

Welcome to INE's CCNA Bootcamp

Keith Bogart



Course Introduction (continued)

- Course Logistics
 - ✓ Start/End times
 - ✓ Breaks
- PLEASE ask questions! Otherwise the instructor will ASSUME you know something.
- Interactivity is crucial for a good learning experience.

Copyright © www.ine.com



- Prerequisites: You've watched all of the CCNA videos...or have read through all of the CCNA Certification Guides
- -
- Course Logistics – 9am until 7pm each day except Friday (we'll end by 3pm)
- -
- Breaks: 15-minute break every 90-minutes of class. / One 60-minute break at 12:30pm PST
- -
- I am assuming everyone has watched the CCNA video series. As such I'm assuming you have a base of knowledge. If I say something that you don't understand...RAISE YOUR HAND AND ASK!!

- Interactivity: Please answer my questions when asked...and please ask questions whenever you need to.

Course Agenda

- » Networking & Cisco IOS Basics
- » Switching (MAC Address-table, VLANs, Trunks, RSTP, etc)
- » IP Routing
- » Security with Access-Lists
- » Wireless Networking
- » Network Address Translation
- » Network Programmability and SDN
- » ...and much more (time permitting)

An Overview Of IPv4, UDP and TCP

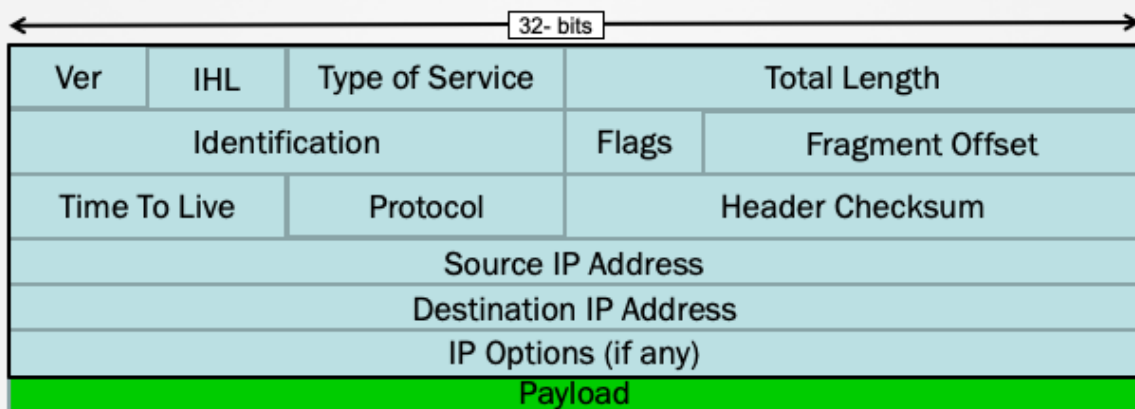


www.ine.com

Introduction to IPv4

» Internet Protocol version 4

- Resides at OSI Layer-3 (Network Layer)
- Connectionless



IHL = number of 32-bit “words” in the IP header.

Minimum size of IP packet = 20bytes

Maximum size of IP packet = 65,535 bytes

Common IP Protocol Numbers:

ICMP = 1

IGMP = 2

TCP = 6

UDP = 17

EIGRP = 88

OSPF = 89

Mention that IP is not the ONLY protocol to work at Layer-3, there are other options: IPv6, IPX, Appletalk, etc

Introduction to IPv4

- » 32-bit addressing system
- » Logical address for a network defined by IANA
- » IPv4 addresses are comprised of 4 octets
- » Dotted decimal notation is used to segment the octet

Communication Types

» Unicast

- One-to-one communication

» Multicast

- One-to-many communication

» Broadcast

- One-to-all communication

****** LAB TIME: “Lab Tasks” overview ___and___ Lab Access & Application Familiarization**

DHCP

» Dynamic Host Configuration Protocol

- Dynamic assignment of IP information
- Based on older BootP protocol
- Client / Server
- Utilizes UDP (port 67 and 68)

WHITEBOARD

ARP

» Address Resolution Protocol

- Used to resolve Layer-2 address of hosts on same LAN.
- Broadcast-based

» Proxy ARP

- Optional feature on routers and Wi-Fi access points
- Router replies on behalf of hosts

DNS

- » **Domain Name Service**
- » **Used by computers to resolve names to IP addresses.**
- » **Typically uses UDP port 53.**
- » **DNS server responds to DNS requests**
 - Host sends DNS A-Record query
 - DNS server responds with A-Record query response.

Copyright © www.ine.com



DNS can use TCP if the records being requested exceed the maximum size that DNS via UDP would allow...but this is rare (over 4096 bytes).

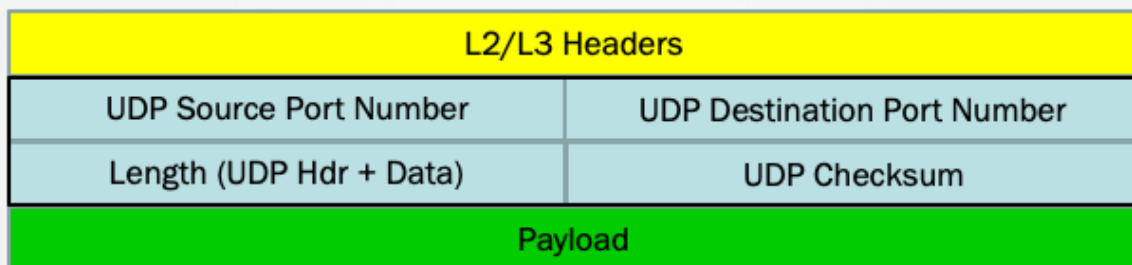
OSI Transport Layer - UDP

» Predominant protocols used at Layer-4

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

» UDP

- Connectionless



Copyright © www.ine.com



Examples of common protocols that use UDP:

TFTP – 69

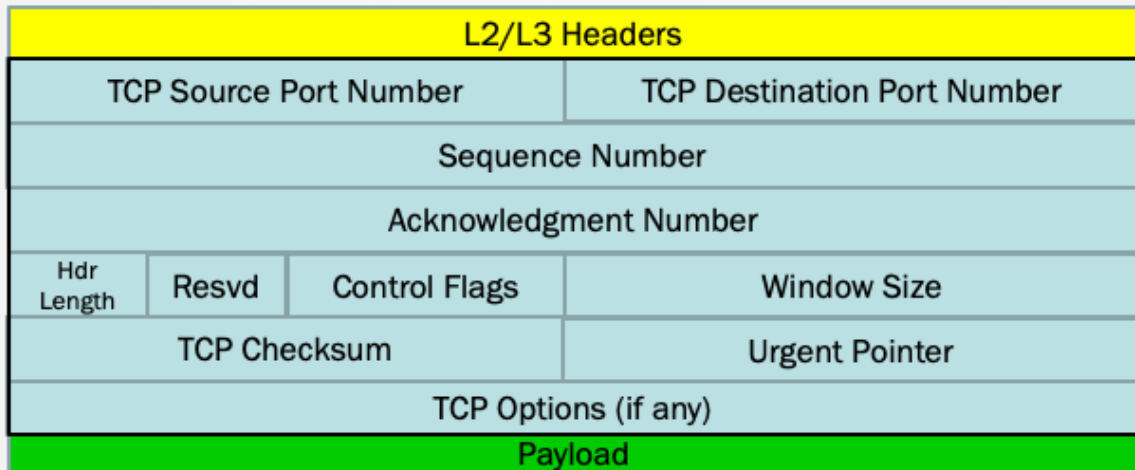
DNS – 53 (can also operate with TCP)

RIP (520)

OSI Transport Layer - TCP

» Transmission Control Protocol

- Connection-oriented



Copyright © www.ine.com

INE

FIRST TALK ABOUT (before explaining headers) 3-way handshake

WIRESHARK Demo

Window Size = Maximum quantity of segments (in bytes) the sender is willing to accept.

Talk about: MSS (Maximum Segment Size) that is sent during TCP 3-way handshake.

Talk about: Common protocols that use TCP:

Telnet (23)

FTP (20 and 21)

POP3 (110)

SMTP (25)

HTTP (80)

HTTPS (443)

ICMP

- » **Internet Control Message Protocol**
- » **Originally defined in RFC 777**
 - “Occasionally a gateway or destination host will communicate with a source host, for example, to report an error in datagram processing. For such purposes this protocol, the Internet Control Message Protocol (ICMP), is used.”
- » **Several different ICMP Message types used for different purposes**
 - ICMP Echo Request / Echo Reply (invoked via the “ping” command)
 - ICMP Redirect
 - ICMP Host Unreachable

Copyright © www.ine.com



*** LAB TIME: Viewing TCP Segments

IPv4 Addressing



www.ine.com

Classes of IPv4

» Classes:

- Class A: 0.0.0.0 through 127.255.255.255
- Class B: 128.0.0.0 through 191.255.255.255
- Class C: 192.0.0.0 through 223.255.255.255
- Class D: 224.0.0.0 through 239.255.255.255
- Class E: 240.0.0.0 through 255.255.255.255
 - Note: 127 ranges are considered as loopbacks
 - Note: 169.254 ranges are considered as APIPA

Subnet Mask

- » **Helps identify network and host portion of network**
- » **Default subnet masks:**
 - Class A: 255.0.0.0 or /8
 - Class B: 255.255.0.0 or /16
 - Class C: 255.255.255.0 or /24
- » **Typically called classful address**

IPv4 Addresses: Public & Private

- » IP addresses “leased” to a corporation are known as ***public IP addresses***.
- » IP addresses that are unregistered and may overlap from one company to the next, are known as ***private IP addresses***.

IPv4 Addresses: Private

» Private IPv4 address:

- Defined in RFC 1918
- For internal use only

» Range of private address

- Class A : 10.0.0.0 through 10.255.255.255
- Class B : 172.16.0.0 through 172.31.255.255
- Class C : 192.168.0.0 through 192.168.255.255

IPv4 Addresses: Public

» Public IPv4 addresses

- Globally unique
- Should be purchased
- Usually used in Internet edge

» Range of public addresses

- Beyond the RFC 1918 space, all addresses are public

Binary to Decimal (vice-versa)

How a subnet mask is used along with an IP address to determine the subnet/network.

----Concept of network, broadcast, and host addresses

Given an address, be able to determine if it is a network, broadcast, or host address.

Given a host address, determine the network and broadcast addresses it belongs to.

Introduction To Cisco IOS



www.ine.com

Introduction To IOS

- » **Internetworking Operating System**
- » **Native software for Cisco routers and switches**
- » **Cisco develops different IOSs for different platforms**
 - Example: Cisco 1841, Cisco 2821, etc.
- » **Usually operated through CLI**

Device Startup Sequence

- » **Cisco routers and switches generally perform the same steps upon initial startup**
 - Discover device hardware
 - Find and load IOS image
 - Find and load configuration file.
- » **Memory Types**
 - Flash, NVRAM, and DRAM

Copyright © www.ine.com



WHITEBOARD: Memory types and what is stored

- Flash: Cisco IOS image
- NVRAM: Startup-config
- DRAM: Running-Config/ running IOS image (also called, “system” memory in output of dir all command)

Accessing Device via CLI

- » **Basically, two methods of configuring router/switch**
 - CLI (command-line interface)
 - GUI (graphical user interface)
- » **Console port is used for initial configuration**
- » **Prerequisites**
 - Console cable
 - Terminal emulator

Copyright © www.ine.com



9600 (baud)-8 (data bits)-None (parity bits)-1 (stop bit) – No flow control

Accessing Device via CLI

- » Connect console cable into the “console” port of a Cisco device
- » Open terminal emulator software like Putty or SecureCRT
- » Choose serial option with default baud rate, such as 9600

IOS Command Structure

» IOS has a command hierarchy

- Router> - User (or EXEC) mode
- Router# - Privileged EXEC (or Enable) mode
- Configuration modes
 - Router(config)# - Global Configuration Mode
 - Router(config-if)# - Interface Configuration Mode
 - Router(config-router)# - Router Configuration Mode
- Usage of Exit, End, Ctrl-Z

Copyright © www.ine.com



Demonstration

- Initial Configuration Dialogue
- Usage of built-in help
- Tab Key
- Ctrl-A and Ctrl-E
- Command history

Initial Configuration Commands

- » **Prevent syslog and event messages from interrupting CLI input**
 - Router(config-line)# logging synchronous
- » **Prevent DNS resolution attempt for mis-typed commands**
 - Router(config)# no ip domain-lookup
 - IOS-XE(config)#no ip domain lookup
- » **Configure descriptive device name**
 - Router(config)# hostname Lab-1-Rtr

Copyright © www.ine.com



Note that CSR routers running IOS-XE don't have the hyphen in the command "no ip domain lookup".

Initial Configuration Commands

- » **Configure informative banner**
 - Router(config)# banner motd
- » **Add IPv4 address to an interface**
 - Router(config-if)# ip address <address><mask>
 - Router(config-if)# no shutdown
- » **Verifying interface naming conventions and IP address assignments:**
 - Router#show ip interface brief

Monitoring Memory and Images

- » **Display current IOS version running**
 - Router# show version
- » **Display all memory locations and file names**
 - Router# dir all
- » **Display saved, startup configuration file**
 - Router# show startup-config
- » **Display current running configuration**
 - Router# show running-config

Saving and Deleting Configurations

» Save current Running Configuration

```
Router# copy running-config startup-config
```

Or...

```
Router# write memory
```

» Setting a router back to factory defaults

- **Step-1: Delete startup configuration**

```
Router# erase startup-config
```

Or...

```
Router# write erase
```

- **Step-2: Reload the router**

```
Router# reload
```

DEMONSTRATION: How to factory reset a router.

Reverting To Saved Configs

- » **Running Configuration can be saved with a unique name**
Router# copy running-config flash:Keith-config
- » **Current running-configuration can be swapped/replaced with saved configurations**

```
Router#config replace flash:Keith-config  
This will apply all necessary additions and deletions  
to replace the current running configuration with the  
contents of the specified configuration file, which is  
assumed to be a complete configuration, not a partial  
configuration. Enter Y if you are sure you want to proceed. ? [no]: y
```

Securing IOS Remote Access



www.ine.com

Securing Device Access

» Configuring enable password

- Switch(config)# enable password <password>

OR

- Switch(config)# enable secret <password>

» Configuring console password

- Switch(config)# line console 0
- Switch(config-line)# password <password>

Remote Device Access

» Telnet

- TCP/IP protocol for connection to remote shells
- Takes the same commands you enter in the console and wraps them in a TCP/IP header
- Entire message body is sent in clear text

» SSH (Secure Shell)

- Same objective as Telnet
- Also utilizes TCP/IP
- Encrypts the message body thus is more secure than Telnet

Configuring Remote Access With Telnet

» Configuring Telnet password

- Switch(config)# line vty 0 4
- Switch(config-line)# password <password>
- Switch(config-line)# login

OR

- Switch(config)# username <username> privilege 15
password <password>
- Switch(config-line)# login local

Configuring Remote Access With SSH

» **Three components needed to enable SSH in an IOS device:**

- Hostname
- Domain-name
- Cryptographic key generation

```
Device(config)#hostname MyRouter  
MyRouter(config)#ip domain-name ine.com  
MyRouter(config)#crypto key generate rsa
```

» **You must also configure VTY lines for password usage (see previous slide)**

Copyright © www.ine.com



Although most routers will allow you to select the default size of 512-bits for your RSA Crypto Key, on some routers this will prevent SSH from working. As a best practice you should configure a size of at least 1024-bits.

Controlling Remote Access Methods

- » By default, Cisco IOS allows both incoming SSH and Telnet connections (after appropriate configuration has been applied)
- » For security purposes, it's better to disallow Telnet connections.
 - Device(config)#line vty 0 4
 - Device(config-line)#transport input ssh

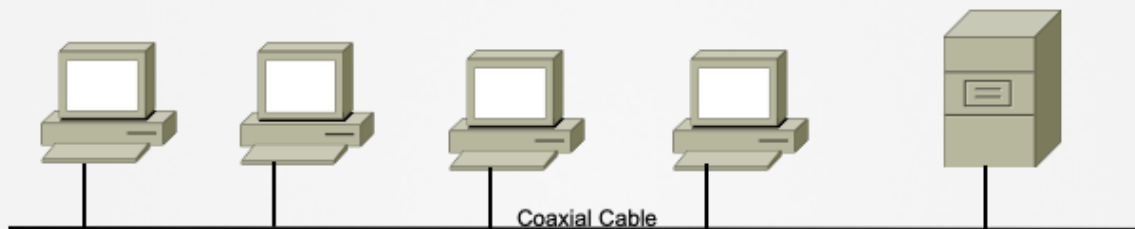
****** LAB TASK TIME: Introduction To Basic IOS CLI Commands**

Let's Learn About Switching



www.ine.com

Evolution of Switching (1)



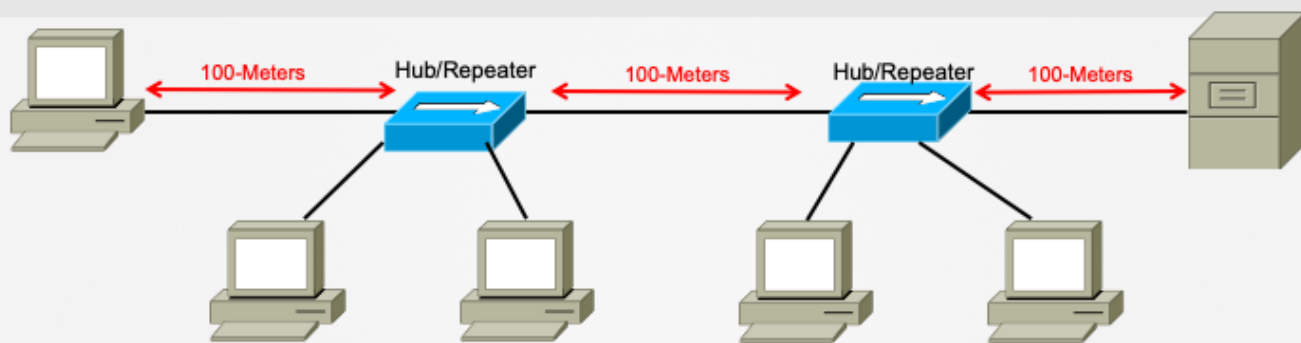
Vampire Tap

Copyright © www.ine.com



Distance limitations = 100-meters

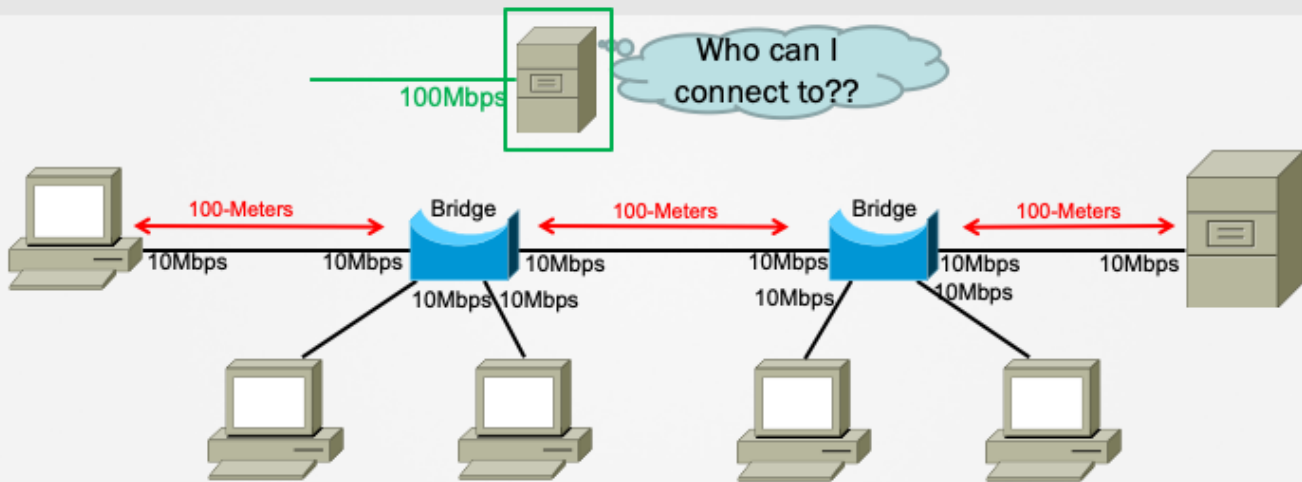
Evolution of Switching (2)



Ethernet Transceiver



Evolution of Switching (3)



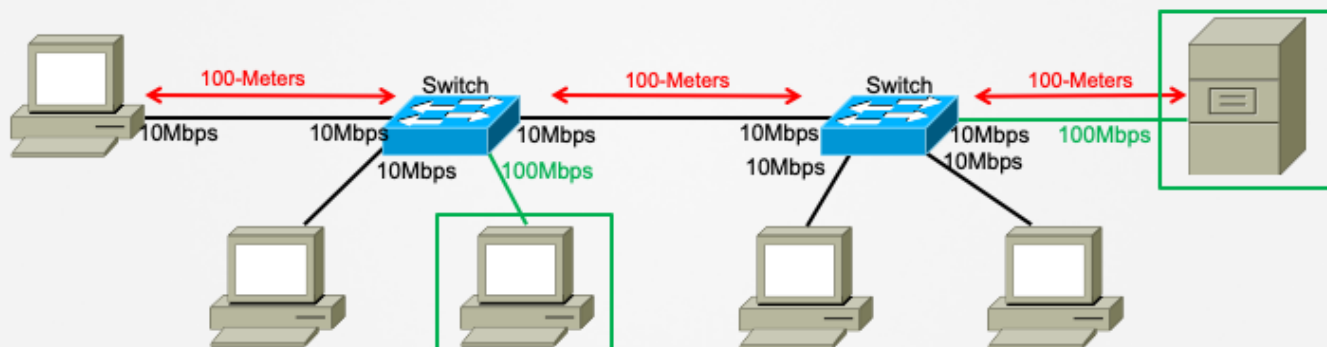
Copyright © www.ine.com



Bridge:

- Limited qty of ports
- Ports all the same speed

Evolution of Switching (4)



Copyright © www.ine.com



Intro to Switching

- » **Switch is a multiport bridge**
 - More ports than a bridge
 - Mixture of port speeds & types
- » **Forwards frames based on the MAC address table**
- » **Separates collision domain**
- » **Operates in data link layer**

MAC-Address Table

» Switch MAC Learning

- Based on Source MAC Address
- Addresses age out after inactivity-timer

» Switching forwarding

- Based on Destination MAC
- Broadcast/Multicast/Unknown flooding
- All ports initially in one, large, broadcast domain

Basic Switch Configuration



www.ine.com

Initial Tasks

» Perform initial configuration on Switch

- Hostname
- Enable password
- Console Password
- Banner
- “Convenience” commands
 - No ip domain-lookup
 - Logging synchronous

» Verify naming convention of ports on your switch

- Show ip interface brief

Basic Switch Configuration

- » **Switchports primarily used for switching Layer-2 Ethernet Frames.**
 - Don't natively support IP addressing
- » **Switch Management IP address configured on a logical interface.**
 - Switched Virtual Interface (SVI)
 - Initially in same broadcast domain as all physical ports.
 - May be disabled by default.

Copyright © www.ine.com



EXPLAIN: Logical versus physical interfaces

Talk about the differences between routers (interfaces) and switches (ports and SVIs) and where IP addresses can be configured.

Configuring Management Address

» Configuration commands

- Switch(config)# interface vlan 1
- Switch(config-if)# ip address <address> <subnet mask>
- Switch(config-if)# no shutdown
- Switch(config-if)# exit
- Switch(config)# ip default-gateway <default-gateway>

EXPLAIN: SVI must have associated physical ports that are “Up” in same VLAN for SVI to also be “Up”.

Verification

» Verification commands

- PING (Packet Internet Grouper)
- Traceroute

» Show commands

- Show ip interface brief
- Show running-configuration
- Show version
- Show mac address-table

Configuration Example (Switch-to-Host)

» Configuration on Sw1

- Switch> enable
- Switch# configure terminal
- Switch(config)# hostname Sw1
- Sw1(config)# interface GigabitEthernet1/0/5
- Sw1(config-if)# description **Connection to Bob Laptop**
- Sw1(config-if)# switchport mode access
- Sw1(config-if)# no shutdown

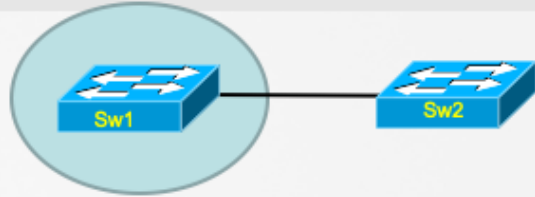


Explain how some switches (Layer-2) have “Switch” as hostname (default) and some (Multilayer Switches) may have “Router” as the default hostname.

Configuration Example (Switch-to-Switch)

» Configuration on Sw1

- Switch> enable
- Switch# configure terminal
- Switch(config)# hostname Sw1
- Sw1(config)# interface GigabitEthernet1/0/1
- Sw1(config-if)# description **Connection to Sw2**
- Sw1(config-if)# switchport mode dynamic desirable
- Sw1(config-if)# no shutdown



Explain how some switches (Layer-2) have “Switch” as hostname (default) and some (Multilayer Switches) may have “Router” as the default hostname.

Configuration Example (Switch-to-Switch)

» Configuration on Sw2

- Switch> enable
- Switch# configure terminal
- Switch(config)# hostname Sw2
- Sw2(config)# interface GigabitEthernet1/0/1
- Sw2(config-if)# description **Connection to Sw1**
- Sw2(config-if)# switchport mode dynamic desirable
- Sw2(config-if)# no shutdown



Explain how some switches (Layer-2) have “Switch” as hostname (default) and some (Multilayer Switches) may have “Router” as the default hostname.

Configuring Interface Ranges

» **“Interface Range” can be useful when applying the same command(s) across multiple interfaces**

- Switch(config)# interface range Fast0/1-7 , Fast0/12 , Gig1/1-2
- Switch(config-if-range)#no shutdown
- Switch(config-if-range)#switchport mode access

Viewing the MAC Address-Table

```
Switch#show mac address-table ?
  address      Address to lookup in the table
  aging-time   MAC address table aging parameters
  count        Number of MAC addresses in the table
  dynamic      List dynamic MAC addresses
  interface    List MAC addresses on a specific interface
  learning     Display learning on VLAN or interface
  move         MAC Move information
  multicast    List multicast MAC addresses
  notification MAC notification parameters and history table
  secure       List secure MAC addresses
  static       List static MAC addresses
  vlan        List MAC addresses on a specific vlan
  |           Output modifiers
  <cr>
```

Copyright © www.ine.com



CCNA Emphasis:

Address

Dynamic

Interface

Adding Static Entries

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#mac add
Switch(config)#mac address-table ?
  aging-time      Set MAC address table entry maximum age
  learning        Enable MAC table learning feature
  move            Move keyword
  notification    Enable/Disable MAC Notification on the switch
  static          static keyword

Switch(config)#mac address-table static ?
  H.H.H          48 bit mac address

Switch(config)#mac address-table static
```

Basic Troubleshooting

- » Check for correct cable type
- » Ensure `no shutdown` command in the interface (disabled by default)
- » For interconnected Access Ports, check for same VLAN
- » For interconnected Trunk, verify DTP compatibility modes

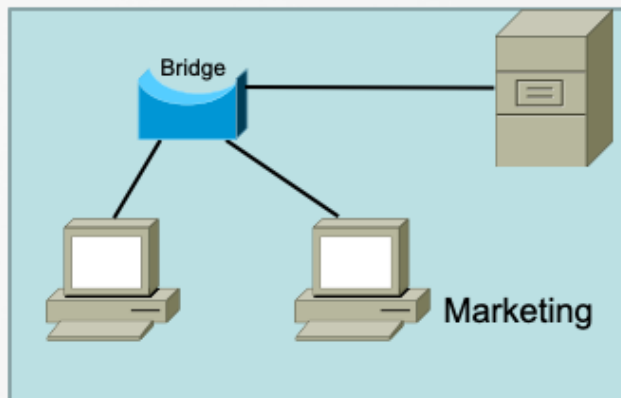
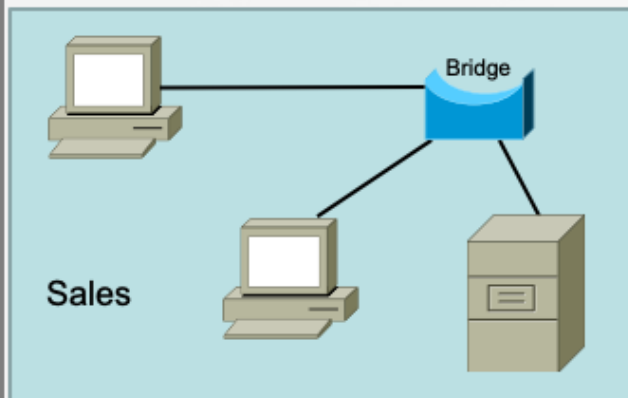
Using Virtual LANs (VLANs) For Network Segmentation



www.ine.com

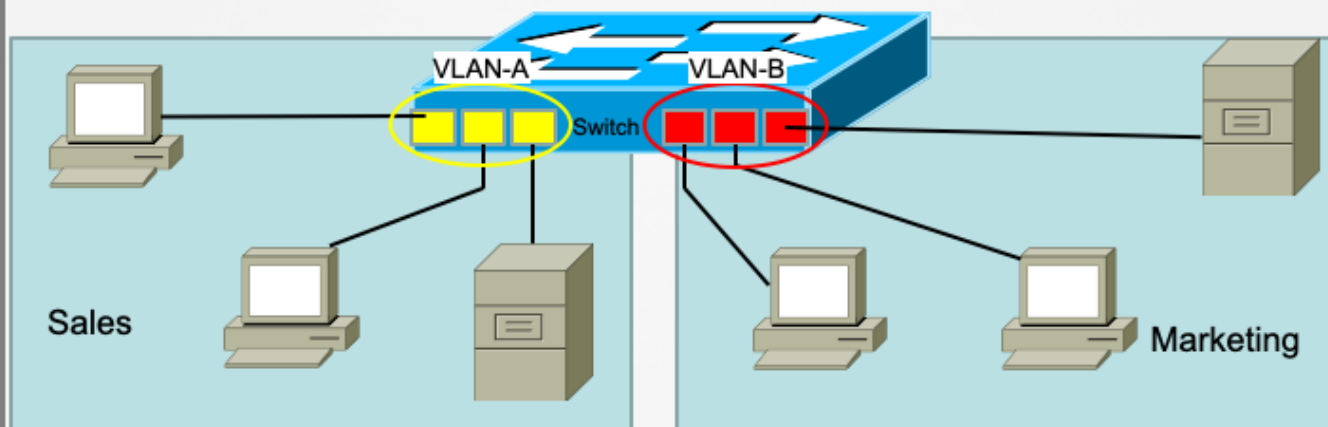
Why VLANs?

From this...



Why VLANs (2)?

To this...



Features

- » Separates broadcast domain
- » Provides better security
- » Controls broadcast like ARP
- » Provides hierarchical subnet usage

VLAN Ranges

- » VLAN range is 1-4094
- » 1-1001 are usable normal-range VLANs
- » 1002-1005 are reserved for token ring
- » 1006-4094 are extended-range VLANs

Configuring VLAN

» Legacy method with VLAN database

- Sw1# vlan database
- Sw1(vlan-database)# vlan <vlan-id>
- Sw1(vlan-database)# end

» Modern method of configuring VLAN

- Sw1(config)# vlan <vlan id>
- Sw1(config-vlan)# name <vlan name>

Configuring Access Ports

- » **Access Port = Switchport configured for only a single broadcast domain (VLAN).**

- » **Access port configuration**
 - Switch(config)# interface <interface>
 - Switch(config-if)# switchport mode access
 - Switch(config-if)# switchport access vlan <vlan-id>

Copyright © www.ine.com



- On some multilayer switches you may need to first enter the “switchport” command by itself – default = routed port.
- Switchport mode trunk command may not work without first entering “switchport trunk encapsulation” command.

Verifying VLAN

» Verification commands

- Sw1# show vlan <brief>
- Sw1# show interface <type><number> switchport

Extending VLANs With VLAN Trunks



www.ine.com

Port Types

» Trunk Port

- Can have two or more VLANs configured
- Can carry multiple VLAN information
- By default, all the VLAN traffic is allowed from a trunk port

Trunking Encapsulation

» 802.1Q

- Open standard
- All traffic except native VLAN is inserted with a 802.1q tag
- Support concept of native VLAN

Native VLAN

- » IEEE 802.1Q supported feature
- » Frame without tag is considered native VLAN traffic
- » Must match on both ends of the trunk
- » By default, native VLAN is 1
- » Can be changed using the **switchport trunk native vlan <vlan-id>** command

Configuring Trunking Encapsulation

» Static trunk configuration

- Switch(config)# interface <interface>
- Switch(config-if)#switchport trunk encapsulation dot1q
- Switch(config-if)#switchport mode trunk
- Switch(config-if)#end

Copyright © www.ine.com



- On some multilayer switches you may need to first enter the “switchport” command by itself – default = routed port.
- Switchport mode trunk command may not work without first entering “switchport trunk encapsulation” command.

Controlling VLAN operation over Trunks

- » By default, all VLANs active on the switch are carried across VLAN Trunks
- » For security or load-balancing reasons, sometimes it is desirable to prevent certain VLANs access to a Trunk
- » Configuration
 - Switch(config)# interface <interface>
 - Switch(config-if)#switchport trunk allowed vlan {add | all | except | remove} <vlan-list>
- » Example:
 - Switchport trunk allowed vlan 3
 - Switchport trunk allowed vlan except 3

Copyright © www.ine.com



- In the first example, ONLY VLAN-3 is allowed across the trunk. Everything else is implicitly denied.
- In the second example, all VLANs EXCEPT VLAN-3 are allowed across the trunk.

Verifying Trunk

» Verifying VLAN and trunking

- Switch# show vlan <brief>
- Switch# show interface trunk
- show interface status
- show interface <interface> switchport

Dynamic Trunking Protocol (DTP)



www.ine.com

Dynamic Trunking Protocol

- » Cisco proprietary feature that allows Cisco switches to negotiate trunk dynamically
- » Three modes:
 - Auto
 - On
 - Desirable
- » Desirable initiates the trunk, whereas Auto responds only

Implementing DTP

» Configuring DTP

- Switch(config-if)# switchport mode dynamic [desirable|auto]

» Disabling DTP

- Switch(config-if)# switchport nonegotiate

Verifying DTP

» Verification command

- Switch# show interface trunk
- Switch# show interface <interface> switchport

****** LAB TASK TIME: Introduction To Cisco Switching**

Mapping The Topology With CDP & LLDP



www.ine.com

Cisco Discovery Protocol (CDP)

- » Cisco proprietary
- » Layer 2 protocol for neighbor discovery
- » Provides information of platform, interface, IP address, and OS version
- » Helps with preparing network diagram

Configuration

» Enabling CDP

- Router(config)# cdp run
- Router(config)# cdp timer <seconds>

» Disabling CDP

- Router(config)# no cdp run
- Router(config-if)#no cdp enable

Default CDP timer is 60-seconds.

Verifying CDP

» Verification commands

- Router# show cdp neighbor
- Router# show cdp neighbor < interface >
- Router# show cdp neighbor <interface> detail

Link Layer Discovery Protocol (LLDP)

- » Open standard protocol, equivalent to CDP
- » Defined in IEEE 802.1ab
- » Media Endpoint Discovery (MED) is an LLDP enhancement for Voice over IP (VoIP) applications.
- » Limited to only 802.1 media types (i.e. Ethernet...but not WAN interfaces)
- » CDP and LLDP can be operational on same interface.

Copyright © www.ine.com



LLDP-MED frames used to support MED. Provide detailed information on Power over Ethernet, network policy, media endpoint location for Emergency Call Services and inventory.

-

Default is to only transmit LLDP unless an LLDP-MED frame is RECEIVED.

-

Mostly supported on Cisco switches...many routers don't support it.

LLDP Configuration

```
Device(config)# lldp run  
Device(config)# lldp holdtime 150  
Device(config)# lldp timer 15  
Device2(config)# interface ethernet 0/0  
Device2(config-if)# lldp transmit  
Device2(config-if)# end
```

Can't demonstrate this...our devices don't support it.

Verifying LLDP

```
Device1# show lldp traffic
LLDP traffic statistics:
  Total frames out: 20
  Total entries aged: 0
  Total frames in: 15
  Total frames received in error: 0
  Total frames discarded: 0
  Total TLVs unrecognized: 0
Device1# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID          Local Intf      Hold-time  Capability    Port ID
Device2            Et0/0          150       R             Et0/0
```