external LSA 192.168.5.0, mask 255.255.255.0, type
5, age 0, metric 20, tag 0, metric-type 2, seq 0x80000001

*Mar 18 23:26:00.503: OSPF: Generate external LSA 192.168.1.0, mask 255.255.255.0, type
5, age 0, metric 20, tag 0, metric-type 2, seq 0x80000001

*Mar 18 23:26:00.503: OSPF: Generate external LSA 192.168.2.0, mask 255.255.255.0, type
5, age 0, metric 20, tag 0, metric-type 2, seq 0x80000001

*Mar 18 23:26:00.507: OSPF: Generate external LSA 192.168.3.0, mask 255.255.255.0, type
5, age 0, metric 20, tag 0, metric-type 2, seq 0x80000001

*Mar 18 23:26:05.507: OSPF: Generate external LSA 192.168.4.0, mask 255.255.255.0, type
5, age 0, metric 20, tag 0, metric-type 2, seq 0x80000006

*Mar 18 23:26:05.535: OSPF: Generate external LSA 192.168.5.0, mask 255.255.255.0, type
5, age 0, metric 20, tag 0, metric-type 2, seq 0x80000006
```

The `debug ip ospf spf` command provides real-time information about Shortest Path First algorithm events. This command can be used in conjunction with the following keywords:

```
R1#debug ip ospf spf ?
  external   OSPF spf external-route
  inter      OSPF spf inter-route
  intra      OSPF spf intra-route
  statistic  OSPF spf statistics
  <cr>
```

As is the case with all `debug` commands, consideration should be given to factors such as the size of the network and the resource utilisation on the router before debugging SPF events. The following is a sample of the output from the `debug ip ospf spf statistic` command:

```
R1#debug ip ospf spf statistic

OSPF spf statistic debugging is on

R1#clear ip ospf process

Reset ALL OSPF processes? [no]: y

R1#

*Mar 18 23:37:27.795: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthernet0/0 from FULL
to DOWN, Neighbor Down: Interface down or detached

*Mar 18 23:37:27.859: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthernet0/0 from
LOADING to FULL, Loading Done

*Mar 18 23:37:32.859: OSPF: Begin SPF at 28081.328ms, process time 608ms

*Mar 18 23:37:32.859:       spf_time 07:47:56.328, wait_interval 5000ms

*Mar 18 23:37:32.859: OSPF: End SPF at 28081.328ms, Total elapsed time 0ms

*Mar 18 23:37:32.859:       Schedule time 07:48:01.328, Next wait_interval 10000ms

*Mar 18 23:37:32.859:       Intra: 0ms, Inter: 0ms, External: 0ms

*Mar 18 23:37:32.859:       R: 2, N: 1, Stubs: 2

*Mar 18 23:37:32.859:       SN: 0, SA: 0, X5: 0, X7: 0

*Mar 18 23:37:32.863:       SPF suspends: 0 intra, 0 total
```

https://t.me/learpingnets

NOTE: Prior to enabling SPF `debug` commands, consider using `show` commands first, such as the `show ip ospf statistics`

and `show ip ospf` commands, when beginning the troubleshooting process.

https://t.me/learningnets

Day 39 Questions

1. OSPF operates over IP number _____.
2. OSPF does NOT support VLSM. True or false?
3. Any router which connects to Area 0 and another area is referred to as an _____ _____ _____ or _____.
4. If you have a DR, you must always have a BDR. True or false?
5. The DR/BDR election is based on which two factors?
6. By default, all routers have a default priority value of _____. This value can be adjusted using the _____ _____ _____ <0-255> interface configuration command.
7. When determining the OSPF router ID, Cisco IOS selects the highest IP address of configured Loopback interfaces. True or false?
8. What roles do the DR and the BDR carry out?
9. Which command would put network 10.0.0.0/8 into Area 0 on a router?
10. Which command would set the router ID to 1.1.1.1?
11. Name the common troubleshooting issues for OSPF.

https://t.me/learningnets

Day 39 Answers

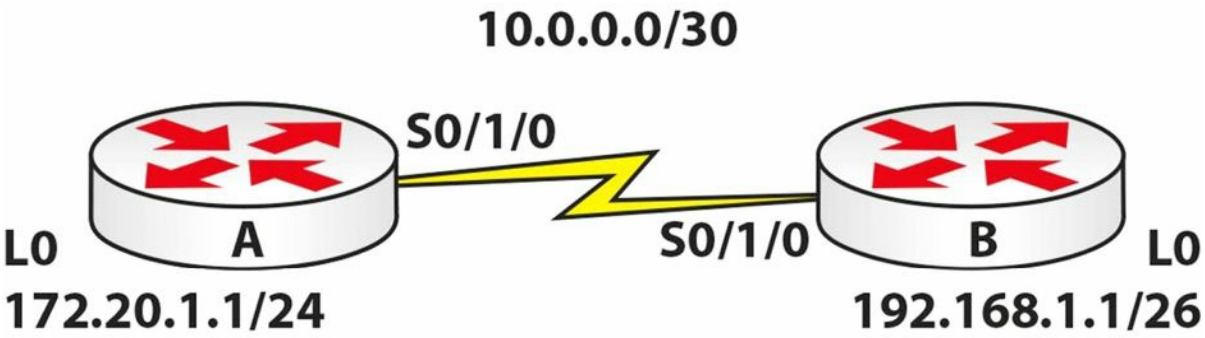
1. 89.
2. False.
3. Area Border Router or ABR.
4. False.
5. The highest router priority and the highest router ID.
6. 1, `ip ospf priority`.
7. True.
8. To reduce the number of adjacencies required on the segment; to advertise the routers on the Multi-Access segment; and to ensure that updates are sent to all routers on the segment.
9. The `network 10.0.0.0 0.255.255.255 area 0` command.
10. The `router-id 1.1.1.1` command.
11. Neighbour relationships and route advertisement.

https://t.me/learningnets

Day 39 Lab

OSPF Lab

Topology



Purpose

Learn how to configure basic OSPF.

Walkthrough

1. Configure all IP addresses based on the topology above. Make sure you can ping across the Serial link.
2. Add OSPF to Router A. Put the network on Loopback0 into Area 1 and the 10 network into Area 0.

```
RouterA(config)#router ospf 4
RouterA(config-router)#network 172.20.1.0 0.0.0.255 area 1
RouterA(config-router)#network 10.0.0.0 0.0.0.3 area 0
RouterA(config-router)#^Z
RouterA#
%SYS-5-CONFIG_I: Configured from console by console
RouterA#show ip protocols
Routing Protocol is "ospf 4"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.20.1.1
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.20.1.0 0.0.0.255 area 1
    10.0.0.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.20.1.1           110      00:00:09
  Distance: (default is 110)
```

https://t.me/learningnets

3. Add OSPF on Router B. Put the Loopback network into OSPF Area 40.

```
RouterB(config)#router ospf 2
RouterB(config-router)#net 10.0.0.0 0.0.0.3 area 0
RouterB(config-router)#
00:22:35: %OSPF-5-ADJCHG: Process 2, Nbr 172.20.1.1 on Serial0/1/0 from LOADING to FULL,
Loading Done
RouterB(config-router)#net 192.168.1.0 0.0.0.63 area 40
RouterB(config-router)# ^Z
RouterB#show ip protocols
Routing Protocol is "ospf 2"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.1.1
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.0.0 0.0.0.3 area 0
    192.168.1.0 0.0.0.63 area 40
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.20.1.1           110      00:01:18
    192.168.1.1          110      00:00:44
  Distance: (default is 110)
```

4. Check the routing table on your routers. Look for the OSPF advertised network. You will see an IA, which means IA – OSPF inter-area. You will also see the AD for OSPF, which is 110.

```
RouterA#sh ip route
...
[Truncated Output]
     10.0.0.0/30 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Serial0/1/0
     172.20.0.0/24 is subnetted, 1 subnets
C       172.20.1.0 is directly connected, Loopback0
     192.168.1.0/32 is subnetted, 1 subnets
O IA    192.168.1.1 [110/65] via 10.0.0.2, 00:01:36, Serial0/1/0
RouterA#
```

5. Issue some of the available OSPF commands on either router.

```
RouterA#sh ip ospf ?
  <1-65535>       Process ID number
```

https://t.me/learningnets

```
  border-routers  Border and Boundary Router Information
  database        Database summary
  interface       Interface information
  neighbor        Neighbor list
```

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 40 – Syslog, SNMP, and Netflow

Day 40 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's lab
- Read the ICND2 cram guide
- Spend 15 minutes on the subnetting.org website

Logging messages and events both locally and to a syslog server is a core maintenance task. Syslog is a protocol that allows a host to send event notification messages across IP networks to event message collectors – also known as syslog servers or syslog daemons. In other words, a host or a device can be configured in such a way that it generates a syslog message and forwards it to a specific syslog daemon (server).

The Simple Network Management Protocol (SNMP) is a widely used management protocol and defined set of standards for communications with devices connected to an IP network. SNMP provides a means to monitor and control network devices. Like Cisco IOS IP SLA operations (which allow customers to analyse IP service levels using active traffic monitoring for measuring network performance), SNMP can be used to collect statistics, monitor device performance, and provide a baseline of the network, and is one of the most commonly used network maintenance and monitoring tools.

While SNMP can provide traffic statistics, SNMP cannot differentiate between individual flows. However, Cisco IOS NetFlow can. A flow is simply a series of packets with the same source and destination IP address, source and destination ports, protocol interface, and Class of Service parameters.

Today you will learn about the following:

- Syslog
- SNMP
- Netflow

This lesson maps to the following CCNA syllabus requirements:

- Configure and verify syslog
  - Utilise syslog outputs
- Describe SNMP v2 and v3
- Utilise netflow data

Logging

https://t.me/learningnets

A syslog daemon or server is an entity that listens to the syslog messages that are sent to it.

You cannot configure a syslog daemon to ask a specific device to send it syslog messages. In other words, if a specific device has no ability to generate syslog messages, then a syslog daemon cannot do anything about it. In the real world, corporations typically use SolarWinds (or similar) software for syslog capturing. Additionally, freeware such as the Kiwi Syslog daemon is also available for syslog capturing.

Syslog uses User Datagram Protocol (UDP) as the underlying transport mechanism, so the data packets are unsequenced and unacknowledged. While UDP does not have the overhead included in TCP, this means that on a heavily used network, some packets may be dropped and therefore logging information will be lost. However, Cisco IOS software allows administrators to configure multiple syslog servers for redundancy. A syslog solution is comprised of two main elements: a syslog server and a syslog client.

The syslog client sends syslog messages to the syslog sever using UDP as the Transport Layer protocol, specifying a destination port of 514. These messages cannot exceed 1024 bytes in size; however, there is no minimum length. All syslog messages contain three distinct parts: the priority, the header, and the message.

The priority of a syslog message represents both the facility and the severity of the message. This number is an 8-bit number. The first 3 least significant bits represent the severity of the message (with 3 bits, you can represent 8 different severities) and the other 5 bits represent the facility. You can use these values to apply filters on the events in the syslog daemon.

NOTE: Keep in mind that these values are generated by the applications on which the event is generated, not by the syslog server itself.

The values set by Cisco IOS devices are listed and described below in Table 40.1 (please memorise the levels and level names):

Table 40.1 – Cisco IOS Software Syslog Priority Levels and Definitions

Level	Level Name	Syslog Definition	Description
0	Emergencies	LOG_EMERG	This level is used for the most severe error conditions, which render the system unusable.
1	Alerts	LOG_ALERT	This level is used to indicate conditions that need immediate attention from administrators.
2	Critical	LOG_CRIT	This level is used to indicate critical conditions, which are less critical than Alerts but still require administrator intervention.
3	Errors	LOG_ERR	This level is used to indicate errors within the system; however, these errors do not render the system unusable.
4	Warnings	LOG_WARNING	This level is used to indicate warning conditions about system operations that did not complete successfully.
5	Notifications	LOG_NOTICE	This level is used to indicate state changes within the system (e.g., a routing protocol adjacency transitioning to a down state).
6	Informational	LOG_INFO	This level is used to indicate informational messages about the normal operation of the system.

https://t.me/learningnets

7	Debugging	LOG_DEBUG	This level is used to indicate real-time (debugging) information that is typically used for troubleshooting purposes.

In syslog, the facility is used to represent the source that generated the message. This source can be a process on the local device, an application, or even an operating system. Facilities are represented by numbers (integers). In Cisco IOS software, there are eight local use facilities that can be used by processes and applications (as well as the device itself) for sending syslog messages. By default, Cisco IOS devices use facility local7 to send syslog messages. However, it should be noted that most Cisco devices provide options to change the default facility level. In Cisco IOS software, the `logging facility [facility]` global configuration command can be used to specify the syslog facility. The options available with this command are as follows:

```
R1(config)#logging facility ?
  auth    Authorization system
  cron    Cron/at facility
  daemon  System daemons
  kern    Kernel
  local0  Local use
  local1  Local use
  local2  Local use
  local3  Local use
  local4  Local use
  local5  Local use
  local6  Local use
  local7  Local use
  lpr     Line printer system
  mail    Mail system
  news    USENET news
  sys10   System use
  sys11   System use
  sys12   System use
  sys13   System use
  sys14   System use
  sys9    System use
  syslog  Syslog itself
  user    User process
  uucp    Unix-to-Unix copy system
```

To send messages via syslog, you must perform the following sequence of steps on the device:

1. Globally enable logging on the router or switch using the `logging on` configuration command. By default, in Cisco IOS software, logging is enabled; however, it is only enabled to send messages to the console. The `logging on` command is a mandatory

https://t.me/learningnets

requirement when sending messages to any destination other than the console.

2. Specify the severity of messages to send to the syslog server using the `logging trap [severity]` global configuration command. You can specify the severity numerically or using the equivalent severity name.
3. Specify one or more syslog server destinations using the `logging [address]` or `logging host [address]` global configuration commands.
4. Optionally, specify the source IP address used in syslog messages using the `logging source-interface [name]`. This is a common practice on devices with multiple interfaces configured. If this command is not specified, then the syslog message will contain the IP address of the router or switch interface used to reach the server. If there are multiple interfaces for redundancy, this address may change when the primary path (interface) is down. Therefore, it is typically set to a Loopback interface.

The following configuration example illustrates how to send all informational (level 6) and below messages to a syslog server with the IP address 192.168.1.254:

```
R2(config)#logging on
R2(config)#logging trap informational
R2(config)#logging 192.168.1.254
```

This configuration can be validated using the `show logging` command, as illustrated below:

```
R2#show logging
Syslog logging: enabled (11 messages dropped, 1 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,filtering disabled
    Buffer logging: disabled, xml disabled, filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
No active filter modules.
    Trap logging: level informational, 33 message lines logged
        Logging to 192.168.1.254(global) (udp port 514, audit disabled,  link up), 2
message lines logged, xml disabled,
                filtering disabled
```

When configuring logging in general, it is important to ensure that the router or switch clocks reflect the actual current time, which allows you to correlate the fault data. Inaccurate or incorrect timestamps on log messages make the fault and problem isolation using a filtration and correlation process very difficult and very time consuming. In Cisco IOS devices, the system clock can be configured manually or the device can be configured to synchronise its clock with a Network Time Protocol (NTP) server. These two options are discussed in the following sections.

Manual clock or time configuration is fine if you have only a few internetwork devices in your network. In Cisco IOS software, the system time is configured using the `clock set hh:mm:ss [day & month | month & day] [year]` privileged EXEC command. It is not configured or specified in

https://t.me/learningnets

Global Configuration mode. The following configuration example illustrates how to set the system clock to October 20 12:15 AM:

```
R2#clock set 12:15:00 20 october 2010
```

Alternatively, the same configuration could be implemented on the router as follows:

```
R2#clock set 12:15:00 october 20 2010
```

Following this configuration, the `show clock` command can be used to view the system time:

```
R2#show clock
12:15:19.419 UTC Wed Oct 20 2010
```

One interesting observation of note is that when the system time is configured manually or set using the `clock set` command, it defaults to the GMT (UTC) time zone, as can be seen above. In order to ensure that the system clock reflects the correct time zone, for those who are not in the GMT time zone, you must use the `clock timezone [time zone name] [GMT offset]` global configuration command. For example, the United States has six different time zones, each with a different GMT offset. These time zones are Eastern Time, Central Time, Mountain Time, Pacific Time, Hawaii Time, and Alaska Time.

In addition, some of the time zones use Standard Time and Daylight Saving Time. Given this, it is important to ensure that the system time is set correctly (Standard or Daylight Saving) on all devices when manually configuring the system clock. The following configuration example illustrates how to set the system clock to 12:40 AM on October 20 for the Central Standard Time (CST) time zone, which is six hours behind GMT:

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#clock timezone CST -6
R2(config)#end
R2#clock set 12:40:00 october 20 2010
```

Following this configuration, the system clock on the local router now shows the following:

```
R2#show clock
12:40:17.921 CST Wed Oct 20 2010
```

NOTE: If you use the `clock set` command before the `clock timezone` command, then the time that you specified using the `clock set` command will be offset by using the `clock timezone` command. For example, assume that the configuration commands that are used in the example above were entered on the router as follows:

```
R2#clock set 12:40:00 october 20 2010
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#clock timezone CST -6
R2(config)#end
```

Because the `clock set` command is used first, the output of the `show clock` command on the router would show the system clock offset by 6 hours, as specified using the `clock timezone`

https://t.me/learningnets

command. This behaviour is illustrated in the following output on the same router:

```
R2#show clock
06:40:52.181 CST Wed Oct 20 2010
```

NOTE: Cisco IOS routers and switches can be configured to switch automatically to summertime (Daylight Saving Time) using the `clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]` global configuration command. This negates the need to have to adjust the system clock manually on all manually configured devices during Standard Time and Daylight Saving Time periods.

The second method of setting or synchronising the system clock is to use a Network Time Protocol (NTP) server as a reference time source. This is the preferred method in larger networks with more than just a few internetwork devices. NTP is a protocol that is designed to time-synchronise a network of machines. NTP is documented in RFC 1305 and runs over UDP.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronise two machines to within a millisecond of one another.

NTP uses the concept of a stratum to describe how many NTP hops away a machine is from an authoritative time source. Keep in mind that this is not routing or switching hops, but NTP hops, which is a totally different concept. A stratum 1 time server typically has a radio or atomic clock directly attached, while a stratum 2 time server receives its time via NTP from a stratum 1 time server, and so on. When a device is configured with multiple NTP reference servers, it will automatically choose as its time source the machine with the lowest stratum number that it is configured to communicate with via NTP.

In Cisco IOS software, a device is configured with the IP addresses of one or more NTP servers using the `ntp server [address]` global configuration command. As previously stated, multiple NTP reference addresses can be specified by repeatedly using the same command. In addition, this command can also be used to configure security and other features between the server and the client. The following configuration example illustrates how to configure a device to synchronise its time with an NTP server with the IP address 10.0.0.1:

```
R2(config)#ntp server 10.0.0.1
```

Following this configuration, the `show ntp associations` command can be used to verify the communications between the NTP devices, as illustrated in the following output:

```
R2#show ntp associations
address      ref clock     st  when  poll reach  delay  offset  disp
*~10.0.0.1   127.127.7.1   5   44    64   377    3.2    2.39    1.2
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

The `address` field indicates the IP address of the NTP server as confirmed by the value 10.0.0.1 specified under this field. The `ref clock` field indicates the reference clock used by that NTP server. In this case, the IP address 127.127.7.1 indicates that the device is using an internal clock (127.0.0.0/8 subnet) as its reference time source. If this field contained another value, such as

https://t.me/learningnets

192.168.1.254, for example, then that would be the IP address the server was using as its time reference.

Next, the `st` field indicates the stratum of the reference. From the output printed above, you can see that the 10.0.0.1 NTP device has a stratum of 5. The stratum on the local device will be incremented by 1 to a value of 6, as shown below, because it receives its time source from a server with a stratum value of 5. If another device was synchronised to the local router, it would reflect a stratum of 7 and so forth. The second command that is used to validate the NTP configuration is the `show ntp status` command, the output of which is illustrated below:

```
R2#show ntp status
Clock is synchronized, stratum 6, reference is 10.0.0.1
nominal freq is 249.5901 Hz, actual freq is 249.5900 Hz, precision is 2**18
reference time is C02C38D2.950DA968 (05:53:22.582 UTC Sun Mar 3 2002)
clock offset is 4.6267 msec, root delay is 3.16 msec
root dispersion is 4.88 msec, peer dispersion is 0.23 msec
```

The output of the `show ntp status` command indicates that the clock is synchronised to the configured NTP server (10.0.0.1). This server has a stratum of 5, hence the local device reflects a stratum of 6. An interesting observation when NTP is configured is that the local time still defaults to GMT, as can be seen in the bolded section above. To ensure that the device displays the correct time zone, you must issue the `clock time-zone` command on the device.

After the system clock has been set, either manually or via NTP, it is important to ensure that the logs sent to the server contain the correct timestamps. This is performed using the `service timestamps log [datetime | uptime]` global configuration command. The `[datetime]` keyword supports the following self-explanatory additional subkeywords:

```
R2(config)#service timestamps log datetime ?
  localtime      Use local time zone for timestamps
  msec           Include milliseconds in timestamp
  show-timezone  Add time zone information to timestamp
  year           Include year in timestamp
  <cr>
```

The `[uptime]` keyword has no additional subkeywords and configures the local router to include only the system uptime as the timestamp for sent messages. The following configuration example illustrates how to configure the local router to include the local time, millisecond information, and the time zone for all messages:

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#logging on
R2(config)#logging console informational
R2(config)#logging host 150.1.1.254
R2(config)#logging trap informational
R2(config)#service timestamps log datetime localtime msec show-timezone
```

https://t.me/learningnets

Following this configuration, the local router console would print the following message:

```
Oct 20 02:14:10.519 CST: %SYS-5-CONFIG_I: Configured from console by console

Oct 20 02:14:11.521 CST: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 150.1.1.254
started - CLI initiated
```

In addition, the syslog daemon on server 150.1.1.254 would also reflect the same, as illustrated in the Kiwi Syslog Manager screenshot in Figure 40.1 below:

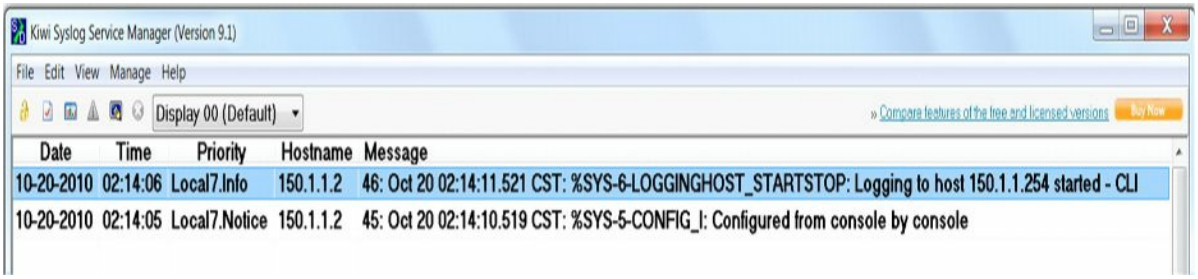


Figure 40.1 – Configuring Log Timestamps

Simple Network Management Protocol

SNMP is an Application Layer (Layer 7) protocol, using UDP ports 161 and 162, that facilitates the exchange of management information between network devices. An SNMP-managed network consists of a management system, agents, and managed devices. The management system executes monitoring applications and controls managed devices. It also executes most of the management processes and provides the bulk of memory resources used for network management. A network might be managed by one or more management systems.

An SNMP agent resides on each managed device and translates local management information data, such as performance information or event and error information caught in software traps, into a readable form for the management system. SNMP agents use get-requests that transport data to the network management software. SNMP agents capture data from Management Information Bases (MIBs), which are device parameter and network data repositories, or from error or change traps.

A managed element, such as a router, a switch, a computer, or a firewall, is accessed via the SNMP agent. Managed devices collect and store management information, making it available through SNMP to other management systems having the same protocol compatibility. Figure 40.2 below illustrates the interaction of the three primary components of an SNMP-managed network:

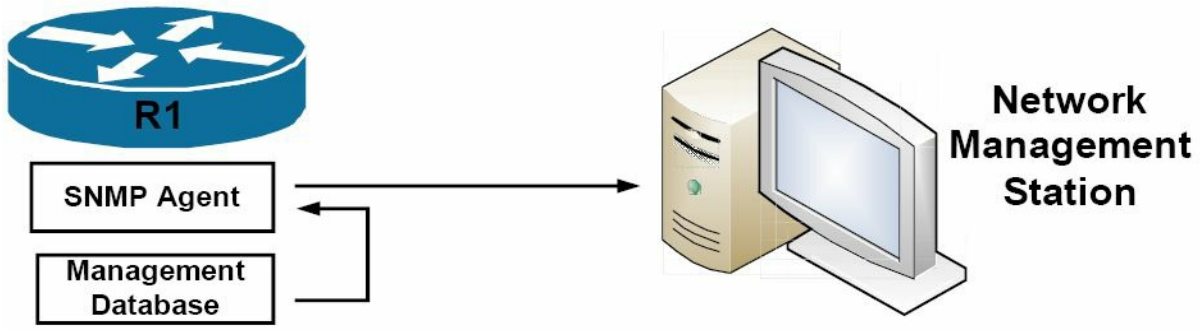


Figure 40.2 – SNMP Network Component Interaction

https://t.me/learningnets

Referencing Figure 40.2, R1 is the SNMP-managed device. Logically residing on the device is the

SNMP agent. The SNMP agent translates local management information data, stored in the management database of the managed device, into a readable form for the management system, which is also referred to as the Network Management Station (NMS).

When using SNMP, managed devices are monitored and controlled using three common SNMP commands: `read`, `write`, and `trap`. The `read` command is used by an NMS to monitor managed devices. This is performed by the NMS examining different variables that are maintained by managed devices. The `write` command is used by an NMS to control managed devices. Using this command, the NMS can change the values of variables stored within managed devices. Finally, the SNMP `trap` command is used by managed devices to report events to the NMS. Devices can be configured to send SNMP traps or informs to an NMS. The traps and informs that are sent are dependent on the version of Cisco IOS software running on the device, as well as the platform.

SNMP traps are simply messages that alert the SNMP manager of a condition on the network. An example of an SNMP trap could include an interface transitioning from an up state to a down state. The primary issue with SNMP traps is that they are unacknowledged. This means that the sending device is incapable of determining whether the trap was received by the NMS.

SNMP informs are SNMP traps that include a confirmation of receipt from the SNMP manager. These messages can be used to indicate failed authentication attempts, or the loss of a connection to a neighbour router, for example. If the manager does not receive an inform request, then it does not send a response. If the sender never receives a response, then the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

While informs are more reliable than traps, the downside is that they consume more resources on both the router and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. In addition, traps are sent only once, while an inform may be resent several times if a response is not received from the SNMP server (NMS).

Figure 40.3 below illustrates the communication between the SNMP manager and the SNMP agent for sending traps and informs:

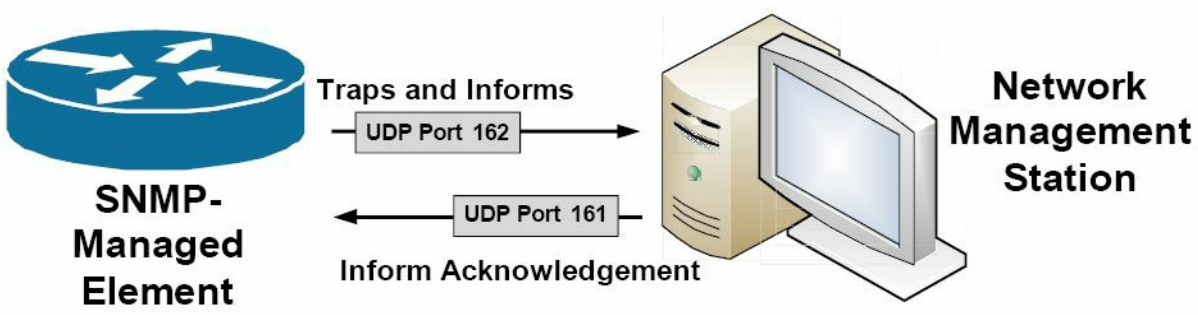


Figure 40.3 – UDP Ports Used by the NMS and the SNMP-Managed Element

The three versions of SNMP are versions 1, 2, and 3. Version 1, or SNMPv1, is the initial implementation of the SNMP protocol. SNMPv1 operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), and the OSI Connectionless Network Service (CLNS).

https://t.me/learningnets

SNMPv1 is widely used and is the de facto network-management protocol used within the Internet community.

SNMPv2 revises SNMPv1 and includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. SNMPv2 also defines two new operations: GetBulk and Inform. The GetBulk operation is used to retrieve large blocks of data efficiently. The Inform operation allows one NMS to send trap information to another NMS and then to receive a response. In SNMPv2, if the agent responding to GetBulk operations cannot provide values for all the variables in a list, then it provides partial results.

SNMPv3 provides the following three additional security services that are not available in previous versions of SNMP: message integrity, authentication, and encryption. SNMPv3 uses message integrity to ensure that a packet has not been tampered with in-transit. SNMPv3 also utilises authentication, which is used to determine whether the message is from a valid source. Finally, SNMPv3 provides encryption, which is used to scramble the contents of a packet to prevent it from being seen by unauthorised sources.

In Cisco IOS software, the `snmp-server host [hostname | address]` command is used to specify the hostname or IP address of the NMS to which the local device will send traps or informs. To allow the NMS to poll the local device, SNMPv1 and SNMPv2c require that a community string be specified for either read-only or read-write access using the `snmp-server community <name> [ro | rw]` global configuration command.

SNMPv3 does not use the same community-based form of security but instead uses user and group security. The following configuration example illustrates how to configure the local device with two community strings, one for read-only access and the other for read-write access. In addition, the local device is also configured to send SNMP traps for Cisco IOS IP SLA operations and syslog to 1.1.1.1 using the read-only community string:

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#snmp-server community unsafe RO
R2(config)#snmp-server community safe RW
R2(config)#snmp-server host 1.1.1.1 traps readonlypassword rtr syslog
```

Figure 40.4 below illustrates a sample report for device resource utilisation and availability based on SNMP polling using ManageEngine OpManager network monitoring software:

https://t.me/learningnets



Figure 40.4 – Sample SNMP Report on Device Resource Utilisation

Cisco IOS NetFlow

Like SNMP, Cisco IOS NetFlow is a powerful maintenance and monitoring tool that can be used to baseline network performance and assist in troubleshooting. However, there are some significant differences between Cisco IOS NetFlow and SNMP. The first difference is that while SNMP reports primarily on device statistics (e.g., resource utilisation, etc.), Cisco IOS NetFlow reports on traffic statistics (e.g., packets and bytes).

The second difference between these two tools is that SNMP is a poll-based protocol, meaning that the managed device is polled for information. It can also be considered push-based in the instance that a SNMP device sends a trap (event report) to a management station. Cisco IOS NetFlow, however, is a push-based technology, meaning that the device on which NetFlow is configured sends out information that it has collected locally to a central repository. For this reason, NetFlow and SNMP complement each other and should be used together as part of the standard network maintenance and monitoring toolkit. However, they are not replacements for each other; this is often a misunderstood concept and it is important that you remember this.

An IP flow is based on a set of five, and up to seven, IP packet attributes, which may include the following:

- ☐ Destination IP address
- ☐ Source IP address
- ☐ Source port
- ☐ Destination port
- ☐ Layer 3 protocol type
- ☐ Class of Service

https://t.me/learningnets

- Router or switch interface

In addition to these IP attributes, other additional information is also included with a flow. This additional information includes timestamps, which are useful for calculating packets and bytes per second. Timestamps also provide information on the life (duration) of a flow. The flow also includes next-hop IP address information, including BGP routing autonomous systems information. Subnet mask information for the flow source and destination addresses is also included, in addition to flags for TCP traffic, which can be used to examine the TCP handshakes.

In short, Cisco IOS NetFlow can be used for network traffic accounting, usage-based network billing, network planning, security, Denial of Service (DoS) monitoring capabilities, and network monitoring, in addition to providing information about network users and applications, peak usage times, and traffic routing. All of this makes it a very powerful maintenance, monitoring, and troubleshooting tool.

Cisco IOS NetFlow gathers the flow information and stores it in a database called the NetFlow cache or simply the flow cache. Flow information is retained until the flow is terminated or stopped, times out, or the cache is filled. Two methods can be used to access the data stored in the flow: using the CLI (i.e., using `show` commands) or exporting the data and then viewing it using some type of reporting tool. Figure 40.5 below illustrates NetFlow operation on a Cisco IOS router and how the flow cache is populated:

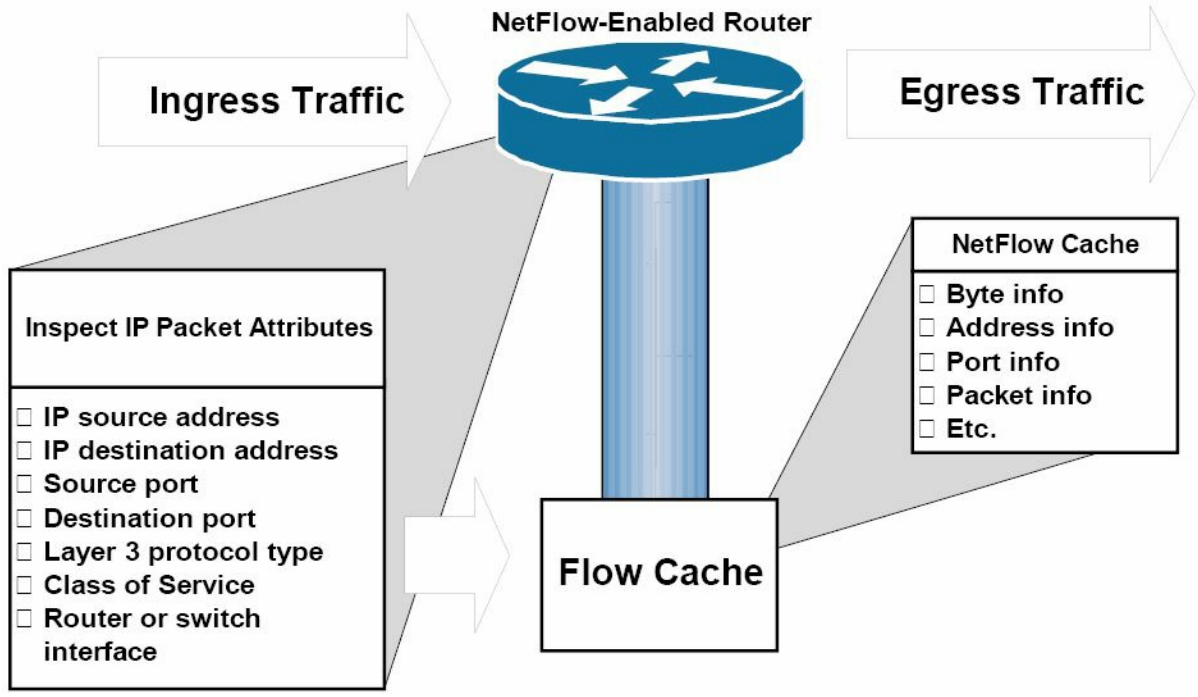


Figure 40.5 – Basic NetFlow Operation and Flow Cache Population

Referencing Figure 40.5, ingress traffic is received on the local router. This traffic is inspected by the router and IP attribute information is used to create a flow. The flow information is then stored in the flow cache. This information can be viewed using the CLI or can also be exported to an external destination, referred to as a NetFlow Collector, where the same information can then be viewed using an application reporting tool. The following steps are used to implement NetFlow data reporting to the NetFlow Collector:

1. Cisco IOS NetFlow is configured on the device to capture flows to the NetFlow cache.

https://t.me/learningnets

2. NetFlow export is configured to send flows to the Collector.
3. The NetFlow cache is searched for flows that have been inactive for a certain period of time, have been terminated, or, for active flows, that last greater than the active timer.
4. Those identified flows are exported to the NetFlow Collector server.
5. Approximately 30 to 50 flows are bundled together and are typically transported via UDP.
6. The NetFlow Collector software creates real-time or historical reports from the data.

Three primary steps are required when configuring Cisco IOS NetFlow, as follows:

1. Configure the interface to capture flows into the NetFlow cache using the `ip flow ingress` interface configuration command on all interfaces for which you want information to be captured and stored in the flow cache. It is important to remember that NetFlow is configured on a per-interface basis only.

Note from Dario: The `ip route-cache flow` command will enable flows on the physical interface and all subinterfaces associated with it.

The `ip flow ingress` command will enable flows on individual subinterfaces, as opposed to all of them on the same interface. This comes in handy when you are not interested in seeing flows on subinterfaces X, Y, and Z, but you do want to see flows on subinterfaces A, B, and C from that same physical interface.

Additionally, with NetFlow v5, the only option was to monitor inbound statistics using the `ip flow ingress` command. However, with the release of NetFlow v9, you now have the option to monitor traffic leaving each interface using the `ip flow egress` command.

NOTE: Effective with Cisco IOS Releases 12.4(2)T and 12.2(18)SXD, the `ip route-cache flow` command has been replaced by the `ip flow ingress` command. Effective with Cisco IOS Releases 12.2(25)S, the output of the `show running configuration` command was modified so that the `ip route-cache flow` command, as well as the `ip flow ingress` command, will appear when either command is configured.

The NetFlow information is then stored on the local router and can be viewed using the `show ip cache flow` command on the local device.

In the event that you want to export data to the NetFlow Collector, two additional tasks will be required, as follows:

2. Configure the Cisco IOS NetFlow version or format using the `ip flow-export version [1 | 5 | 9]` global configuration command. NetFlow version 1 (v1) is the original format supported in the initial NetFlow releases. This version should be used only when it is the only NetFlow data export format version that is supported by the application that you are using to analyse the exported NetFlow data. Version 5 exports more fields than version 1 does and is the most widely deployed version. Version 9 is the latest Cisco IOS NetFlow version and is the basis of a new IETF standard. Version 9 is a flexible export format version.
3. Configure and specify the IP address of the NetFlow Collector, and then specify the UDP port that the NetFlow Collector will use to receive the UDP export from the Cisco device, using the `ip flow-export destination [hostname | address] <port> [udp]` global

https://t.me/learninghets

configuration command. The `[udp]` keyword is optional and does not need to be specified when using this command because User Datagram Protocol (UDP) is the default transport protocol used when sending data to the NetFlow Collector.

The following example illustrates how to enable NetFlow for a specified router interface:

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface Serial0/0
R1(config-if)#ip flow ingress
R1(config-if)#end
```

Following this configuration, the `show ip cache flow` command can be used to view collected statistics in the flow cache, as illustrated in the output below:

```
R1#show ip cache flow
IP packet size distribution (721 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .980 .016 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .002 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 56 added
  1195 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  4 active, 1020 inactive, 56 added, 56 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           2      0.0        34    40      0.0      10.5      15.7
TCP-WWW              2      0.0         9    93      0.0       0.1       1.5
UDP-NTP              1      0.0         1    76      0.0       0.0      15.4
UDP-other           42      0.0         5    59      0.0       0.0      15.7
ICMP                 5      0.0        10    64      0.0       0.0      15.1
Total:              52      0.0         7    58      0.0       0.4      15.1
SrcIf      SrcIPaddress   DstIf   DstIPaddress   Pr SrcP DstP  Pkts
Se0/0      150.1.1.254    Local   10.0.0.1       01 0000 0800   339
Se0/0      10.0.0.2       Local   1.1.1.1        06 C0B3 0017     7
Se0/0      10.0.0.2       Local   10.0.0.1       11 07AF D0F1     1
Se0/0      10.0.0.2       Local   10.0.0.1       11 8000 D0F1    10
```

https://t.me/learningnets

```
Se0/0      150.1.1.254    Local   10.0.0.1        01 0000 0800   271
Se0/0      10.0.0.2       Local   1.1.1.1         06 C0B3 0017    59
```

The following example illustrates how to configure and enable NetFlow data collection for the specified router interfaces, and then export the data to a NetFlow Collector with the IP address 150.1.1.254 over UDP port 5000 using NetFlow version 5 data format:

```
R1(config)#interface Serial0/0
R1(config-if)#ip flow ingress
R1(config-if)#exit
R1(config)#interface FastEthernet0/0
R1(config-if)#ip flow ingress
R1(config-if)#exit
R1(config)#interface Serial0/1
R1(config-if)#exit
R1(config)#ip flow-export version 5
R1(config)#ip flow-export destination 150.1.1.254 5000
R1(config)#exit
```

Following this configuration, the collected information can then be viewed using an application reporting tool on the NetFlow Collector. Despite the export of data, the `show ip cache flow` command can still be used to view statistics on the local device, which can be a useful tool when troubleshooting network issues or problem reports.

Troubleshooting Utilising NetFlow Data

A typical enterprise network has thousands of connections generating massive amounts of NetFlow data in only a short period of time. NetFlow data can be transformed into useful graphs and tables that help network administrators understand what is going on inside the network. NetFlow data can assist with the following:

- Improve overall network performance
- Support latency-sensitive applications, such as voice over IP (VoIP)
- Better manage traffic spikes
- Enforce network policies
- Expose traffic patterns that point to malicious activities

NetFlow statistics can also help administrators understand what percentage of network resources is being consumed by each data type at any given time. You can see at a glance how much bandwidth is being used by e-mail, accounting and ERP systems, and other applications, as well as how many users are watching YouTube videos or making Internet phone calls during the work day.

NetFlow data can be presented in an easy to understand format that enables administrators to easily drill down into more details. They can examine traffic flows by user, application, department, conversation, interface, and protocol. Some examples of situations that can be

https://t.me/learningnets

solved using NetFlow data include the following:

- Capacity issues: NetFlow can clearly show what applications use the most bandwidth and when. This information can help in changing the application traffic patterns in order to improve network performance. This can also be applied to user traffic.
- Security issues: NetFlow data can detect unauthorised traffic patterns across the network and can stop the threat before any harm is done to the network.
- VoIP problems (poor quality, for example) can be corrected after being identified using NetFlow analysers. NetFlow reports can show insufficient bandwidth, latency, or jitter issues that affect the VoIP calls.

https://t.me/learningnets

Day 40 Questions

1. What underlying protocol does syslog use?
2. The syslog client sends syslog messages to the syslog sever using UDP as the Transport Layer protocol, specifying a destination port of _____.
3. The priority of a syslog message represents both the facility and the severity of the message. This number is an _____ -bit number.
4. Name the eight Cisco IOS syslog priority levels.
5. In Cisco IOS software, the _____ _____ _____ global configuration command can be used to specify the syslog facility.
6. Which command do you use to globally enable logging on a router?
7. Name the command used to specify the syslog server destination.
8. Name the command used to set the clock on a Cisco IOS router.
9. On which ports does SNMP operate?
10. Name the command you can use to change the NetFlow version.

https://t.me/learningnets

Day 40 Answers

1. UDP.
2. 514.
3. 8.
4. Emergencies, alerts, critical, errors, warnings, notifications, informational, and debugging.
5. The `logging facility [facility]` command.
6. The `logging on` command.
7. The `logging [address]` or `logging host [address]` command.
8. The `clock set` command.
9. UDP 161 and 162.
10. The `ip flow-export version x` global configuration command.

https://t.me/learningnets

Day 40 Labs

Logging Lab

Configure logging on a Cisco router:

- ☐ Choose the logging facility local3: logging facility local2
- ☐ Issue the global `logging on` command
- ☐ Choose logging severity informational
- ☐ Configure a free syslog server on a PC and connect it to the router
- ☐ Issue the `logging [address]` command to specify the syslog server
- ☐ Specify the `logging source-interface` command
- ☐ Verify the `show logging` command
- ☐ Configure the `service timestamps log datetime localtime msec show-timezone` command
- ☐ Verify the syslog messages on the PC

SNMP Lab

Configure SNMP on a Cisco router:

- ☐ Configure the SNMP server with the `snmp-server host` command
- ☐ Configure SNMP RO and RW communities using the `snmp-server community` command

NetFlow Lab

Configure NetFlow on a Cisco router:

- ☐ Enable IP flow ingress and egress on a router interface
- ☐ Verify the `show ip cache flow` command after traffic passes the router
- ☐ Configure the NetFlow version using the `ip flow-export` command
- ☐ Configure an external NetFlow server using `ip flow-export` destination

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 41 – Wide Area Networking

Day 41 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete the lab(s) of your choice
- Read the ICND2 cram guide
- Spend 15 minutes on the subnetting.org website

Cisco split WAN concepts between the ICND1 and ICND2 exams, with the latter focusing on Frame Relay and PPP protocols. For this reason, we will look at basic WAN concepts, technologies, and protocols.

Today you will learn about the following:

- WAN components
- WAN protocols
- Basic serial line configuration
- Troubleshooting WAN connections

This lesson maps to the following ICND2 syllabus requirements:

- Identify different WAN Technologies
  - Metro Ethernet
  - VSAT
  - T1 / E1
  - T3 / E3
  - ISDN
  - DSL
  - Cable
  - Cellular 3G / 4G
  - VPN
  - MPLS
- Configure and verify a basic WAN serial connection
- Implement and troubleshoot PPPoE

WAN Overview

https://t.me/learningnets

Wide Area Networks (WAN) span across large geographical distances in order to provide

connectivity for various parts of the network infrastructure. Unlike the Local Area Network (LAN) environment, not all WAN components are owned by the specific enterprise they serve. Instead, WAN equipment or connectivity can be rented or leased from service providers.

Most service providers are well trained in order to make sure they can properly support not just the traditional data traffic but also voice and video services (which are more delay sensitive) over large geographical distances.

Another interesting thing about WANs is that, unlike LANs, there is typically some initial fixed cost and some periodic recurring fees for the services. With wide area networking, not only do you not own the connection and some of the equipment but you will also have to regularly pay fees to the service providers. This is one of the reasons why you should avoid over-provisioning (i.e., buy only the bandwidth you think you will use). This leads to the need for implementing effective Quality of Service mechanisms to avoid buying additional WAN bandwidth. The high costs are usually associated with the recurring fees that might appear in the case of over-provisioning the bandwidth.

WAN technology design requirements are typically derived from the following:

- Application type
- Application availability
- Application reliability
- Costs associated with a particular WAN technology
- Usage levels for the application

WAN Categories

An essential concept in WAN categorisation is circuit-switched technology, the most relevant example of this technology being the Public Switched Telephone Network (PSTN). One of the technologies that fall into this category is ISDN. The way circuit-switched WAN connections function is by becoming established when needed and terminating when they are no longer required. Another example that reflects this circuit-switching behaviour is the old-fashioned dial-up connection (dial-up modem analog access over the PSTN).

NOTE: Not too long ago, dial-up technology was the only way to access Internet resources, offering an average usable bandwidth of around 40Kbps. Nowadays, this technology is almost extinct.

The opposite of the circuit-switched option is leased-line technology. This is a fully dedicated connection that is permanently up and is owned by the company. Examples of leased lines include Time Division Multiplexing (TDM)-based leased lines. These are usually very expensive because a single customer has full use of the connection.

Another popular category of WAN technology involves packet-switched networks. In a packet-switched infrastructure, shared bandwidth utilises virtual circuits. The customer can create a virtual path (similar to a leased line) through the service provider infrastructure cloud. This virtual circuit has a dedicated bandwidth, even though technically this is not a real leased line.

https://t.me/learningnets

Frame Relay is an example of this type of technology.

Some legacy WAN technologies include X.25, which is the predecessor of Frame Relay. This technology is still present in some implementations but it is very rare (Frame Relay is also pretty rare nowadays).

Another WAN category you may have heard about is cell-switched technology. This is often included in packet-switched technologies, as they are very similar. A cell-switched technology example is ATM (Asynchronous Transfer Mode, which is also pretty rare nowadays). This operates by using fixed-size cells, instead of using packets (as used in Frame Relay). Cell-switched technologies form a shared bandwidth environment so that the service provider can guarantee customers a certain level of bandwidth through their infrastructure.

Broadband is another growing WAN category and this includes technologies such as the following:

- DSL
- Cable
- Wireless

Broadband has the capability of taking a connection, like the old-fashioned coaxial cable that carries TV signals, and figuring out how to use different aspects of that bandwidth. For example, by using multiplexing an additional data signal could be transmitted along with the original TV signal.

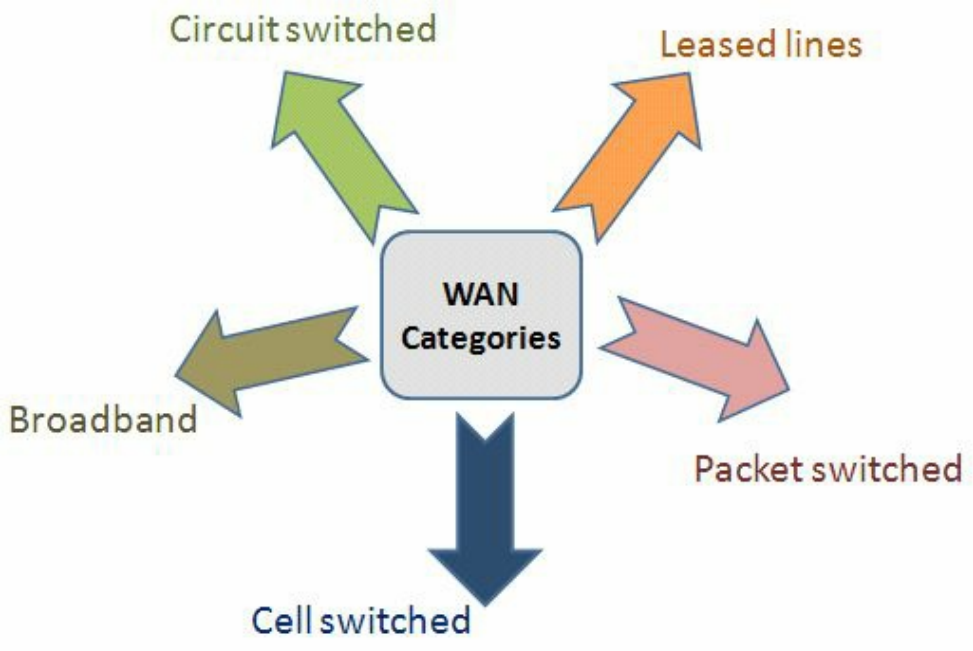


Figure 41.1 – WAN Categories

As detailed in Figure 41.1 above, there are many options when discussing WAN categories and this is just a general introduction to them. All of these technologies can support the needs of modern networks that operate under the 20/80 design rule, meaning 80% of the network traffic uses some kind of WAN technology in order to access remote resources.

NBMA Technologies

https://t.me/tanmiogrets

A special technology that appears in wide area networking is Non-Broadcast Multi-Access (NBMA). This presents some challenges that are not present in traditional broadcast networking. The need for NBMA arises when there is no native Broadcast support for a group of systems that want to communicate over the same network. Issues arise when the devices cannot natively send a packet destined for all the devices on the Multi-Access segment. Frame Relay, ATM, and ISDN are examples of technologies that are NBMA by default.

All of these technologies do not have any native ability to support Broadcasts. This prevents them from running routing protocols that use Broadcasts in their operation. Native Multicast support is also missing in Non-Broadcast networks. In the case of a routing protocol, all the nodes that participate must receive Multicast updates. One approach to this using an NBMA network is sending the Multicast or Broadcast packets as replicated Unicast packets. In this way, the Broadcast/Multicast frames are individually sent to every node in the topology. The tricky part in this scenario is that the device has to come up with a way to solve the Layer 3 to Layer 2 resolution. Particular packets have to be addressed for the specific machines that need to receive them.

Methodologies must exist for addressing this Layer 3 to Layer 2 resolution issue. The Layer 3 address is typically the IP address and the Layer 2 address usually varies, based on the technology used. In the case of Frame Relay, this will consist of the Data Link Connection Identifier (DLCI) number, so a way to resolve the DLCI to the IP address must be found.

In the case of Broadcast networks, Layer 3 resolution uses MAC addresses as the Layer 2 address and this has to be resolved to IPv4 addresses. This is accomplished with the Address Resolution Protocol (ARP). In a Broadcast-based network, the devices broadcast the requests by specifying the devices it wants to communicate with (typically learned via DNS) and asking for the MAC addresses specific to those devices. The reply is via Unicast and includes the requested MAC address.

In NBMA environments you still need to bind the Layer 3 address (IP address) to the Layer 2 address (DLCI). This can be done in an automated fashion using Inverse ARP. This is used to resolve the remote Layer 3 address to a Layer 2 address and is only used locally. Inverse ARP can be utilised in Frame Relay environments. The issue with Inverse ARP as the solution for the Layer 3 to Layer 2 resolution in an NBMA environment is that it is limited to directly connected devices. This creates issues in partial-mesh NBMA networks (where not all devices are directly connected).

Two types of NBMA interfaces exist – Mulitipoint and Point-to-Point, as illustrated in Figure 41.2 below . Multipoint interfaces require some kind of Layer 3 to Layer 2 resolution methodology. As its name implies, it can be the termination point of multiple Layer 2 circuits.

https://t.me/learningnets

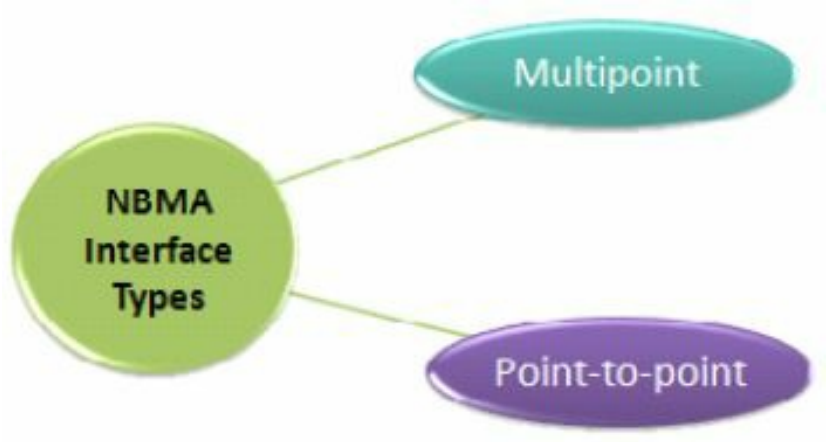


Figure 41.2 – NBMA Interface Types

If Frame Relay is configured on the main physical interface of a device, that interface will be Multipoint by default. If a subinterface is created on a Frame Relay physical interface, the option of creating it as Multipoint exists. Layer 3 to Layer 2 resolution has to be configured for both the physical interfaces and for the subinterfaces. There are two options for doing this in Frame Relay:

- Inverse ARP
- Statically map

Layer 3 to Layer 2 resolution is not always an issue on NBMA interfaces because Point-to-Point WAN interfaces can be created. A Point-to-Point interface can only terminate a single Layer 2 circuit, so if the interface communicates with only one device, Layer 3 to Layer 2 resolution is not necessary. With only one circuit, there is only one Layer 2 address to communicate with. Layer 3 to Layer 2 resolution issues disappear when running a Frame Relay Point-to-Point subinterface type or an ATM Point-to-Point subinterface, for example.

WAN Components

WAN requires a number of physical components to enable a connection. These will differ depending upon the type of connection you are using (e.g., ISDN, ADSL, Frame Relay, leased line, etc.) and other factors, such as back-up connections and the number of incoming networks.

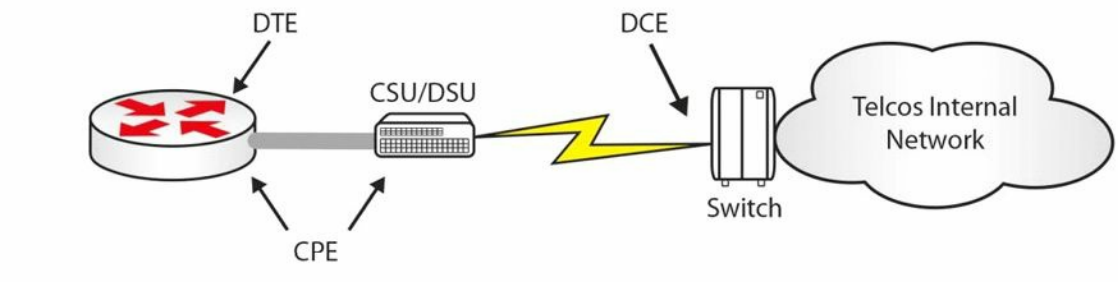


Figure 41.3 – Basic WAN Components

Figure 41.3 above shows a basic serial connection going out to an ISP. As the customer, you are responsible for the Data Terminal Equipment (DTE), which is your router interface accepting the incoming link. You will also be responsible for the cable going to your Channel Service

https://t.me/learningnets

Unit/Data Service Unit (CSU/DSU), which converts your data into a format that your ISP can transport. The CSU/DSU is usually built into your router WAN interface card (WIC). CPE is the Customer Premise Equipment, which is your responsibility.

From this point on, your ISP or Telco is usually responsible for the connection. They lay the cables and provide switching stations, which transport the data across their network. The ISP owns the Data Communication Equipment (DCE), which is the end that provides the clocking, meaning the rate at which the data can pass on the line.

Common types of WAN connections include the following:

- Leased-line – a dedicated connection available 24/7
- Circuit-switching – set up when required
- Packet-switching – shared link/virtual circuit

The type of link you buy depends on your requirements and budget. If you can afford a dedicated line, you will have exclusive use of the bandwidth and security is less of an issue. A shared connection can mean a slower connection during peak times.

WAN Protocols

Common WAN protocols include PPP, HDLC, and Frame Relay. There are many others, of course, but you need to focus on those included in the CCNA syllabus.

Point-to-Point Protocol (PPP) can be used when you have a Cisco device connecting to a non-Cisco device. PPP also has the advantage of including authentication. It can be used over a number of connection types, including DSL, circuit-switched, and asynchronous/synchronous connections.

Cisco's High-Level Data Link Control (cHDLC) is its implementation of the open standard version of HDLC. HDLC requires DTE and DCE and is the default encapsulation type on Cisco routers (serial interfaces). Keepalives are sent from the DCE in order to check link status.

As already discussed, Frame Relay is a packet-switching technology which has become less popular in recent years, as DSL has become both more affordable and more readily available. It works at speeds from 56Kbps to 2Mbps and builds virtual circuits every time a connection is required. There is no security built into Frame Relay (but see Farai's comment below). Frame Relay will be covered in more detail later.

> Farai says – "Frame Relay commonly uses Permanent Virtual Circuits (PVCs), which are always present, although it can use Switched Virtual Circuits (SVCs), which are created on demand. A PVC is a type of Virtual Private Network (VPN). However, some people run PPP over Frame Relay (PPPoFR) to allow for PPP security for Frame Relay connections."

Metro Ethernet

Metro Ethernet technologies involve the use of carrier Ethernet in Metropolitan Area Networks (MANs). Metro Ethernet can connect company LANs and individual end-users to a WAN or to the Internet. Companies often use Metro Ethernet to connect branch offices to an intranet.

https://t.me/learningnets

A typical Metro Ethernet deployment uses a star or a mesh topology with interconnected network nodes using copper or fibre optic cables. Using the standard and widely deployed Ethernet technology in Metro Ethernet deployments offers a number of advantages, as opposed to using SONET/SDH or MPLS technologies:

- Less expensive
- Easier to implement
- Easier to manage
- Easy to connect customer equipment because it uses the standard Ethernet approach

A typical MAN can be structured under the access/aggregation/core standard design (a Cisco design model), as follows:

- Access Layer – usually at the customer's premises. This may include an office router or residential gateway
- Aggregation Layer – usually comprises microwave, DSL technologies, or Point-to-Point Ethernet links.
- Core Layer – may use MPLS to interconnect different MANs

Customer traffic separation is usually ensured in a MAN by using Ethernet VLAN tags that allow the differentiation of packets.

VSAT

Very Small Aperture Terminal (VSAT) technology is a telecommunication system based on wireless satellite technology. A VSAT deployment is made up of a small satellite earth station and a typical antenna, as shown in Figure 41.4 below:

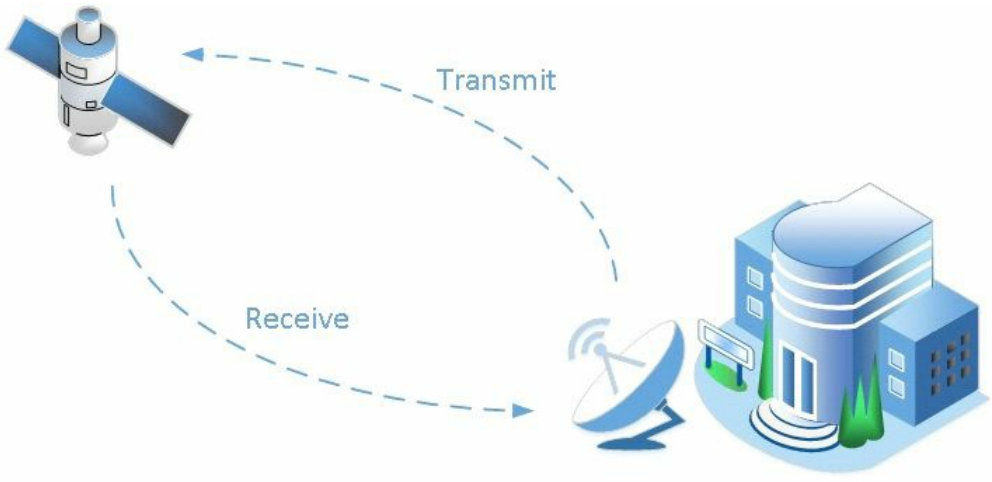


Figure 41.4 – Satellite Communication

Typical VSAT components include the following:

- Master earth station
- Remote earth station
- Satellite

https://t.me/learningnets

The master earth station is the network control centre for the entire VSAT network. This is the place where the configuration, management, and monitoring of the entire network is done.

The remote earth station is the hardware installed at the customer premises and includes the following components:

- ODU (outdoor unit)
- IDU (indoor unit)
- IFL (interfacility link)

The VSAT satellite orbits round the globe and receives and transmits signals from and to the earth stations.

VSAT networks can be configured in one of the following topologies:

- Star topology
- Mesh topology
- Star-mesh combination

Using satellite technology to ensure WAN connectivity is generally more expensive than using a traditional terrestrial network connection. The speeds offered by such connections can reach 5Mbps download and 1Mbps upload, which is usually enough for remote sites.

A significant disadvantage of using satellite connectivity is the increased traffic latency, which can reach up to 250 ms one way (antenna to satellite or satellite to antenna) due to the use of radio signals over a very long distance. This should be carefully analysed when planning to install a satellite WAN connection because the increased latency could prevent sensible applications from functioning, while it has no impact on other applications.

Another challenge of using satellite connectivity is that the satellite dish has to have line of sight to the satellite. This means that you have to make use of high frequency ranges (2 GHz), and any type of interference (e.g., natural phenomena like rain or storm clouds) may affect the connection throughput and availability.

T1/E1

Standards for T1 and E1 wide area networking have been around for a very long time. T1 stands for T-Carrier Level 1, which is a line that uses Time Division Multiplexing with digital signals associated with different channels based on time. T1 operates using 24 separate channels at a 1.544Mbps line rate, thus allocating 64Kbps per individual channel. You can use the 24 channels any way you want to, and you can even buy just a few channels from the service provider based on your needs. In general terms, consider a T1 connection as a trunk/bundle carrying 24 separate lines. T1 is a standard often used in the following geographical regions:

- North America
- Japan
- South Korea

https://t.me/learningnets

E1 (E-Carrier Level 1) is a standard similar to T1 but it is used exclusively in Europe. The main difference between E1 and T1 is that E1 uses 32 channels instead of 24, also operating at 64kbps, thus offering a total line rate of 2.048Mbps. E1 functions based on Time Division Multiplexing, just like T1, so all other functionalities are common between the two standards.

T3/E3

T3 and E3 standards offer higher bandwidth than their T1 and E1 predecessors. T3 stands for T-Carrier Level 3 and is a type of connection usually based on coaxial cable and a BNC connector. This differs from T1, which is usually offered over twisted-pair media.

T3 connections are often referred to as DS3 connections, which is related to the data carried on the T3 line. T3 offers additional throughput because it uses the equivalent of 28 T1 circuits, meaning 672 T1 channels. This offers a total line rate of 44.736Mbps.

E3 connections are similar to those of T3, with the exception of being equivalent to 16 E1 circuits, meaning 512 E1 channels and a total line rate of 33.368Mbps.

T3/E3 connections are usually used in large data centres because they offer the ability to increase the total amount of throughput when needed.

ISDN

Integrated Services Digital Network (ISDN) is a technology that allows digital communication over a traditional analog phone line, so both voice and data can be digitally transmitted over the PSTN. ISDN never had the popularity that it was expected to have because it came along at a time when other alternative technologies were developed.

There are two flavours of ISDN:

- ISDN BRI (Basic Rate Interface)
- ISDN PRI (Primary Rate Interface)

The ISDN-speaking devices are called terminal emulation equipment and the devices can be categorised into native ISDN and non-native ISDN equipment. The native ISDN equipment is made up of devices that were built to be ISDN-ready and are called TE1 devices (Terminal Equipment 1). Non-native ISDN equipment is made up of TE2 devices. Non-native ISDN equipment can be integrated with native ISDN equipment by using special Terminal Adapters (TAs), meaning only TE2 devices require TA modules.

Moving towards the ISDN provider, you will find Network Termination 2 (NT2) devices and Network Termination 1 (NT1) devices. These are translation devices for media, transforming five-wire connections into two-wire connections (the local loop). The local loop is the user connection line and it is a two-wire link.

An interesting thing about the network termination devices is that in North America the customer is responsible for NT1 devices, while in other parts of the world this is the service provider's responsibility. Because of this issue, some Cisco routers provide built-in NT1 functionality and they will feature a visible "U" under the port number so that the user can quickly see this capability. The "U" notation comes from the ISDN reference points terminology

https://t.me/learningnets

that describes where you might have a problem in the ISDN infrastructure, as shown in Figure 41.5 below:

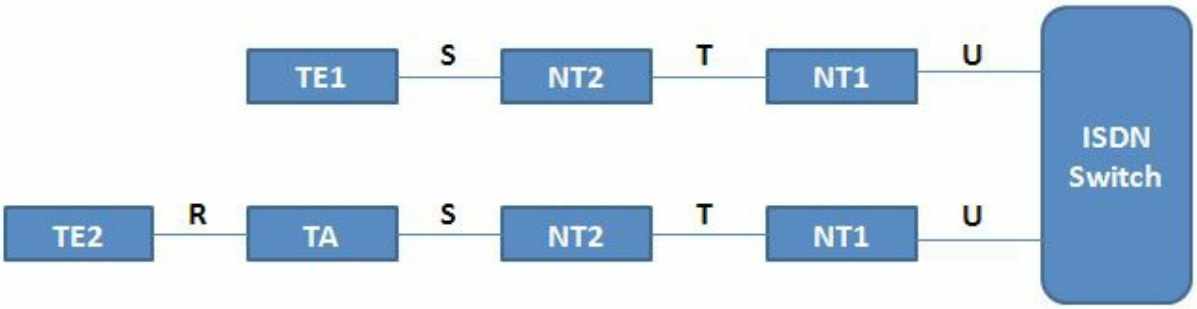


Figure 41.5 – ISDN Reference Points

These reference points are important during the troubleshooting or maintaining process of an ISDN network. The ISDN switch is usually located at the service provider location. The different ISDN reference points are as follows:

- U reference point – between the ISDN switch and the NT1 device
- T reference point – between the NT2 and the NT1 devices
- S reference point – between terminals (TE1 or TA) and NT2 devices
- R reference point – between non-ISDN native devices and TAs

The ISDN Basic Rate Interface (BRI) connectivity contains two B (bearer) channels for carrying data and one D (delta) channel for signaling. The BRI connection is abbreviated as 2B+D to remind you about the number of channels each provides. Each of the bearer channels in ISDN will operate at a speed of 64Kbps. Multilink PPP can be configured on top of these interfaces to allow the user to reach a bandwidth of 128Kbps. This bandwidth is considered to be very low according to modern networks requirements.

The delta (D) channel in BRI ISDN is dedicated to 16Kbps for control traffic. There are also 48Kbps overall for framing control and other overhead in the ISDN environment, meaning the total ISDN bandwidth for BRI is 192Kbps (128Kbps from the B channels + 16Kbps from the D channel + 48Kbps overhead).

ISDN Primary Rate Interface (PRI) has 23 B channels and one D channel in the US and Japan. The bearer channels and the delta channels all support 64Kbps. If you include the overhead, the total PRI bandwidth is 1.544Mbps. In other parts of the world (i.e., Europe and Australia) the PRI connection contains 30 B channels and one D channel.

ISDN PRI connections are commonly used as connectivity from the PSTN to large phone systems (PBX). Each of the 23 or 30 B channels can be used as a single phone line, so the entire PRI connection can be considered a trunk that carries multiple lines. The main advantage of using a PRI connection instead of multiple individual lines is that it is easier to manage and it offers scalability.

The technologies described above are called Time Division Multiplexing (TDM) technologies. TDM refers to being able to combine multiple channels over a single overall transmission medium and using these different channels for voice, video, and data. Time division refers to

https://t.me/learningnets

splitting the connection into small windows of time for the various communication channels.

In a PSTN, you need to be able to transmit multiple calls along the same transmission medium, so TDM is used to achieve this goal. TDM actually started in the days of the telegraph and later on gained popularity with fax machines and other devices that use TDM technologies.

When you have leased lines (buying dedicated bandwidth), the circuits that are sold are measured in terms of bandwidth. A DS1 or T1 circuit in North America provides 24 time slots of 64Kbps each and a 9Kbps control time slot (for a total of 1.544Mbps, as mentioned earlier). TDM terminology is tightly connected with the leased-line purchasing process.

DSL

Digital Subscriber Line (DSL) is used as an alternative to ISDN for home users. There are a number of types of DSL connections, but the most important ones include the following:

- ☐ ADSL
- ☐ HDSL
- ☐ VDSL
- ☐ SDSL

Asymmetric Digital Subscriber Line (ADSL) is the most common form of DSL connection that functions over standard telephone lines. The reason it is called asymmetric is that it offers unequal download and upload throughput, with the download rate being higher than the upload rate. A standard ADSL connection usually offers a maximum of 24Mbps download throughput and a maximum of 3.5Mbps upload throughput over a distance of up to 3 km.

With ADSL the customer connects to a Digital Subscriber Line Access Multiplexer (DSLAM) located at the service provider. DSLAM is a DSL concentrator device that aggregates connections from multiple users.

NOTE: One of the issues with ADSL is the limited distance a subscriber can be from a DSLAM.

High Bitrate DSL (HDSL) and Very High Bitrate DSL (VDSL) are other DSL technologies used on a large scale that offer increased throughput when compared to ADSL. VDSL can operate at rates of up to 100Mbps.

Symmetric DSL (SDSL) offers the same download and upload throughput, but it was never standardised or used on a large scale.

Cable

Digital signals can also be received by home users over standard TV cable connections. Internet access can be provided over cable by using the Data Over Cable Service Interface Specification (DOCSIS) standard. This is usually a low-cost service, as the provider does not need to install a new infrastructure for the data services. The only upgrade to the existing network is the installation of a low-cost cable modem in the customer premises that usually offers RJ45 data

https://t.me/learningnets

connectivity for the user devices.

Data traffic transmission rates over cable technology can go up to 100Mbps, which is more than enough for home users and even small businesses.

NOTE: Besides TV and data signals, cable connection can also carry voice traffic.

Point-to-Point Protocol over Ethernet (PPPoE) is another technology that can be used in conjunction with cable. This can be used between the cable modem and the endpoint devices to add security to the cable modem infrastructure. This allows the user to log on and provide a username and a password that has to be authenticated in order for the cable service to be used. The credentials are carried across the Ethernet connection to the cable modem and beyond by using the PPP running over the Ethernet. We will cover PPPoE shortly.

Cellular Networks

Cellular networks are used in conjunction with mobile devices (e.g., cell phones, tablets, PDAs etc.) to send and receive data traffic with classic voice service. These networks cover large geographical areas by splitting them into cells. Antennas are strategically placed to ensure optimal coverage across these cells and seamless cell roaming for users going from one location to another. The traditional connectivity type is also called 2G and includes the following:

- GSM (Global System for Mobile Communications)
- CDMA (Code Division Multiple Access)

Depending upon the carrier you use and the country you live in, you might use a GSM or CDMA type of communication, although functionally they are often referred to as 2G networks. These networks were designed as analog connections using circuit switching and were not originally designed to send data. Because the data connections use a packet-switching technology, 2G connections offer limited data transmission support.

Newer connection types over cellular networks that allow full-featured packet switching and proper data transmission include the following:

- HSPA+ (High Speed Packet Access)
- LTE (Long Term Evolution)

LTE and HSPA+ are standards created by the 3rd Generation Partnership Project (3GPP), which is a collaboration between a number of telecommunications companies that decided they needed a standardised way to send data on cellular networks.

HSPA+ is a standard based on CDMA that offers download rates up to 84Mbps and upload rates of up to 22Mbps. LTE is a standard based on GSM/EDGE that offers download rates up to 300Mbps and upload rates up to 75Mbps.

NOTE Each of these standards continues to develop, so the throughput rates might increase in the future.

https://t.me/learningnets

GSM 3G (third generation) is a general term that describes networks with a capability of offering transmission rates of up to several Mbps. This can be achieved by increasing the channels' allocated bandwidth, along with using packet-switching technology.

GSM 4G (fourth generation) is the latest addition to the GSM portfolio and it is still under implementation in most countries. 4G offers transmission rates that exceed 100Mbps, which are suitable for high-speed broadband Internet access. GSM 4G is based exclusively on IP communication, as the spread spectrum radio technology used in 3G networks is replaced by ODFMA multi-carrier transmission that can assure high transmission rates.

VPN Technologies

VPN is a technology that overlays communications networks and gives them the security and manageability required by businesses. With VPN technology, you can set up secure relationships, automated connections, authorisations, and encryption, while still enjoying the low cost and availability of the Internet.

VPNs protect data while in transit across the Internet, or within a company's enclave. The VPN has many capabilities, but the primary functions include the following:

- Keep data confidential (encryption)
- Ensure the identities of two parties communicating (authentication)
- Safeguard the identities of communicating parties (tunnelling)
- Ensure data is accurate and in its original form (non-repudiation)
- Guard against packets being sent over and over (replay prevention)

Even though the VPN concept implies security most of the time, unsecured VPNs also exist. Frame Relay is an example of this, as it provides private communications between two locations but it might not have any security features on top of it. Whether you should add security to the VPN connection depends upon the specific requirements for that connection.

VPN troubleshooting is difficult to manage because of the lack of visibility in the service provider infrastructure. The service provider is usually seen as a cloud that aggregates all the network locations' connections. When performing VPN troubleshooting, you should first make sure that the problem does not reside on your devices and only then should you contact your service provider.

There are many types of VPN technologies, including the following:

- Site-to-Site VPNs, or Intranet VPNs, for example Overlay VPNs (like Frame Relay) or Peer-to-Peer VPNs (like MPLS). You would use these when you want to connect different locations over the public infrastructure. When using a peer-to-peer infrastructure, you can seamlessly communicate between your sites without worrying about IP addressing overlap.
- Remote Access VPNs, for example Virtual Private Dial-up Network (VPDN), which is a dial-up approach for the VPN that is usually done with security in mind.

https://timelearningnets

- Extranet VPNs, when you want to connect to business partners or customer networks.

When you use VPNs, you are often tunnelling traffic in order to send it over an infrastructure. One tunnelling methodology for Layer 3 is called Generic Routing Encapsulation (GRE). GRE allows you to tunnel traffic but it does not provide security. In order to tunnel traffic and also provide security, you can use a technology called IP Security (IPSec). This is a mandatory implementation component of IPv6 but it is not a requirement for IPv4. IPSec is also used in conjunction with Authentication, Authorization, and Accounting (AAA) services, which allows tracking of user activity.

The main benefits of VPNs include the following:

- Scalability (you can continuously add more sites to the VPN)
- Flexibility (you can use very flexible technologies like MPLS)
- Cost (you can tunnel traffic through the Internet without much expense)

MPLS

Multiprotocol Label Switching (MPLS) functions by appending a label to any type of packet. The packet is then forwarded through the network infrastructure based on this label value, instead of any Layer 3 information. The labeling of the packet provides very efficient forwarding and allows MPLS to work with a wide range of underlying technologies. By simply adding a label in the packet header, MPLS can be used in many Physical and Data Link Layer WAN implementations.

The MPLS label is positioned between the Layer 2 header and the Layer 3 header. By using MPLS, overhead is added only when the packet enters the service provider cloud. After entering the MPLS network, packet switching is done much faster than in traditional Layer 3 networks because it is based only on swapping the MPLS label, instead of stripping the entire Layer 3 header.

MPLS comes in two different flavours:

- Frame Mode MPLS
- Cell Mode MPLS

Frame Mode MPLS is the most popular MPLS type, and in this scenario the label is placed between the Layer 2 header and Layer 3 header (for this reason MPLS is often considered a Layer 2.5 technology). Cell Mode MPLS is used in ATM networks and uses fields in the ATM header that are used as the label.

MPLS-capable routers are also called Label Switched Routers (LSRs), and these routers come in two flavours:

- Edge LSR (PE routers)
- LSR (P routers)

PE routers are Provider Edge devices that take care of label distribution; they forward packets

https://t.me/learningnets

based on labels and they are responsible for label insertion and removal. P routers are Provider routers and their responsibility consists of label forwarding and efficient packet forwarding based on labels.

Basic Serial Line Configuration

If you don't want to change the default HDLC encapsulation, then, in order to set up your WAN connection, you need only to do the following:

1. Add an IP address to your interface
2. Bring the interface up (with the `no shut` command)
3. Ensure there is a clock rate on the DCE side

Here is the configuration if you have the DCE cable attached:

```
Router#config t
Router(config)#interface Serial0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
Router(config-if)#^Z
Router#
```

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol used to encapsulate PPP frames inside Ethernet frames.

As customers deploy ADSL, they must support PPP-style authentication and authorisation over a large installed base of legacy bridging customer premises equipment (CPE). PPPoE provides the ability to connect a network of hosts over a simple bridging access device to a remote access concentrator or aggregation concentrator. With this model, each host uses its own PPP stack, thus presenting the user with a familiar user interface. Access control, billing, and type of service can be done on a per-user, rather than a per-site, basis.

As specified in RFC 2516, PPPoE has two distinct stages: a discovery stage and a session stage. When a host initiates a PPPoE session, it must first perform discovery to identify which server can meet the client's request, and then identify the Ethernet MAC address of the peer and establish a PPPoE session ID. While PPP defines a peer-to-peer relationship, discovery is inherently a client-server relationship.

PPPoE Configuration

The following sections cover server (ISP premises) and client PPPoE configurations. I've included them because the CCNA syllabus now mandates that you know how to configure PPPoE!

Server Configuration

The first step in creating the PPPoE server configuration is to define a BBA (broadband aggregation) group which will manage the incoming connections. This BBA group must be associated to a virtual template:

https://t.me/learningnets

```
Router(config)#bba-group pppoe GROUP
```

```
Router(config-bba-group)#virtual-template 1
```

The next step is to create a virtual template for the customer-facing interface. On the virtual template you need to configure an IP address and a pool of addresses from which clients are assigned a negotiated address:

```
Router(config)#interface virtual-template 1
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#peer default ip address pool POOL
```

The IP pool is defined in global configuration mode. This is similar to a DHCP pool configuration:

```
Router(config)#ip local pool POOL 10.10.10.2 10.10.10.254
```

The final step is to enable the PPPoE group on the customer-facing interface:

```
Router(config)#interface FastEthernet0/0
Router(config-if)#no ip address
Router(config-if)#pppoe enable group GROUP
Router(config-if)#no shutdown
```

Client Configuration

On the client side a dialer interface has to be created. This will manage the PPPoE connection. The dialer interface can be assigned a manual IP address or can be instructed to request one from the server (using the `ip address negotiated` command):

```
Router(config)#interface dialer1
Router(config-if)#dialer pool 1
Router(config-if)#encapsulation ppp
Router(config-if)#ip address negotiated
Router(config)#interface FastEthernet0/0
Router(config-if)#no ip address
Router(config-if)#pppoe-client dial-pool-number 1
Router(config-if)#no shutdown
```

Authentication

In order to secure the PPPoE connection, you can use two methods:

- PAP (Password Authentication Protocol) – insecure, sends the credentials (both username and password) in plain text
- CHAP (Challenge Handshake Authentication Protocol) – secure (clear text username and MD5 hashed password), the preferred method

PAP can be configured as follows:

```
Server(config)#username Client password Password
Server(config)#interface virtual-template 1
Server(config-if)#ppp authentication pap
Server(config-if)#ppp pap sent-username Server password Password
```

https://t.me/learningnets

```
Client(config)#username Server password Password
Client(config)#interface dialer 1
Client(config-if)#ppp authentication pap
Client(config-if)#ppp pap sent-username Client password Password
```

CHAP can be configured as follows:

```
Server(config)#username Client password Password
Server(config)#interface virtual-template 1
Server(config-if)#ppp authentication chap
Client(config)#username Server password Password
Client(config)#interface dialer 1
Client(config-if)#ppp authentication chap
```

PPPoE Verification and Troubleshooting

The following message appears on the client console after the PPPoE session has successfully formed:

```
%DIALER-6-BIND: Interface Vi1 bound to profile Di1
%LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
```

The following command can be used on the client router to verify the dialer interface obtained (negotiated) and the IP address from the PPPoE server:

```
Router#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Virtual-Access1            unassigned      YES unset  up/up
Dialer1                    10.10.10.2      YES IPCP   up/up
```

The following command can be used on the client router to show the PPPoE session status:

```
Router#show pppoe session
1 client session
Uniq ID  PPPoE  RemMAC      Port       Source   VA         State
       SID  LocMAC                             VA-st
N/A     16  ca00.4843.0008  Fa0/0      Di1      Vi1        UP
            ca01.4843.0008                               UP
```

Useful troubleshooting commands for PPPoE connections are as follows:

```
Router#debug ppp ?
  authentication  CHAP and PAP authentication
  bap             BAP protocol transactions
  cbcp            Callback Control Protocol negotiation
  elog            PPP ELOGs
  error           Protocol errors and error statistics
  forwarding      PPP layer 2 forwarding
  mppe            MPPE Events
```

https://t.me/learningnets

```
  multilink       Multilink activity
  negotiation     Protocol parameter negotiation
  packet          Low-level PPP packet dump
```

Troubleshooting WAN Connections

When trying to bring up a WAN connection (forgetting PPP and Frame Relay for the moment), you could use the OSI model:

Layer 1 – Check the cable to ensure that it is attached correctly. Has the `no shut` command been applied? Is there a clock rate applied to the DCE side?

```
RouterA#show controllers serial 0
HD unit 0, idb = 0x1AE828, driver structure at 0x1B4BA0
buffer size 1524 HD unit 0, V.35 DTE cable
```

```
RouterA#show ip interface brief
Interface     IP-Address     OK? Method Status                Protocol
Serial0       11.0.0.1       YES unset  administratively down down
Ethernet0     10.0.0.1       YES unset  up                    up
```

Layer 2 – Check to ensure that the correct encapsulation is applied to the interface. Ensure that the other side of the link has the same encapsulation type.

```
RouterB#show interface Serial0
Serial1 is down, line protocol is down
Hardware is HD64570
Internet address is 12.0.0.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

Layer 3 – Is the IP address and subnet mask correct? Does the subnet mask match the other side?

```
RouterB#show interface Serial0
Serial1 is down, line protocol is down
Hardware is HD64570
Internet address is 12.0.0.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

https://t.me/learningnets

Day 41 Questions

1. Name at least three WAN categories.
2. The need for NBMA appears when there is no native _____ support for a group of systems that want to communicate over the same network.
3. In NBMA environments you still need to bind the Layer 3 address (IP address) to the Layer 2 address (DLCI). This can be done in an automated fashion, using a technology called Inverse ARP. True or false?
4. Name 2 NBMA interface types.
5. _____ requires DTE and DCE and is the default encapsulation type on Cisco routers.
6. _____ technologies involve the use of carrier Ethernet in Metropolitan Area Networks (MANs).
7. T1 is a standard often used in what geographical regions?
8. What are the two flavours of ISDN?
9. _____ is the most common form of DSL connection that functions over standard telephone lines. It offers unequal download and upload throughput, with the download rate being higher than the upload rate.
10. _____ functions by appending a label to any type of packet.

https://t.me/learningnets

Day 41 Answers

1. Circuit-switched, cell-switched, broadband, leased-line, and packet-switched.
2. Broadcast.
3. True.
4. Multipoint and Point-to-Point.
5. HDLC.
6. Metro Ethernet.
7. North America, Japan, and South Korea.
8. BRI and PRI.
9. ADSL.
10. MPLS.

https://t.me/learningnets

Day 41 Lab

PPPoE Lab

Configure PPPoE with CHAP authentication between two routers as per the information presented in this module:

Server configuration:

```
Router(config)#bba-group pppoe GROUP
Router(config-bba-group)#virtual-template 1
Router(config)#interface virtual-template 1
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#peer default ip address pool POOL
Router(config)#ip local pool POOL 10.10.10.2 10.10.10.254
Router(config)#interface FastEthernet0/0
Router(config-if)#no ip address
Router(config-if)#pppoe enable group GROUP
Router(config-if)#no shutdown
```

Client configuration:

```
Router(config)#interface dialer1
Router(config-if)#dialer pool 1
Router(config-if)#encapsulation ppp
Router(config-if)#ip address negotiated
Router(config)#interface FastEthernet0/0
Router(config-if)#no ip address
Router(config-if)#pppoe-client dial-pool-number 1
Router(config-if)#no shutdown
```

CHAP Authentication:

```
Server(config)#username Client password Password
Server(config)#interface virtual-template 1
Server(config-if)#ppp authentication chap
Client(config)#username Server password Password
Client(config)#interface dialer 1
Client(config-if)#ppp authentication chap
```

Verify the configuration:

```
Router#show pppoe session
1 client session
Uniq ID  PPPoE  RemMAC      Port       Source   VA         State
       SID  LocMAC                             VA-st
N/A     16  ca00.4843.0008  Fa0/0       Di1     Vi1        UP
N/A     16  ca01.4843.0008                                 UP
```

https://t.me/learningnets

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 42 – Frame Relay and PPP

Day 42 Tasks

- Read today's lesson notes (below)
- Review yesterday's lesson notes
- Complete today's lab
- Read the ICND2 cram guide
- Spend 15 minutes on the subnetting.org website

Frame Relay was an important part of the CCNA to CCIE syllabus for several years; however, its popularity has waned recently due to the wide availability of DSL connections for businesses and the price of leased lines becoming more affordable. We cover it here because it is included in the CCNA syllabus. PPP is still widely used.

Today you will learn about the following:

- Frame Relay operations
- Configuring Frame Relay
- Troubleshooting Frame Relay
- PPP operations
- Configuring PPP
- Troubleshooting PPP

This lesson maps to the following CCNA syllabus requirements:

- Identify different WAN technologies
    - Frame Relay
- Configure and verify a PPP connection between Cisco routers

Frame Relay Operations

Frame Relay is a Layer 2 WAN protocol based on an older protocol called X.25, which is still used by ATMs due to its extensive error-checking capabilities. Frame Relay is comprised of one physical circuit upon which many logical circuits can form. Connections are made on an as-needed basis. An example of a Frame Relay network is illustrated below:

https://t.me/learningnets

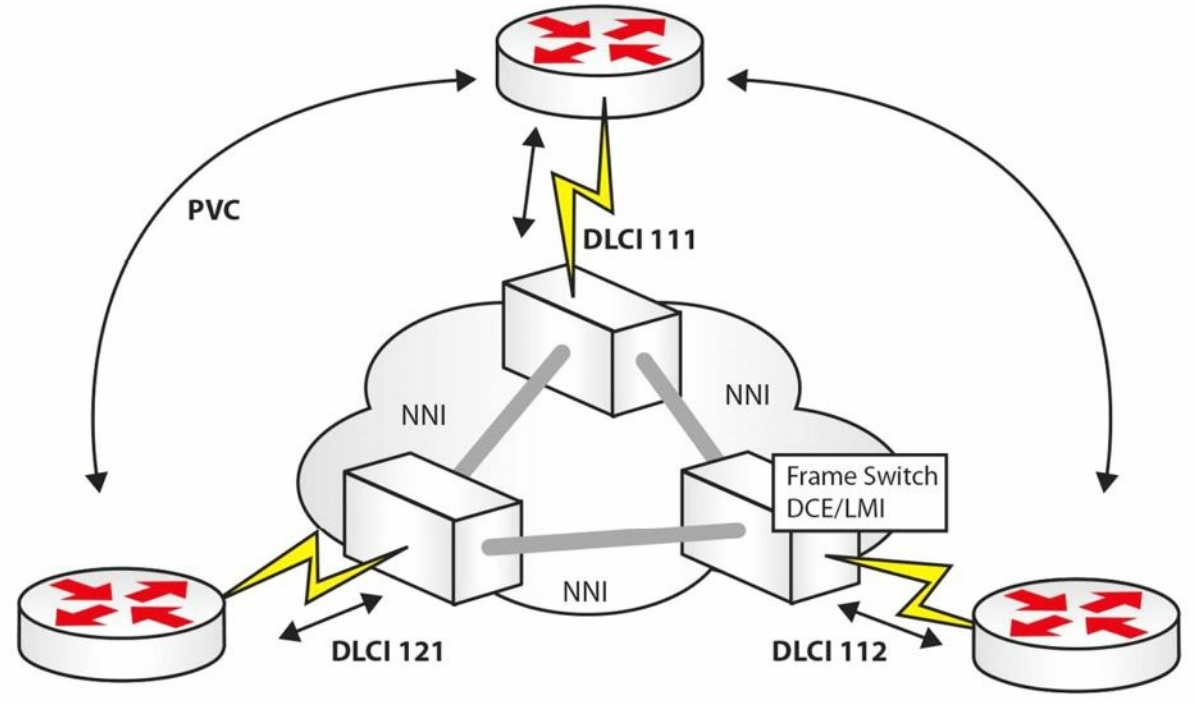


Figure 42.1 – A Frame Relay Network

Common Frame Relay Terms

LMI

Local Management Interface (LMI) is a keepalive which runs from the Frame Relay switch. This switch belongs to your service provider and is located at their premises. You will need to specify the LMI type on your router, unless the CISCO default is used. The three types of LMIs available are as follows:

- CISCO
- ANSI
- Q933a

LMIs are illustrated in Figure 42.2 below:

https://t.me/learningnets

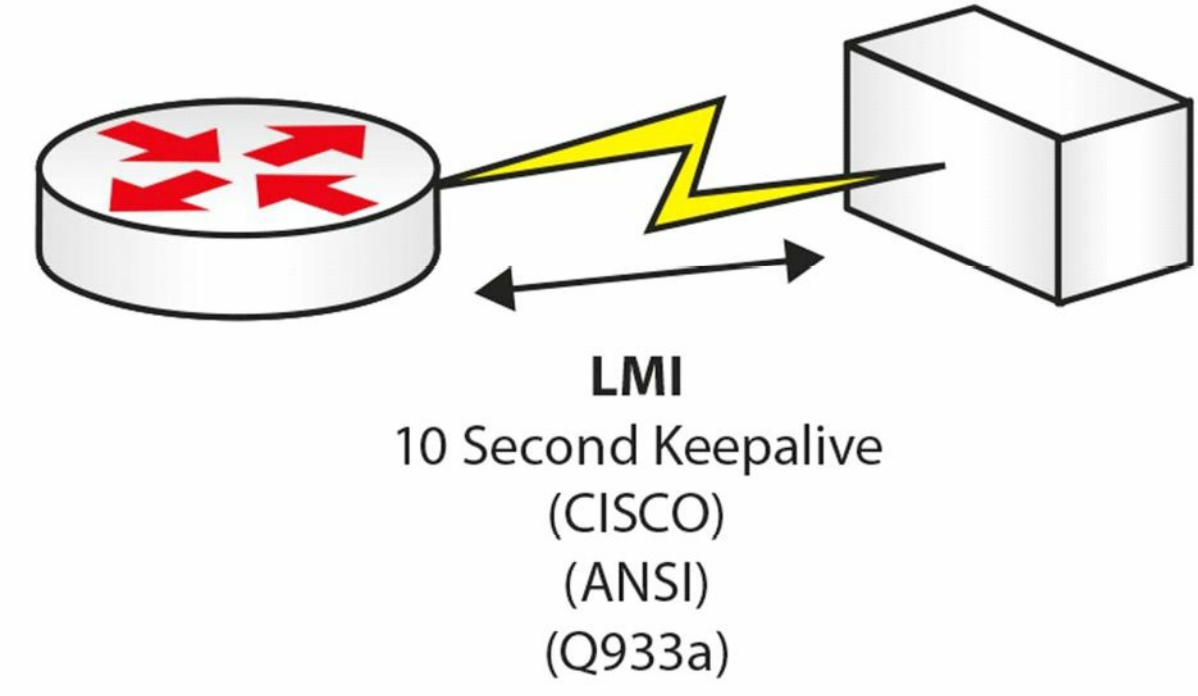


Figure 42.2 – LMI Types

If you have a fault with your Frame Relay connection, then debugging the LMI messages would be one of your troubleshooting steps, as illustrated in the output below:

```
RouterA#debug frame-relay lmi

00:46:58: Serial0(in): Status, myseq 55
00:46:58: RT IE 1, length 1, type 0
00:46:58: KA IE 3, length 2, yourseq 55, myseq 55
00:46:58: PVC IE 0x7 , length 0x6 , dlci 100, status 0x2 , bw 0
```

An LMI is sent every 10 seconds, and every sixth message is a full status update. As above, you want it to report `status 0x2`, which is an active link.

PVC

A Permanent Virtual Circuit (PVC) is the logical end-to-end connection formed from one end of your Frame Relay network to the other, as illustrated in Figure 42.3 below. Each endpoint is given a DLCI number (see the next section) to identify it.

https://t.me/learningnets

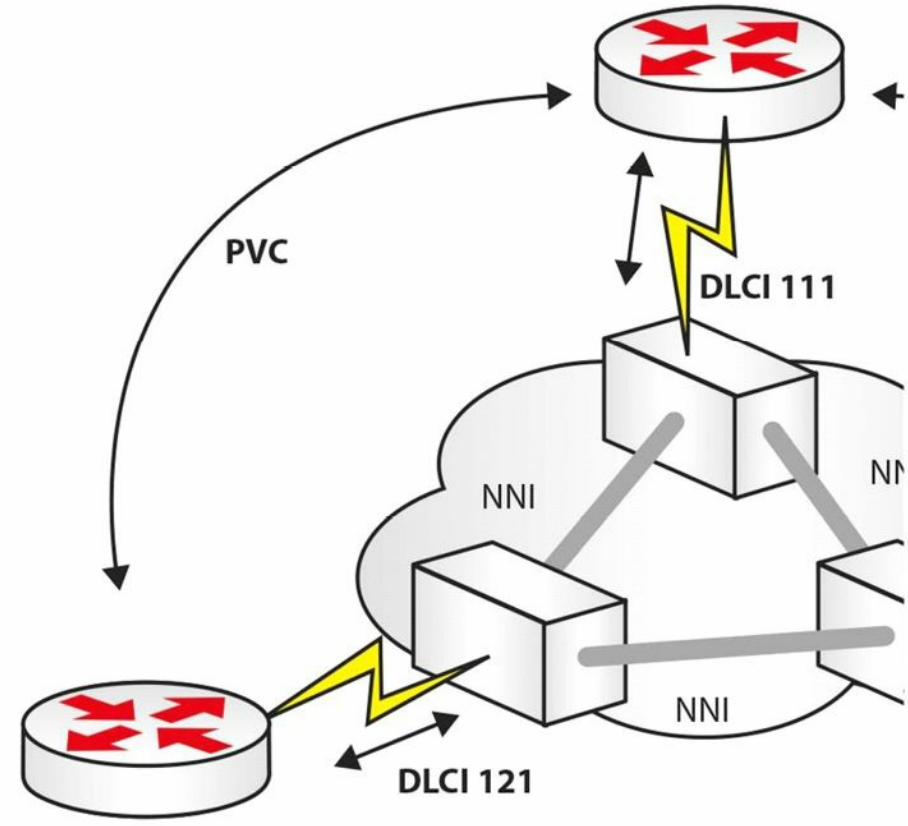


Figure 42.3 – A PVC

DLCI

The Data Link Connection Identifier (DLCI) is a locally significant number used to identify your connection to the Frame Relay switch, as illustrated in Figure 42.4 below. This number can be anything from 10 to 1007, inclusive.

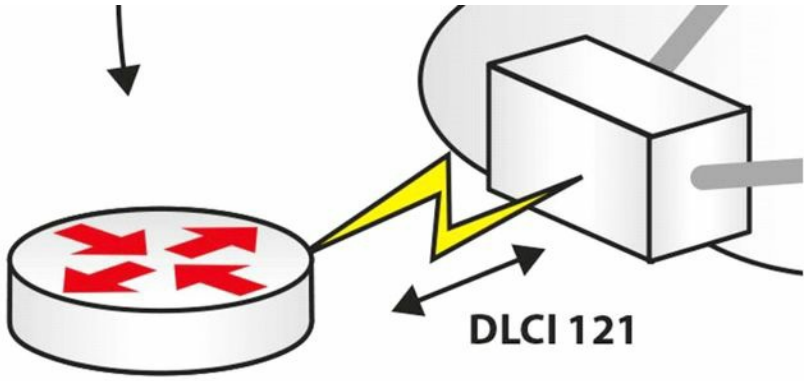


Figure 42.4 – DLCI Identifies Your Router to the Telco

Often, when troubleshooting Frame Relay links, the issue lies with either the customer or the service provider using the wrong DLCI number on their configuration.

When your DLCI is active, an end-to-end connection forms in the following order:

1. Active DLCI sends Inverse ARP request
2. DLCI waits for reply with network address
3. Map created of remote router address
4. DLCI status of Active/Inactive/Deleted

https://t.me/learningnets

NNI

The Network-to-Network Interface (NNI) is the connection between Frame Relay switches.

Frame Relay Technology

Frame Relay is a Non-Broadcast Multi-Access (NBMA) technology. This means that you have to deal with address resolution issues, except for the situations in which you use Point-to-Point interfaces.

The local Layer 2 addresses in Frame Relay are called Data Link Connection Identifiers (DLCI) and this is only locally significant. For example, in a hub-and-spoke environment, the hub device should have a unique DLCI to communicate to each of its spokes.

When you inspect the Frame Relay PVC status on a Cisco device, you will see a status code defined by LMI that can be any one of the following:

- Active (everything is okay)
- Inactive (no problems on the local node but possible problems on the remote node)
- Deleted (problem in the service provider network)

As an example, Cisco devices offer three flavours of LMI:

- CISCO
- ANSI
- Q.933a

Cisco routers are configured to automatically try all three of these LMI types (starting with the CISCO LMI) and use the one that matches whatever the service provider is using, so this should not be of much concern in the design phase.

One of the most important aspects that needs to be considered in the design phase is the address resolution methodology used. If you are utilising Multipoint interfaces in your design (i.e., interfaces that can terminate multiple Layer 2 circuits), you need to find a way to provide the Layer 3 to Layer 2 resolution. As discussed previously, you have two options that can help you achieve this:

- Dynamically, utilising Inverse ARP
- Statically, via the `frame-relay map` static configuration command on Cisco devices

> **NOTE:** In order to verify that the Layer 3 to Layer 2 resolution has succeeded, you can use the `show frame-relay map` command.

On a Multipoint interface, Inverse ARP would happen automatically. This functionality is enabled right after adding an IP address on an interface configured for Frame Relay. At that moment, requests start being sent out all of the circuits assigned to that specific interface for any supported protocol the interface is running.

https://t.me/learningnets

The request process can be disabled with the `no frame-relay inverse-arp` command, but you can never design a network that will stop responding to requests. By design, Inverse ARP replies cannot be disabled, so the Frame Relay speaker will always attempt to assist somebody that attempts to do a Layer 3 to Layer 2 resolution via the Frame Relay Inverse ARP.

The Inverse ARP behaviour in the Frame Relay design will automatically assist with Broadcasts through the replicated Unicast approach discussed before. When using Inverse ARP, Broadcast support exists by default.

If you connect two routers to the Frame Relay cloud using physical interfaces, this means that the specific interfaces are Multipoint from a Frame Relay perspective, because a physical Frame Relay interface by default is a Multipoint structure. Even though the connection between the two routers may appear to be Point-to-Point, it is a Frame Relay Multipoint connection.

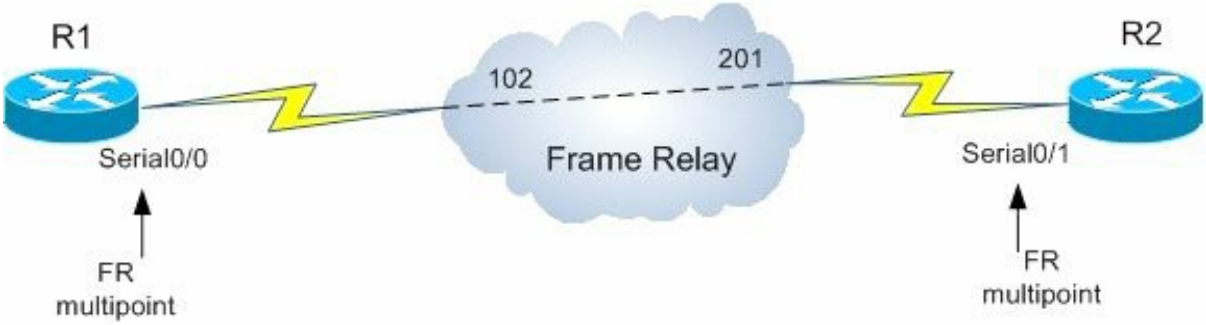


Figure 42.5 – Frame Relay Multipoint Example

Because they use Multipoint interfaces, by default the two devices will handle the Layer 3 to Layer 2 resolution dynamically by using Inverse ARP. If you would like to design a solution in which Inverse ARP would not be used, you can turn off the dynamic mapping behaviour on each device and then configure static Frame Relay mappings.

Point-to-point configurations are the ideal choice when it comes to Layer 3 to Layer 2 resolution because this process does not occur when using such interface types. When configuring Point-to-Point Frame Relay, you would use Point-to-Point subinterfaces and these subinterfaces would not get the DLCI assignments from LMI, like in the Multipoint situation.

Another option would be to create subinterfaces and declaring them as Multipoint. These types of interfaces behave exactly like the physical Multipoint interfaces, so you need to decide on the resolution method to be used, either Inverse ARP or static mappings. A combination of these methods can be used, for example, by implementing Inverse ARP on one end of the connection and defining static maps on the other end.

The interface type settings and the selected Layer 3 to Layer 2 resolution method is only locally significant. This means that you can have all kinds of variations in your Frame Relay design, such as those listed in Table 42.1 below:

Table 42.1 – Variations in the Frame Relay Design

Local Interface		Remote Interface
Main interface		Main interface
Main interface		Multipoint subinterface

https://t.me/learningnets

Main interface	**connected to**	Point-to-Point subinterface
Multipoint subinterface		Multipoint subinterface
Multipoint subinterface		Point-to-Point subinterface
Point-to-Point subinterface		Point-to-Point subinterface

Partial-mesh designs and configurations will be the most challenging. This implies that Layer 2 circuits will not be provisioned between all endpoints involved in the Frame Relay environment.

In a hub-and-spoke environment, the spokes are not directly connected to each other, so this means that they cannot resolve each other via Inverse ARP. In order to solve these issues, you can do any of the following:

- Provide additional static mappings
- Configure Point-to-Point subinterfaces
- Design the hub-and-spoke infrastructure so that the Layer 3 routing design can solve the resolution problems (e.g., by using the OSPF Point-to-Multipoint network type)

Frame Relay supports markings that can impact Quality of Service (QoS). For example, the Frame Relay header contains a DE (Discard Eligible) bit. With Frame Relay environments for QoS, packets can be marked with the DE bit and this informs the service provider that those specific packets are not very important and can be discarded in case of congestion. This behaviour will prioritise packets that do not have the DE bit set.

Other parameters that can be configured in the Frame Relay environment are Forward Explicit Congestion Notifications (FECNs) and Backwards Explicit Congestion Notifications (BECNs) which commonly crops up as an exam question. The Frame Relay equipment, if configured to do so, can notify devices of congestion and can cause the slowing down of the sending rates.

Configuring Frame Relay

Unfortunately, it can be somewhat tricky to configure Frame Relay, and this is because different network types require different commands. The reason for this is to overcome how network addresses resolve over the WAN and how routing protocols operate. The steps to configure Frame Relay are as follows:

1. Set encapsulation
2. Set LMI type (optional)
3. Configure static/dynamic address mapping
4. Address protocol-specific problems

You will not be expected to know how to configure a telco Frame Relay switch in the CCNA exam. You would only want to know how to do this if you are setting up your own Frame Relay connection on a home or remote lab.

https://t.me/learningnets

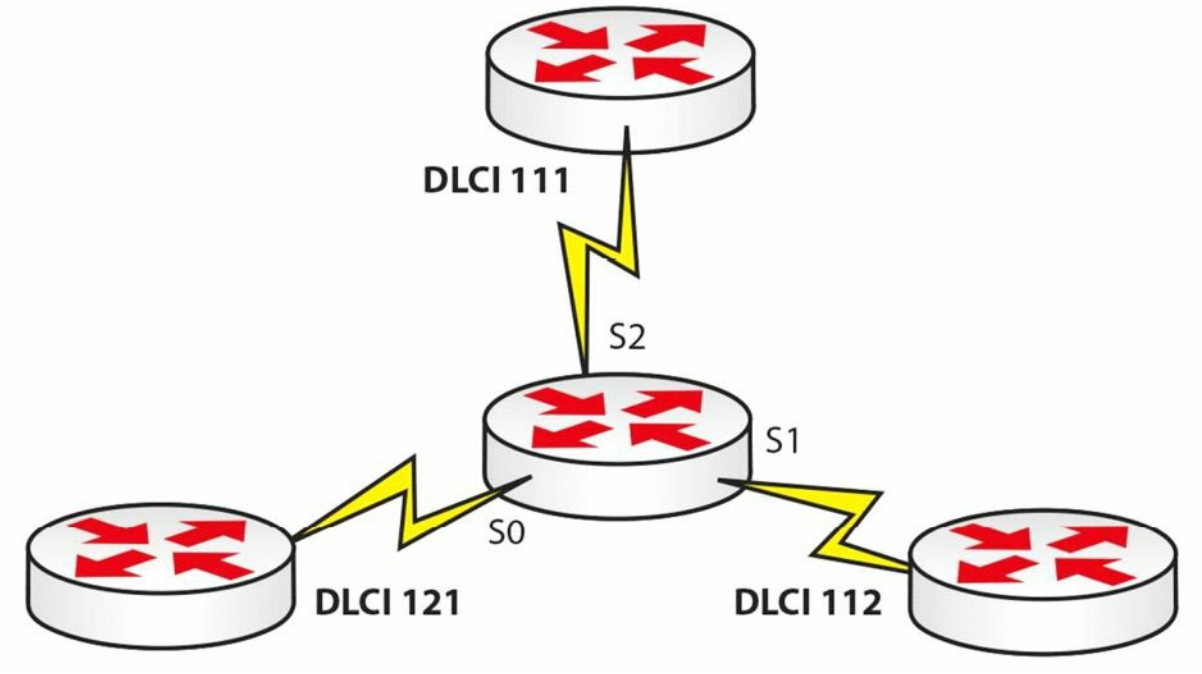


Figure 42.6 – Frame Relay Network

For the network topology above, you would configure the following on the Frame Relay switch in the middle. Please only use this information for reference, as you won't need it for the exam:

```
Router#conf t
Router(config)#frame-relay switching
Router(config)#int s0
Router(config-if)#clock rate 64000
Router(config-if)#encapsulation frame-relay
Router(config-if)#frame-relay intf-type dce
Router(config-if)#frame-relay route 121 interface s1 112
Router(config-if)#frame-relay route 121 interface s2 111
Router(config-if)#no shut
Router(config-if)#int s1
Router(config-if)#clock rate 64000
Router(config-if)#encapsulation frame-relay
Router(config-if)#frame-relay intf-type dce
Router(config-if)#frame-relay route 112 interface s0 121
Router(config-if)#frame-relay route 112 interface s2 111
Router(config-if)#int s2
Router(config-if)#clock rate 64000
Router(config-if)#encapsulation frame-relay
Router(config-if)#frame-relay intf-type dce
Router(config-if)#frame-relay route 111 interface s0 121
Router(config-if)#frame-relay route 111 interface s1 112
Router(config-if)#no shut
Router#show frame-relay route
```

https://t.me/learningnets

Troubleshooting Frame Relay

As stated earlier, often the telco gets the mapping information wrong when they map your DLCI to the wrong port or get the number wrong. You will need to prove that they are at fault before calling them or logging a ticket, using the following commands:

- `show frame-relay pvc`
- `show frame-relay lmi`
- `show frame-relay map`
- `debug frame-relay pvc`
- `debug frame-relay lmi`

Frame Relay Errors

Annoyingly, in the exam they sometimes like to ask you about errors on the Frame Relay link, so here is what you need to know:

- BECN – Frames in the direction opposite of the frame transmission experienced congestion
- FECN – Congestion was experienced in the direction of the frame transmission

PPP Operations

PPP is considered an Internet-friendly protocol due to the following factors:

- It supports data compression
- Authentication is built in (PAP and CHAP)
- Network Layer address negotiation
- Error detection

You can use PPP over several connection types, including the following:

- DSL
- ISDN
- Synchronous and asynchronous links
- HSSI

PPP can be broken down into the following Layer 2 sublayers:

- NCP – establishes Network Layer protocols (serves the Network Layer)
- LCP – establishes, authenticates, and tests link quality (serves the Physical Layer)
- HDLC – encapsulates datagrams over the link

Knowing the above may well come in handy during your CCNA exam!

https://t.me/learningnets

Configuring PPP

PPP is very easy to configure, as shown in Figure 42.7 and the following output below. You can also add authentication, which will be demonstrated in a moment.



Figure 42.7 – A PPP Connection

```
R1#conf t
R1(config)#interface s0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#encapsulation ppp
R1(config-if)#no shut
R2#conf t
R2(config)#interface s0
R2(config-if)#ip add 192.168.1.2 255.255.255.0
R2(config-if)#encapsulation ppp
R2(config-if)#no shut
```

PPP Authentication

PPP has built-in authentication in the form of Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). PAP sends the passwords over the link in clear text, which poses a security risk, whereas CHAP sends a hashed value using MD5 security. Here is a CHAP configuration:

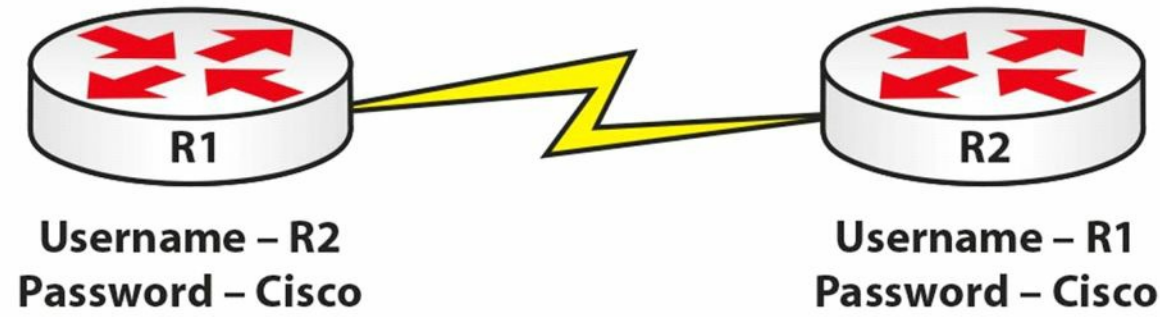


Figure 42.8 – PPP with CHAP

```
R1#conf t
R1(config)#username R2 password Cisco
R1(config)#interface s0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#encapsulation ppp
```

https://t.me/learningnets

```
R1(config-if)#ppp authentication chap
R1(config-if)#no shut
R2#conf t
R2(config)#username R1 password Cisco
R2(config)#interface s0
R2(config-if)#ip add 192.168.1.2 255.255.255.0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
R2(config-if)#no shut
```

To configure PAP, you would replace the `[chap]` keyword in the configuration above with the [`pap`] keyword. You can also configure PPP to attempt authentication using CHAP, but if this isn't successful, attempt with PAP. This is known as PPP fallback and here is the command:

```
R2(config-if)#ppp authentication chap pap
```

Troubleshooting PPP

Issue a `show interface serial 0/0` command, or the relevant interface number, to display the IP address, interface status, and the encapsulation type, as illustrated in the output below:

```
RouterA#show interface Serial0/0

Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 192.168.1.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
```

If you are using CHAP, then check to ensure that the username matches that of the router you are calling, and bear in mind that the hostnames are case sensitive. You troubleshoot PPP session establishment with the commands `debug ppp authentication` and `debug ppp negotiation`.

https://t.me/learningnets

Day 42 Questions

1. Frame Relay is based on which older protocol?
2. What are the three types of LMIs available?
3. An LMI is sent every _____ seconds, and every _____ message is a full status update.
4. The DLCI number is only locally significant, so you could have a different one for the other end of your Frame Relay connection. True or false?
5. Explain the difference between BECNs and FECNs.
6. PPP does not include data compression or error detection. True or false?
7. Name the PPP sublayers.
8. Write out the command to configure CHAP with PPP.
9. Which command will show you the encapsulation type on your Serial interface?
10. _____ sends the passwords over the link in clear text, which poses a security risk, whereas _____ sends a hashed value using MD5 security.

https://t.me/learningnets

Day 42 Answers

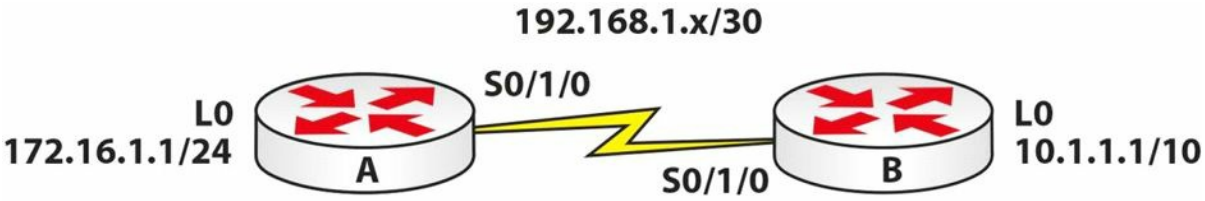
1. The X.25 protocol.
2. CISCO, ANSI, and Q933a.
3. 10, sixth.
4. True.
5. Backward Explicit Congestion Notification (BECN): Frames in the direction opposite of the frame transmission experienced congestion; Forward Explicit Congestion Notification (FECN): Congestion was experienced in the direction of the frame transmission.
6. False.
7. NCP, LCP, and HDLC.
8. `ppp authentication chap`.
9. The `show interface serial [number]` command.
10. PAP, CHAP.

https://t.me/learningnets

Day 42 Labs

HDLC Lab

Topology



Purpose

Try your hand at WAN troubleshooting.

Walkthrough

No walkthrough for this lab. Configure the network above. Your WAN will work using HDLC automatically. Ping across the Serial link to ensure that it is working. Then, break the network in the following ways.

1. Change the encapsulation type on Router B to PPP (thus breaking the link at layer 2). Do this with the following configuration:

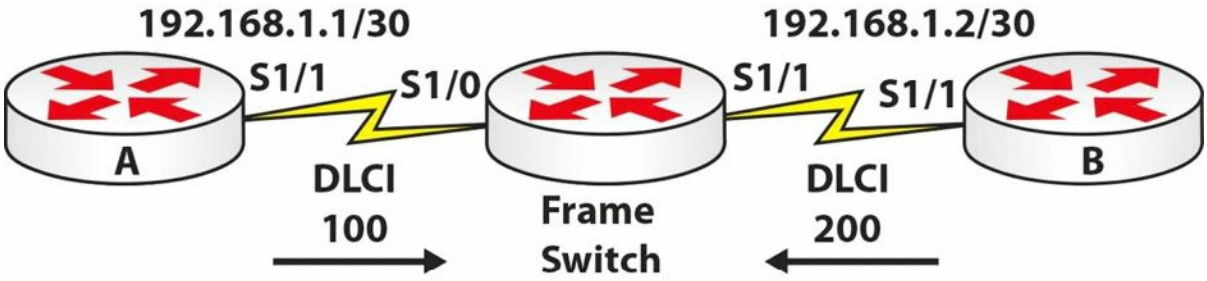
```
RouterB(config)#int Serial0/1/0
RouterB(config-if)#encapsulation ppp
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down
RouterB(config-if)#
```

2. Issue a `shut` command on the Serial interface on Router A. Then issue a `show ip interface brief` command. You should see your interface up/down.
3. Take the clock rate off your DCE interface side. Then issue the `show controllers serial x` command. It should tell you there is no clock rate configured.
4. Change the subnet mask on the Router B side to 255.255.255.0. You can see the subnet mask with a `show interface serial x` command. If that command isn't permitted in the exam, then issue a `show run` command.
5. Now fix all of the issues above. This is what you will have to do in the exam, and these are the most common issues. Please do test the commands you would enter if you were troubleshooting this issue to show you the IP address, encapsulation type, and clock rate.
6.

Frame Relay Lab

Topology

https://t.me/learningnets



Purpose

Learn to configure basic Frame Relay.

Walkthrough

1. Configure the Frame Relay switch first. You will never have to do this in the CCNA exam. Also, add the IP addresses to the Serial interfaces on Routers A and B.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router#hostname FrameSwitch
FrameSwitch(config)#frame-relay switching
FrameSwitch(config)#int s1/0
FrameSwitch(config-if)#encap frame-relay
FrameSwitch(config-if)#frame-relay intf-type dce
FrameSwitch(config-if)#clock rate 64000
FrameSwitch(config-if)#frame-relay route 100 int s1/1 200
FrameSwitch(config-if)#no shut
*May 10 04:28:13.275: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
*May 10 04:28:29.275: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed
state to up
FrameSwitch(config-if)#int s1/1
FrameSwitch(config-if)#encap frame
FrameSwitch(config-if)#frame-relay intf-type dce
FrameSwitch(config-if)#clock rate 64000
FrameSwitch(config-if)#frame route 200 int s1/0 100
FrameSwitch(config-if)#no shut
FrameSwitch(config-if)#^Z
FrameSwitch#show frame route
Input Intf   Input Dlci   Output Intf     Output Dlci   Status
Serial1/0    100          Serial1/1       200           inactive
Serial1/1    200          Serial1/0       100           inactive
FrameSwitch#
```

2. Configure Frame Relay on Router A.

```
RouterA(config)#interface s0/1/0
RouterA(config-if)#encap frame-relay
```

https://t.me/learningnets

```
RouterA(config-if)#frame-relay interface-dlci 100
```

```
RouterA(config-if)#no shut
```

3. Copy these commands on Router B, but your DLCI number is 200.
4. Ping across the Frame Relay link to test whether it has come up.

```
RouterB#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/17/20 ms
RouterB#
```

5. Check the Frame Relay PVC and mapping.

```
RouterB#show frame-relay pvc
PVC Statistics for interface Serial1/1 (Frame Relay DTE)
               Active     Inactive      Deleted       Static
  Local           1            0            0            0
  Switched        0            0            0            0
  Unused          0            0            0            0
DLCI = 200, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial1/1
  input pkts 1             output pkts 1             in bytes 34
  out bytes 34             dropped pkts 0            in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0            out FECN pkts 0
  out BECN pkts 0          in DE pkts 0              out DE pkts 0
  out bcast pkts 1         out bcast bytes 34
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:00:26, last time pvc status changed 00:00:26
RouterB#
RouterB#show frame map
Serial1/1 (up): ip 192.168.1.1 dlci 200(0xC8,0x3080), dynamic,
               broadcast, status defined, active
RouterB#
```

6. Debug Frame Relay LMI exchanges. When you see the `status 0x2` tag, issue an `undebug all` command to turn off debugs.

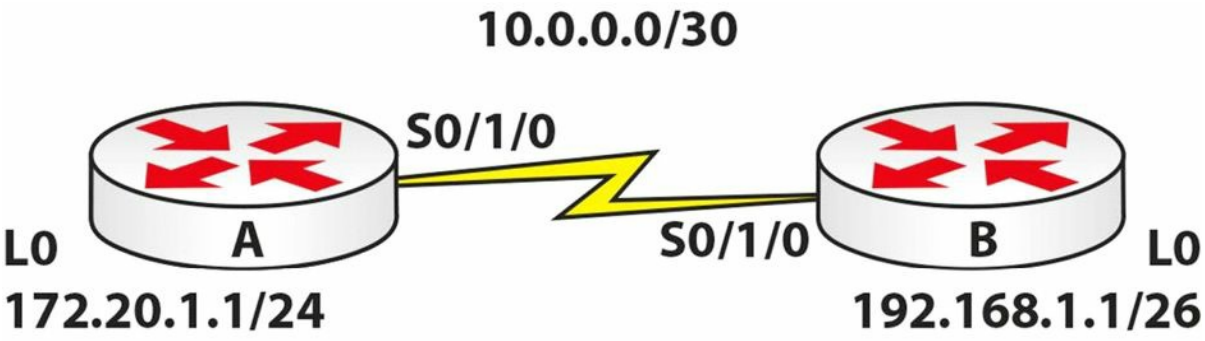
```
Router3#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
Router3#
*May 10 04:42:48.311: Serial1/1(out): StEnq, myseq 24, yourseen 23, DTE up
*May 10 04:42:48.311: datagramstart = 0xF1A6FCC4, datagramsize = 13
```

https://t.me/learningnets

```
*May 10 04:42:48.311: FR encap = 0xFCF10309
*May 10 04:42:48.311: 00 75 01 01 01 03 02 18 17
*May 10 04:42:48.311:
*May 10 04:42:48.319: Serial1/1(in): Status, myseq 24, pak size 13
*May 10 04:42:48.319: RT IE 1, length 1, type 1
*May 10 04:42:48.319: KA IE 3, length 2, yourseq 24, myseq 24
Router3#
*May 10 04:42:58.311: Serial1/1(out): StEnq, myseq 25, yourseen 24, DTE up
*May 10 04:42:58.311: datagramstart = 0xF1A73AFC, datagramsize = 13
*May 10 04:42:58.311: FR encap = 0xFCF10309
*May 10 04:42:58.311: 00 75 01 01 00 03 02 19 18
*May 10 04:42:58.311:
*May 10 04:42:58.319: Serial1/1(in): Status, myseq 25, pak size 21
*May 10 04:42:58.319: RT IE 1, length 1, type 0
*May 10 04:42:58.319: KA IE 3, length 2, yourseq 25, myseq 25
*May 10 04:42:58.319: PVC IE 0x7, length 0x6, dlci 200, status 0x2, bw 0
Router3#un all
```

Point-to-Point Protocol Lab

Topology



Purpose

Learn how to configure PPP and CHAP.

Walkthrough

1. Configure IP addresses and hostnames as per the topology above.
2. Set the encapsulation on each side to PPP. Here is the command for Router A:

```
RouterA(config)#interface s0/1/0
RouterA(config-if)#encapsulation ppp
```

3. Set CHAP on each router. You will set the hostname of the opposite router and the password `cisco`.

```
RouterA(config)#username RouterB password cisco
RouterA(config-if)#ppp authentication chap
RouterA(config-if)#exit
```

https://t.me/learningnets

```
RouterB(config)#username RouterA password cisco
RouterB(config-if)#ppp authentication chap
RouterB(config-if)#exit
```

4. Ping across the link to ensure it is up.

```
RouterB#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/31/32 ms
RouterB#
```

5. Break the connection by changing the hostname on Router A to Router C. You will also want to turn on PPP debugs and `shut/no shut` the interface to open negotiation again. You will have to be quick to type `undebug all`. If you are at the interface prompt, then type `do undebug all`.

```
RouterA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RouterA(config)#hostname RouterC
RouterC(config)#exit
RouterC#
RouterC#debug ppp neg
PPP protocol negotiation debugging is on
RouterC#debug ppp auth
RouterC#config t
RouterC(config)#int s0/1/0
RouterC(config-if)#shut
Serial0/1/0 LCP: State is Open
Serial0/1/0 PPP: Phase is AUTHENTICATING
Serial0/1/0 IPCP: O CONFREQ [Closed] id 1 len 10 ← Router won't authenticate
RouterC(config-if)#do undebug all
RouterC#sh int s0/1/0
Serial0/1/0 is up, line protocol is down (disabled)
```

Visit www.in60days.com and watch me do this lab for free.

https://t.me/learningnets

Day 43 – Review 1

Day 43 Tasks

- Take the exam below
- Complete the challenge lab
- Review switchport security (it can appear in the ICND2 exam)
- Read the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam)
- Spend 15 minutes on the subnetting.org website

Day 43 Exam

1. How do you turn off CDP on a router interface?
2. Write down the configuration to enable IPv6 on your router.
3. Write down all the administrative distances you remember.
4. What are the two available PPP authentication types? How do you configure them?
5. What are the OSI Data Link sublayers of PPP?

Day 43 Answers

1. Issue the `no cdp enable` command.
2. Enabling IPv6 on the router:

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router eigrp 1
R1(config-rtr)#eigrp router-id 1.1.1.1
R1(config-rtr)#no shutdown
R1(config-rtr)#exit
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ipv6 address 3fff:1234:abcd:1::1/64
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 eigrp 1
R1(config-if)#exit
```

3. Administrative distances:

Route Source	AD
Connected Interfaces	0
Static Routes	1
Enhanced Interior Gateway Routing Protocol (EIGRP) Summary Routes	5
External Border Gateway Protocol (eBGP) Routes	20
Internal Enhanced Interior Gateway Routing Protocol (EIGRP) Routes	90

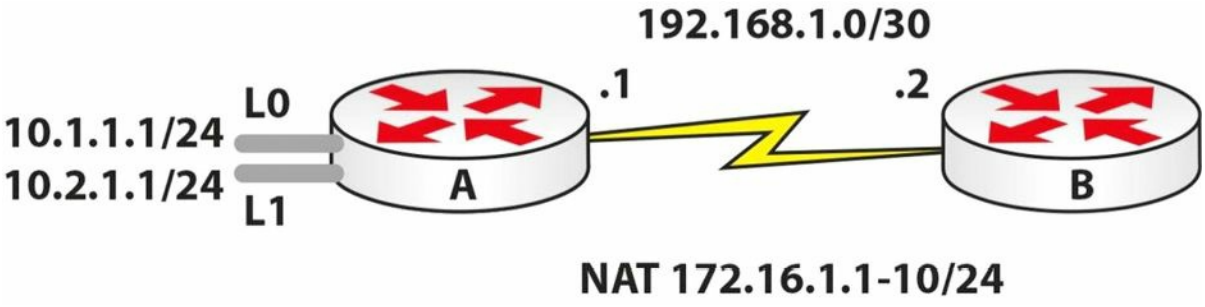
https://t.me/learningnets

Open Shortest Path First (OSPF) Internal and External Routes	110
Intermediate System-to-Intermediate System (IS-IS) Internal and External Routes	115
Routing Information Protocol (RIP) Routes	120
Exterior Gateway Protocol (EGP) Routes	140
On-Demand Routing (ODR) Routes	160
External Enhanced Interior Gateway Routing Protocol (EIGRP) Routes	170
Internal Border Gateway Protocol (iBGP) Routes	200
Unreachable or Unknown Routes	255

4. Check the PPP labs.
5. NCP, LCP, and HDLC.

Day 43 Lab – PPP and NAT

Topology



Instructions

Connect two routers together with a serial or crossover cable:

1. Add IP addresses to the routers and a Loopback interface on Router A, according to the diagram (NAT shouldn't be in the ICND2 exam but it's been known to appear again!)
2. Turn on `debug ppp negotiation` and `debug ppp authentication`
3. Configure PPP authentication CHAP for the WAN connection
4. Designate NAT inside and outside interfaces
5. Add a static route on Router B to send all traffic back to Router A
6. Ping between Router A and Router B to test the serial line (remember clock rates)
7. Turn off all debugging with the `undebug all` command
8. Create a NAT pool of 172.16.1 to 10, inclusive
9. Create two ACL lines to permit the Loopback networks (/24) for NAT
10. Turn on NAT debugging
11. Source two extended pings, one each from L0 and L1 from A to B
12. Check the NAT translation table

https://t.me/learningnets

Solution Hints and Commands

- ☐ CHAP authentication: define a username and password for the remote devices; add the `ppp authentication chap` command on the interface
- ☐ Issue the `ip nat inside` and `ip nat outside` commands on the interfaces to enable NAT
- ☐ Issue the `ip route` command to configure a static route
- ☐ Issue the `ip nat pool <name> <start_ip> <end_ip> netmask <mask>` command
- ☐ Issue the `ip nat inside source list x pool <name> overload` command
- ☐ Issue the de`bug ip nat` command

https://t.me/learningnets

Day 44 – Review 2

Day 44 Tasks

- Take the exam for Day 44 on www.in60days.com
- Review EIGRP, EIGRPv6, and OSPFv3 configuration commands
- Complete the lab below
- Read the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam)
- Spend 15 minutes on the subnetting.org website

Day 44 Lab – PPPoE

Please review the configuration commands in the PPPoE section.

Solution Hints and Commands

- See previous lesson for command details.

https://t.me/learningnets

Day 45 – Review 3

Day 45 Tasks

- Take the exam below
- Complete the challenge lab (it's on www.in60days.com)
- Review all switching
- Read the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam)
- Spend 15 minutes on the subnetting.org website

Day 45 Exam

1. Write down the configuration to create a VLAN, and put an interface into a VLAN on a switch.
2. Write down the configuration to create a trunk link.
3. Which two ways can you force a switch to become the Root Bridge for STP?
4. Which command configures RSTP on a switch?

Day 45 Answers

1.

```
Vlan 100
Name test
Int fax/x
Switchport mode access
Switchport access vlan 100
```

2.

```
sw mode trunk
sw trunk enc dot
sw trunk all vlan x,y,z (optional)
```

3. The `spanning tree vlan x root primary` command or the `spanning tree vlan x priority low_priority` command.
4. The `span mode rapid` command (this shortened version may not work on the exam sim).

https://t.me/learningnets

Day 46 – Review 4

Day 46 Tasks

- Take the exam below
- Complete the challenge lab
- Review SNMP and syslog, as well as OSPF
- Read the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam)
- Spend 15 minutes on the subnetting.org website

Day 46 Exam

1. What is the default STP priority on a switch?
2. Write down the port costs for STP connections for all the bandwidths from 4Mbps to 10Gbps.
3. Explain the purpose of Port Fast, BPDU Guard, BPDU Filter, Uplink Fast, and Backbone Fast.
4. Which command configures the Spanning Tree cost on a port?

Day 46 Answers

1. 32768
2.

Bandwidth	Default Port Cost
4Mbps	250
10Mbps	100
16Mbps	62
100Mbps	19
1Gbps	4
10Gbps	2

3. Port Fast is a feature that is typically enabled only for a port or interface that connects to a host. When the link comes up on this port, the switch skips the first stages of the STA and directly transitions to the Forwarding state. Contrary to popular belief, the Port Fast feature does not disable Spanning Tree on the selected port. This is because even with the Port Fast feature, the port can still send and receive BPDUs.

   The BPDU Guard feature is used to protect the Spanning Tree domain from external influence. BPDU Guard is disabled by default but is recommended for all ports on which the Port Fast feature has been enabled. When a port that is configured with the BPDU Guard feature receives a BPDU, it immediately transitions to the errdisable state.

https://t.me/learningnets

The BPDU Guard and the BPDU Filter features are often confused or even thought to be the same. They are, however, different, and it is important to understand the differences between them. When Port Fast is enabled on a port, the port will send out BPDUs and will accept and process received BPDUs. The BPDU Filter feature prevents the port from receiving any BPDUs but does not prevent it from sending them. If any BPDUs are received, the port will be errdisabled.

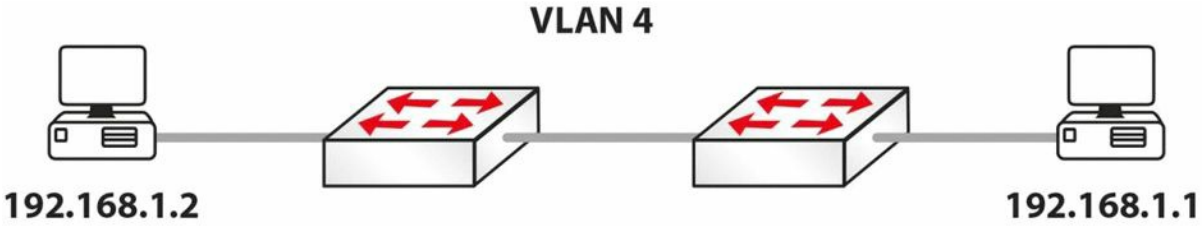
The Uplink Fast feature provides faster failover to a redundant link when the primary link fails (direct failure of the Root Port). The primary purpose of this feature is to improve the convergence time of STP in the event of a failure of an uplink. This feature is of most use on Access Layer switches with redundant uplinks to the Distribution Layer; hence, the name.

The Backbone Fast feature provides fast failover when an indirect link failure occurs in the STP domain. Failover occurs when the switch receives an inferior BPDU from its designated bridge (on it's Root Port). An inferior BPDU indicates that the designated bridge has lost its connection to the Root Bridge, so the switch knows there was an upstream failure and without waiting for timers to expire changes the Root Port.

1. The `spanning-tree cost` command.

Day 46 Lab – VLANs and STP

Topology



Instructions

Connect to the switch using a console connection. Connect a PC to each switch, or connect the switch to the FastEthernet port on a router:

1. Add IP addresses to the PCs or router Ethernet interfaces
2. Create VLAN4 on the switches
3. Set the ports the PCs connect to as access ports (default, but do it anyway)
4. Put the two switch ports into VLAN4
5. Configure the link between the switches as trunk ports and `no shut` them
6. Wait about 30 seconds, at most, and then ping from PC to PC
7. Check which switch is the Root Bridge with the `show spanning-tree vlan 4` command
8. Set the other switch as the Root Bridge with the `spanning-tree vlan 4 priority 0` command
9. Now check to see whether the switch has become the Root Bridge

https://networkingnerds.

10. Remove the `spanning-tree vlan 4 priority 0` command to reset the original switch as the Root Bridge (put `no` in front of the command)
11. Now set the other switch as the Root Bridge with the `spanning-tree vlan 4 root primary` command

Solution Hints and Commands

- ☐ `vlan 4 to create a VLAN`
- ☐ `sw mode access`
- ☐ `sw mode trunk`
- ☐ `sw access vlan 4`

https://t.me/learningnets

Day 47 – Review 5

Day 47 Tasks

- Take the exam below
- Complete the challenge lab
- Review OSPF
- Read the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam)
- Spend 15 minutes on the subnetting.org website

Day 47 Exam

1. You can see the ASN with the `show ip _____` command.
2. Every router you want to communicate with in your routing domain must have a different ASN. True or false?
3. What is the purpose of the EIGRP topology table?
4. By default, EIGRP uses the _____ bandwidth on the path to a destination network and the total _____ to compute routing metrics.
5. Dynamic neighbour discovery is performed by sending EIGRP Hello packets to the destination Multicast group address _____.
6. EIGRP packets are sent directly over IP using protocol number _____.
7. To populate the topology table, EIGRP runs the _____ algorithm.
8. The _____ _____ includes both the metric of a network as advertised by the connected neighbour, plus the cost of reaching that particular neighbour.
9. Cisco IOS software supports equal cost load sharing for a default of up to four paths for all IGP routing protocols. True or false?
10. Which EIGRP command can be used to enable unequal cost load sharing?

Day 47 Answers

1. `protocols.`
2. False.
3. The topology table allows all EIGRP routers to have a consistent view of the entire network. All known destination networks and subnets that are advertised by neighbouring EIGRP routers are stored there.
4. Minimum, delay.
5. 224.0.0.10.
6. 88.

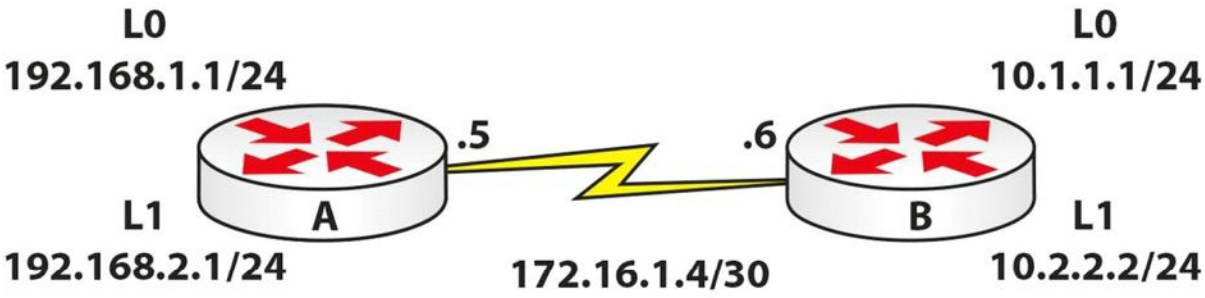
https://t.me/learningnets

7. DUAL.
8. Feasible Distance.
9. True*.
10. `variance`.

* Four entries is the default in IOS for IGPs, but for BGP one entry is the default. Six different paths configured is the maximum number.

Day 47 Lab – EIGRP and ACL

Topology



Instructions

Connect two routers together with a serial or crossover cable:

1. Add IP addresses to the routers and a Loopback interface on Router A and Router B, according to the diagram
2. Ping between Router A and Router B to test the serial line (remember clock rates)
3. Configure EIGRP 30 on both routers
4. Add all routes and add wildcard masks
5. Check the routing table. Were the routes summarised?
6. Now add the `no auto-summary` command to the EIGRP process
7. Ping all routes
8. Now add a named ACL on Router B; only Telnetting to 10.2.2.2 should be permitted
9. Make sure you have enabled Telnet and have added a username/password
10. Test the ACL by attempting to connect to 172.16.1.6 first, and then to 10.2.2.2
11. If EIGRP is no longer working, why would that be and how do you fix the issue?

Solution Hints and Commands

☐ `router eigrp 30`

```
network 0.0.0.0 255.255.255.255
```

☐ `show ip route` to check the routing table

☐ `ip access-list` to add a named ACL

https://t.me/learningnets

□ username x password y

https://t.me/learningnets

Day 48 – Review 6

Day 48 Tasks

- Take the exam below
- Complete the challenge lab
- Review EIGRP/FHRP
- Read the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam)
- Spend 15 minutes on the subnetting.org website

Day 48 Exam

1. Name two FHRP protocols that are Cisco proprietary.
2. Name the open standard FHRP protocol.
3. By default, when HSRP is enabled in Cisco IOS software, version 1 is enabled. True or false?
4. Which Multicast address does HSRP version 2 use to send Hello packets?
5. HSRP version 1 group numbers are restricted to the range of 0 to 255, whereas the version 2 group numbers have been extended from 0 to 4095. True or false?
6. What parameter can be adjusted in order to influence the HSRP primary gateway election?
7. How does HSRP interface tracking influence the primary gateway election process?
8. Which command can you use to configure an HSRP address on an interface?
9. Just like HSRP, VRRP has the option of allowing the gateway to use the BIA or a statically configured address as the MAC address for VRRP groups. True or false?
10. Which command can you use to configure a GLBP group "up" address on a router interface?

Day 48 Answers

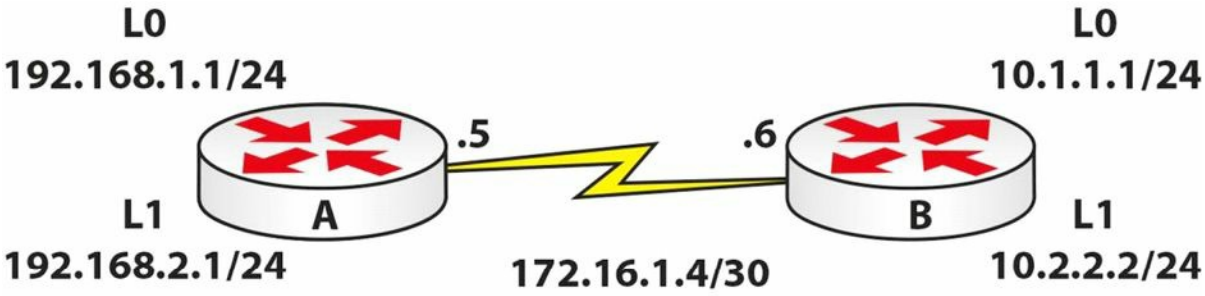
1. HSRP and GLBP.
2. VRRP.
3. True.
4. 224.0.0.102.
5. True.
6. The HSRP priority parameter.
7. It modifies HSRP priority based on interface status.
8. The `standby x up y` command.

https://t.me/learningnets

9. False.
10. The `glbp x ip y` command.

Day 48 Lab – OSPF

Topology



Instructions

Connect two routers together with a serial or crossover cable:

1. Add IP addresses to the routers and a Loopback interface on Router A and Router B, according to the diagram
2. Ping between Router A and Router B to test the serial line (remember clock rates)
3. Configure OSPF on both routers
4. Ensure that you add all the correct wildcard masks
5. Double-check the WAN wildcard mask and subnet: it ISN'T 172.16.1.0 0.0.0.3!!
6. Put all networks into an area, but put 192.168.2.0/24 into Area 1 and 10.2.2.0 into Area 2
7. Check the routing table
8. Check the router ID for each router
9. How would you change the router ID for each router?

Solution Hints and Commands

- ☐ Use the `router ospf x` command to enter OSPF Configuration mode
- ☐ Use the `network x.x.x.x y.y.y.y area z` command to configure a network in an area
- ☐ Use the `show ip route` command to view the routing table
- ☐ Use the `router-id x.x.x.x` command to change the OSPF router ID under the OSPF Process Configuration mode

https://t.me/learningnets

Day 49 – Review 7

Day 49 Tasks

- Take the exam below
- Complete the challenge lab
- Review IPv6/OSPF/Syslog/SNMP/Netflow/EIGRP
- Read the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam)
- Spend 15 minutes on the subnetting.org website

Day 49 Exam

1. What service and port does DNS use?
2. How would you block EIGRP with an ACL?
3. How does EIGRP and OSPF offer a way of sending route updates securely?
4. Where do switches get their base MAC address from? How would you find it?
5. Does PPP work with asynchronous links, or just synchronous?
6. How would you join OSPF Area 2 to the OSPF domain if it was connected only to Area 1?

Day 49 Answers

1. TCP/UDP port 53.
2. Issue the `acces-list x deny eigrp any any` command.
3. EIGRP: Interface mode authentication; and OSPF: authentication under router OSPF and under interface configuration.
4. From the `show version` command (see below).
5. Both types of links.
6. Use the `virtual-link` command (this is not in the CCNA syallbus but I thought I'd add it just in case).

https://t.me/learningnets

```
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(
E SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE
4)

System returned to ROM by power-on

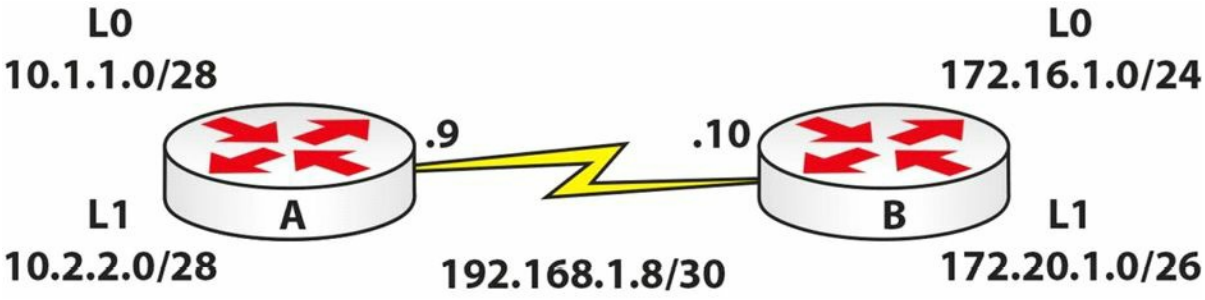
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K b
y.


24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0009.7C37.9EB9
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC1033Z1EY
--More--
```

Day 49 Lab – OSPF and ACL

Topology



Instructions

Connect two routers together with a serial or crossover cable:

1. Add IP addresses to the routers and a Loopback interface on Router A and Router B, according to the diagram
2. Ping between Router A and Router B to test the serial line (remember clock rates)
3. Configure OSPF on both routers
4. Ensure that you add all the correct wildcard masks (which subnet is the WAN link in?)
5. Put all networks into an area, but put 172.20.1.0/26 into Area 1 and 10.2.2.0/28 into Area 20
6. Check the routing table and ping all IP addresses
7. Configure an extended ACL on Router B
8. Block www traffic into Router B destined for the 172.20.1.0/26 network; permit all other IP traffic

https://t.me/learningnets

9. You can only test this if you have a web server behind the router OR on live routers by adding the `ip http server` command to the router and Telnetting on port 80:

   `RouterA#telnet 172.20.1.0 80` [this won't work on Packet Tracer]

Solution Hints and Commands

- ☐ Use the `router ospf x` command to configure OSPF
- ☐ `network x.x.x.x y.y.y.y area z`
- ☐ `access-list 100 deny tcp any 172.20.1.0 0.0.0.63 eq www`

https://t.me/learningnets

Day 50 – Review 8

Day 50 Tasks

- Take the exam below
- Complete the challenge lab
- Review the subjects of your choice
- Read the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam)
- Spend 15 minutes on the subnetting.org website

Day 50 Exam

1. Can a router in Area 0 running OSPF process ID 2 swap LSAs with a router in Area 0 running OSPF process ID 10?
2. What is the port cost for a FastEthernet interface in STP? What about for a 1Gigabit interface?
3. What is the difference between the `enable secret cisco` command and the `enable password cisco` command?
4. List the seven Cisco enhancements to STP.
5. Name the three LMI Frame Relay encapsulation types.
6. What does a DLCI do?
7. Is it true that the DLCI number must be the same across the entire Frame Relay circuit?

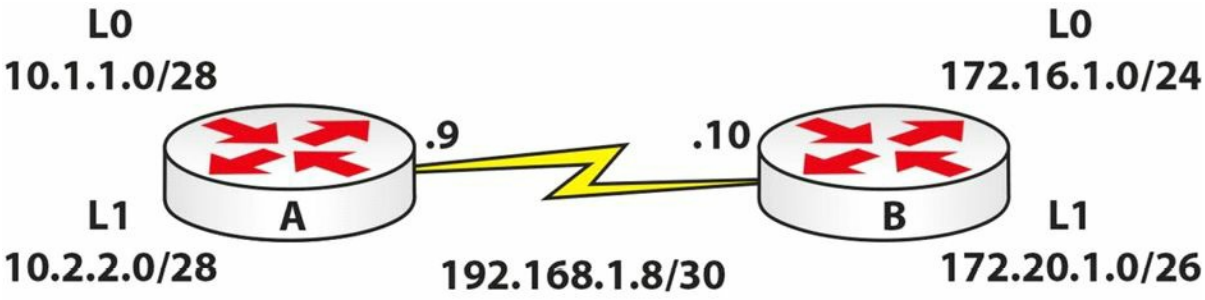
Day 50 Answers

1. Yes. The OSPF `process-id` configuration is only locally significant.
2. For FastEthernet, it is 19; for 1Gigabit, it is 4.
3. The `enable secret cisco` command is encrypted with MD5.
4. Port Fast, BPDU Guard, BPDU Filter, Loop Guard, Root Guard, Uplink Fast, and Backbone Fast.
5. CISCO, ANSI, and Q933a.
6. Identifies (tags) a connection with a Frame Relay switch.
7. No, it is locally significant only.

Day 50 Lab – EIGRP with PPP and ACL

Topology

https://t.me/learningnets



Instructions

Connect two routers together with a serial or crossover cable:

1. Add IP addresses to the routers and a Loopback interface on Router A and Router B, according to the diagram
2. Ping between Router A and Router B to test the serial lines (remember clock rates)
3. Now set the serial lines to use PPP but with no authentication required
4. Configure EIGRP on both routers; add wildcard masks and turn off `auto summary`
5. Check the routing table and ping all IP addresses
6. Configure an extended ACL on Router A
7. Block Telnet traffic to the router, unless destined for the 10.2.2.0/28 subnet
8. Configure Telnet access on the VTY lines for Router A, and do a login and password under the VTY line (not username and password)
9. Test the ACL by Telnetting to 10.1.1.1 (the IP address for Loopback0) from Router B
10. Test that it works by Telnetting to 10.2.2.1

Solution Hints and Commands

- ☐ Use the `router eigrp x` command to enter EIGRP Configuration mode
- ☐ Use the `show ip route` command to verify the IP routing table
- ☐ Use the `line vty 0 4` command to enter Line Configuration mode
- ☐ Use the `access-class` command under the VTY line to filter Telnet sources

https://t.me/learningnets

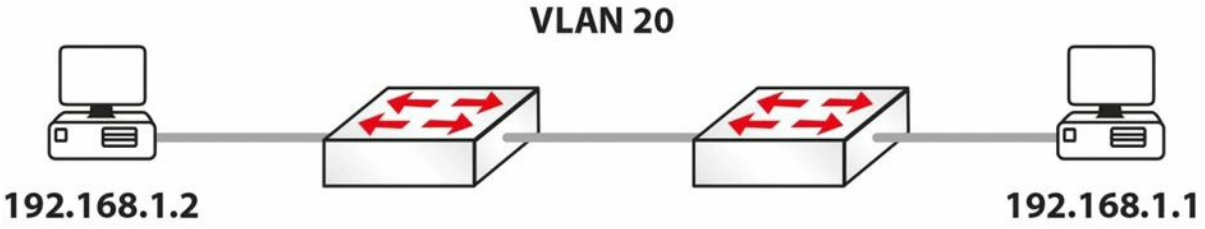
Day 51 – Review 9

Day 51 Tasks

- Complete the challenge labs below
- Review the subject of your choice
- Read the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam)
- Spend 15 minutes on the subnetting.org website

Day 51 Lab 1 – STP and VLANs

Topology



Instructions

Connect to the switch using a console connection. Connect a PC to each switch, or connect the switch to the FastEthernet port on a router:

1. Add IP addresses to the PCs or router Ethernet interfaces
2. Create VLAN20 on the switch
3. Set the ports the PCs connect to as access ports (default, but do it anyway)
4. Put the two switch ports into VLAN20
5. Check which switch is the Root Bridge
6. Force the other switch to become the Root Bridge
7. Hard set the switch ports to the PCs to 100Mbps and full duplex
8. Wait 30 seconds and test a ping

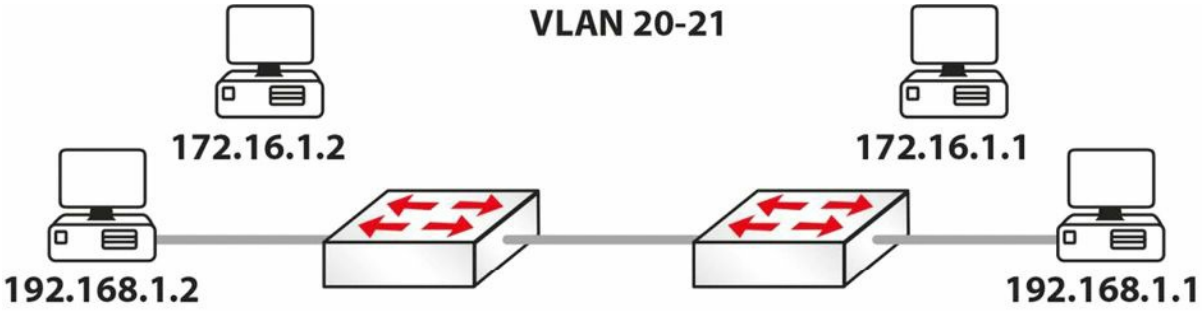
Solution Hints and Commands

- Use the `vlan 20` command to create VLAN
- `sw mode access`
- `sw access vlan 20`
- `show spanning-tree [parameters]`
- `span vlan 20 root primary`
- `speed 100 / duplex full`

https://t.me/learningnets

Day 51 Lab 2 – VLANs

Topology



Instructions

Connect to the switch using a console connection. Connect two PCs to each switch, or connect the switch to the FastEthernet port on two routers:

1. Add IP addresses to the PCs or router Ethernet interfaces
2. Create VLAN20 and VLAN21 on the switch
3. Set the ports the PCs connect to as access ports (default, but do it anyway)
4. Put two switch ports into VLAN20 and two switch ports into VLAN21; you can choose which subnets go into which VLANs
5. Check which switch is the Root Bridge
6. Force the other switch to become the Root Bridge for VLAN21 only
7. Ping from 172.16.1.1 to 172.16.1.2, and then from 192.168.1.1 to 192.168.1.2; you won't be able to ping between subnets, as there is no router involved

Solution Hints and Commands

- Same as in the previous lab.

https://t.me/learningnets

Day 52 – Review 10

Day 52 Tasks

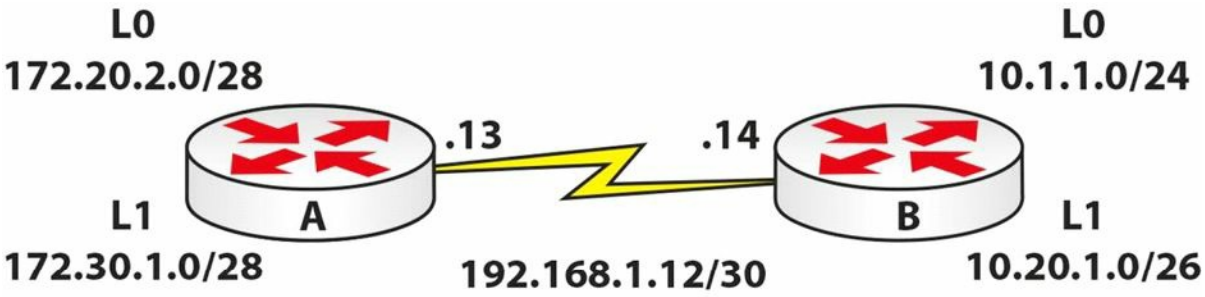
- Follow the exam tasks below
- Complete the challenge lab
- Review the subject of your choice
- Read the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam)
- Spend 15 minutes on the subnetting.org website

Day 52 Exam

- Spend some extra time on www.subnetting.org
- Write out the cram guide(s) from memory

Day 52 Lab – OSPF and Router Security

Topology



Instructions

Connect two routers together with a serial or crossover cable.

1. Add IP addresses to the routers and a Loopback interface on Router A and Router B, according to the diagram
2. Ping between Router A and Router B to test the serial lines (remember clock rates)
3. Now set the serial lines to use PPP with CHAP (also set usernames and passwords)
4. Configure OSPF on both routers and place one Loopback network in another area
5. Lock down both routers with enable secret passwords and Telnet passwords
6. Turn CDP off on one router and off the interface of the other router
7. Add a banner message on one router
8. Issue a `service password-encryption` command on one router
9. Check the routing tables

Solution Hints and Commands

https://t.me/learningnets

- ☐ Use the `router ospf x` command to enter OSPF Configuration mode.
- ☐ Use the `network x.x.x.x y.y.y.y area z` command to place a network in an area
- ☐ Use the `enable secret` command in Global Configuration mode
- ☐ Use the `no cdp run` command globally
- ☐ Issue a `no cdp enable` command per interface
- ☐ Use the `banner motd` command to configure a banner
- ☐ Use the `show ip route` command to check the routing table

https://t.me/learningnets

Day 53 – Review 11

Day 53 Tasks

- Take the exam below
- Complete the challenge lab
- Review the subject of your choice
- Read the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam)
- Spend 15 minutes on the subnetting.org website

Day 53 Exam

1. Write out the syntax for standard, extended, and named ACLs, and how to apply them to interfaces and the VTY line.
2. OSPF operates over IP protocol _____.
3. OSPF does NOT support VLSM. True or false?
4. Any router which connects to Area 0 and another area is referred to as an _____ _____ router or _____.
5. If you have a DR, you must always have a BDR. True or false?
6. The DR/BDR election is based upon which two factors?
7. By default, all routers have a default priority value of _____. This value can be adjusted using the _____ _____ _____ `<0-255>` interface configuration command.
8. When determining the OSPF router ID, Cisco IOS selects the highest IP address of configured Loopback interfaces. True or false?
9. What roles do the DR and the BDR carry out?
10. Which command would put network 10.0.0.0/8 into Area 0 on a router?

Day 53 Answers

1. Standard ACL: `access-list x permit host y.y.y.y` or `access-list x permit x.x.x.x x.x.x.x`

   Exnteded ACL: `access-list x permit/deny {service/protocol} {source network/IP} {destination network/IP} {port#}`

   Named ACL:

   ```
   Ip access-list extended NAME
   Permit x.x.x.x x.x.x.x
   Deny x.x.x.x x.x.x.x
   ```

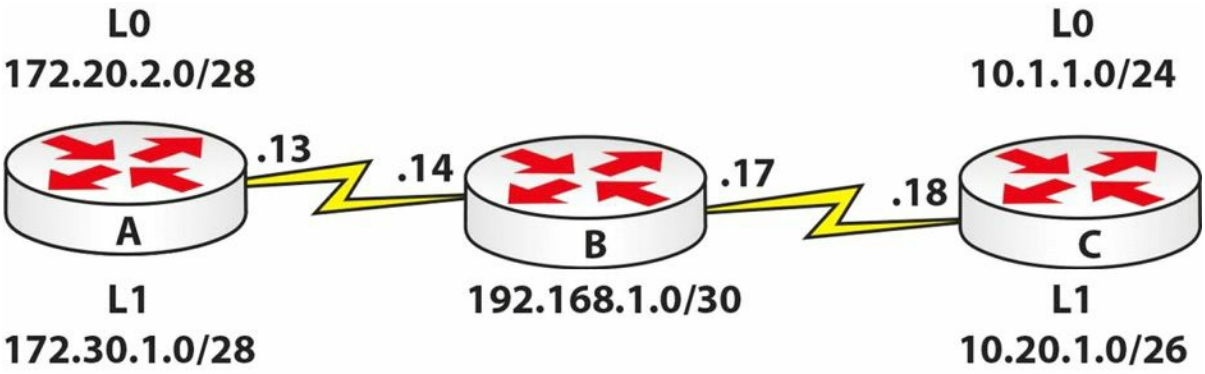
   Apply ACLs: `ip access-group x inside/outside on interface, access-class class x in/out on vty line`

https://t.me/learningnets

2. 89.
3. False.
4. Area Border or ABR.
5. False.
6. The highest router priority and the highest router ID.
7. 1, `ip ospf priority`.
8. True.
9. To reduce the number of adjacencies required on the segment, to advertise the routers on the Multi-Access segment, and to ensure that updates are sent to all routers on the segment.
10. The `network 10.0.0.0 0.255.255.255 area 0` command.

Day 53 Lab – EIGRP and ACL

Topology



Instructions

Connect three routers together with a serial or crossover cable:

1. Add IP addresses to the routers and Loopback interfaces on Routers A, B, and C, according to the diagram
2. Ping between Routers A and B and between Routers B and C to test the serial lines (remember clock rates)
3. Now set the serial lines to use PPP with CHAP (also set usernames and passwords)
4. Configure EIGRP 40 on all routers
5. Check the routing tables and make sure that you include both of the 192.168.1.x networks
6. Set an ACL to Router A; Telnet should be permitted from the Router C Serial address, but not from Router B; permit Telnet on Router A first, of course

Solution Hints and Commands

```
router eigrp 40
```

https://t.me/learningnets

- Use the `network` command to advertise the network in EIGRP
- Use the `access-class` command on VTY lines to filter traffic
- **NOTE:** The two networks on Router B are 192.168.1.12/30 and 192.168.1.16/30

https://t.me/learningnets

Day 54 – Review 12

Day 54 Tasks

- Take the exam below
- Complete the challenge lab
- Review the subject of your choice
- Read the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam)
- Spend 15 minutes on the subnetting.org website

Day 54 Exam

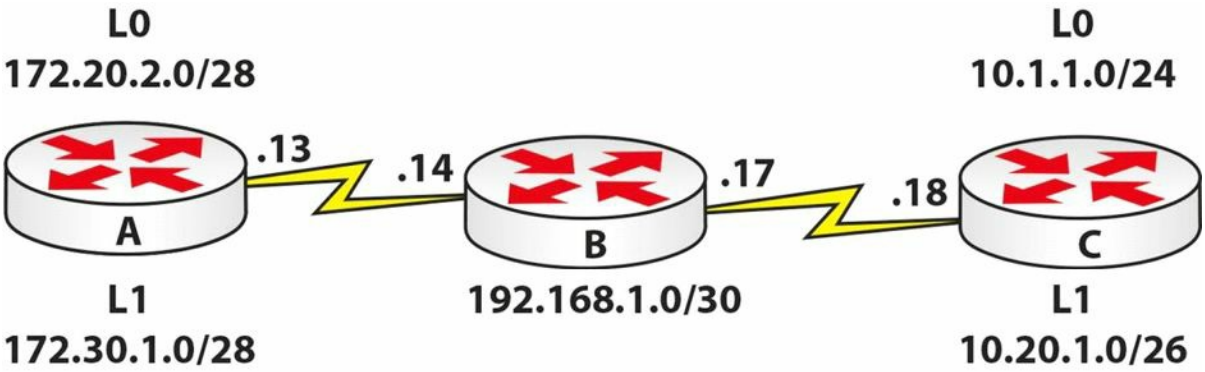
1. What is the default priority number for STP on switches?
2. What are the states STP ports transition through (in the correct order)?
3. What are the timers for the port transition states?
4. The STP Bridge ID is made from what?
5. What does IEEE 802.1W refer to?
6. Name the RSTP port roles.

Day 54 Answers

1. 32768.
2. Disabled, Blocking, Listening, Learning, and Forwarding.
3. Forward time: 15 seconds; Max Age: 20 seconds.
4. 2 bytes priority + 6 bytes system ID.
5. RSTP.
6. Root, Designated, Alternate, and Backup.

Day 54 Lab – OSPF and ACL

Topology



Instructions

https://timelearningnets

Connect three routers together with a serial or crossover cable:

1. Add IP addresses to the routers and Loopback interfaces on Routers A, B, and C, according to the diagram
2. Ping between Routers A and B and between Routers B and C to test the serial lines (remember clock rates)
3. Now set the serial lines to use PPP with CHAP (also set usernames and passwords)
4. Configure OSPF on all routers; put one Loopback on either end in a non-zero area
5. Check the routing tables and make sure that you include both of the 192.168.1.x networks
6. Set a named ACL on Router A; DNS traffic should be permitted into Router A only if it comes from Router C; all other IP traffic should be permitted (excluding DNS!)

You won't be able to test this ACL unless you have a DNS service running behind the router, or have live (or GNS3) equipment and can Telnet on the correct port. Post on the study page if you get stuck.

Solution Hints and Commands

- ☐ Use the `ip address` command on the interface to set an IP address
- ☐ CHAP: `username` and `password` for remote peer, `ppp authentication chap` on interfaces
- ☐ Use the `router ospf x` command to enter Router Configuration mode
- ☐ Define networks under the `router ospf` command with the network statement
- ☐ Use the `ip access-list` command for named ACLs
- ☐ **NOTE:** The two networks on Router B are 192.168.1.12/30 and 192.168.1.16/30

Please also complete the above lab using OSPFv3.

https://t.me/learningnets

Day 55 – Review 13

Day 55 Tasks

- Take the exam below
- Complete the challenge lab
- Review the subject of your choice
- Write out the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam) from memory
- Spend 15 minutes on the subnetting.org website

Day 55 Exam

1. Name at least three reasons for EIGRP neighbour relationships not forming.
2. Which command can you use to verify EIGRP K values?
3. Which command can you use to verify EIGRP packets statistics?
4. Name at least two common reasons for EIGRP route installation failures.
5. The administrative distance concept is used to determine how reliable the route source is. True or false?
6. By default, EIGRP automatically summarises at classful boundaries and creates a summary route pointing to the Null0 interface. True or false?
7. Name the command you can use to debug FSM events.
8. Which command can you use to see the originating router ID of a specific prefix?
9. Which command can you use to show the EIGRP event log?
10. What is the best command to use when debugging various routing issues?

Day 55 Answers

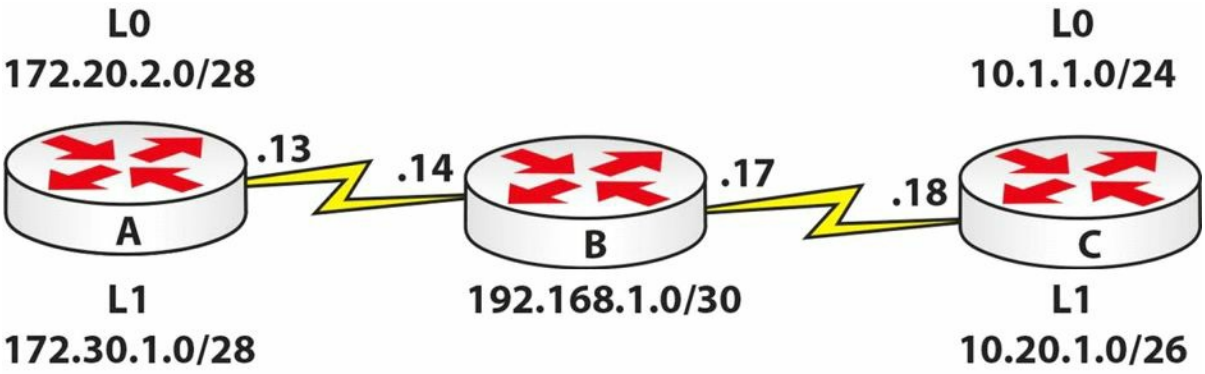
1. The neighbour routers are not on a common subnet; mismatched primary and secondary subnets; mismatched K values; mismatched ASN; ACLs are filtering EIGRP packets; Physical Layer issues; Data Link Layer issues; and mismatched authentication parameters.
2. The `show ip protocols` command.
3. The `show ip eigrp traffic` command.
4. The same route is received via another protocol with a lower administrative distance; EIGRP summarisation; duplicate router IDs are present within the EIGRP domain; and the routes do not meet the Feasibility Condition.
5. True.
6. True.

https://t.me/learningnets

7. The `debug eigrp fsm` command.
8. The `show ip eigrp topology x.x.x.x y.y.y.y` command.
9. The `show ip eigrp events` command.
10. The `debug ip routing` command.

Day 55 Lab – OSPF and NAT

Topology



Instructions

Connect three routers together with a serial or crossover cable:

1. Add IP addresses to the routers and Loopback interfaces on Routers A, B, and C, according to the diagram
2. Ping between Routers A and B and between Routers B and C to test the serial lines (remember clock rates)
3. Now set the serial lines to use PPP with CHAP (also set usernames and passwords)
4. Configure OSPF on all routers; put one Loopback on either end in a non-zero area, but do not add 172.30.1.0 to OSPF
5. Check the routing tables and make sure that you include both of the 192.168.1.x networks
6. Create a NAT pool of 192.168.2.1 to 10/24, inclusive, on Router A; set an ACL to match the 172.30.1.0/28 subnet
7. Set a static route on Router B for traffic destined to 192.168.2.0/24 to next-hop 192.168.1.13
8. Turn on NAT debugging on Router A, and do an extended ping from 172.30.1.1 to Router B

Solution Hints and Commands

- ☐ Use the `ip address on interface` command to set an IP address
- ☐ CHAP: `username` and `password` for remote peer, `ppp authentication chap` on interfaces
- ☐ Use the `router ospf x` command to enter Router Configuration mode

https://t.me/learningnets

☐ Define networks under the `router ospf` command with a network statement

☐ Use the `ip access-list` command for named ACLs

☐ Use the `ip route` command for static route configuration

☐ `debug ip nat`

NOTE: The two networks on Router B are 192.168.1.12/30 and 192.168.1.16/30

https://t.me/learningnets

Day 56 – Review 14

Day 56 Tasks

- Complete the challenge labs below
- Review the subject of your choice
- Write out the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam) from memory
- Spend 15 minutes on the subnetting.org website

Day 56 Lab

Repeat the following three challenge labs, each in 10 minutes, without looking at the configuration guide:

- ☐ OSPF with NAT
- ☐ OSPF with ACL
- ☐ VLANs and STP

Please also review the configurations for EtherChannels and FHRP protocols.

https://t.me/learningnets

Day 57 – Review 15

Day 57 Tasks

- Complete the challenge labs below
- Review the subject of your choice
- Write out the ICND2 cram guide (and the ICND1 cram guide, if taking the CCNA exam) from memory
- Spend 15 minutes on the subnetting.org website

Day 57 Labs

Repeat the following four challenge labs:

- ☐ PPP and NAT
- ☐ VLANs
- ☐ VLANs and STP
- ☐ EIGRP

https://t.me/learningnets

Day 58 – Review 16

Day 58 Tasks

Check the entire list of exam topics for your exam (ICND2 or CCNA). Mark them out of 10 for how well you understand them. Anything less than an 8, review today. They are listed at the start of the book.

https://t.me/learningnets

Day 59 – Review 17

Day 59 Tasks

Review any areas of your choice.

https://t.me/learningnets

Day 60 – Review 18

Day 60 Tasks

Exam day for you (or tomorrow).

Nothing else I can teach you or recommend. You know your weak areas, so good luck.

When you pass the exam, please drop me a line at howtonetwork@gmail.com, along with a photo of you holding your CCNA certificate.

Code Words

Please use the correct word in order to get access to all the book bonuses on www.in60days.com

1. Cheese23
2. Sausage44
3. Potato56
4. Apple90
5. Banana11
6. Pizzapie84
7. Chicken55
8. Sultana33
9. Orange03
10. Battery28

https://t.me/learningnets