SPADVROUTE

Deploying Cisco Service Provider Advanced Network Routing

Course Administration Guide

Version 1.2

Part Number: 97-3433-01 and 97-3434-01

Americas Headquarters	Asia Pacific Headquarters	Europe Headquarters
Cisco Systems, Inc. San Jose, CA	Cisco Systems (USA) Pte. Ltd. Singapore	Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Table of Contents

Course High Level Design

Course Goal

The goal of the course is to to train service provider network professionals on the techniques to plan, implement, and monitor a scalable IP routing.

Job Tasks and Domain and Skill Objectives

These are the job tasks (domains and skill objectives from the audience, as well as job definition and job task analyses that will be taught and practiced in the course).

Domain 1	**Domain Name**	**Skill Objectives/Job Tasks**
1.00	Describe the operation of IP and data network	
1.08		Describe service provider principles and reference NGN architecture
1.09		Differentiate between LAN and WAN operation and features
Domain 2	**Domain Name**	**Skill Objectives/Job Tasks**
2.00	Implement and troubleshoot IPv4 and IPv6 addressing schemes	
2.03		Implement and troubleshoot IPv6 transitioning technologies
2.04		Design, implement, and troubleshoot types of IP addressing
Domain 4	**Domain Name**	**Skill Objectives/Job Tasks**

4.00	Implement and troubleshoot routed network technologies	
4.05		Design, implement, and troubleshoot OSPFv2 and OSPFv3
4.06		Design, implement, and troubleshoot IS-IS
4.10		Implement and troubleshoot BGP
4.11		Implement and troubleshoot multihomed BGP networks
4.14		Implement and troubleshoot BGP customer connectivity requirements (classify customer's routing table requirements)
4.15		Implement and troubleshoot BGP transit AS (functions, routing policy)
4.16		Implement and troubleshoot BGP route reflectors and confederations
4.17		Implement and troubleshoot advanced BGP configuration (limiting the number of prefixes, AS path prepending, peer group, route flap dampening, and scaling BGP)
Domain 5	**Domain Name**	**Skill Objectives/Job Tasks**
5.00	Implement and troubleshoot IP services	
5.01		Design, implement, and troubleshoot NAT (IPv4)
5.02		Describe NAT 444, NAT 64, and NAT PT
5.03		Implement and troubleshoot DHCP IPv4
5.04		Implement and troubleshoot DHCP IPv6
5.05		Analyze ICMPv4 and ICMPv6
5.06		Describe DNS
Domain 6	**Domain Name**	**Skill Objectives/Job Tasks**
6.00	Configure Cisco operating systems and platforms	
6.01		Configure Cisco IOS
6.02		Configure Cisco IOS XR

6.03		Configure Cisco IOS XE
Domain 9	**Domain Name**	**Skill Objectives/Job Tasks**
9.00	Implement and troubleshoot security in the network	
9.01		Design, implement, and troubleshoot management plane security
9.04		Design, implement, and troubleshoot control plane security
9.06		Implement and troubleshoot attack mitigation (BTSH and RTBH)
Domain 12	**Domain Name**	**Skill Objectives/Job Tasks**
12.00	Implement and troubleshoot multicast	
12.01		Describe multicast addresses
12.02		Describe multicast concepts (pruning, tree, application requirements, and RPF)
12.03		Implement and troubleshoot Auto-RP, BSR, static RP, anycast RP, and MSDP
12.04		Implement and troubleshoot IGMPv1, IGMPv2, IGMPv3, and snooping
12.05		Design, implement, and troubleshoot PIM SM, PIM DM, SSM, and BiDir-PIM
12.06		Implement and troubleshoot multicast security (IGMP and PIM filters)
12.07		Describe ICMPv6, IPv6 multicast, and MLD
Domain 13	**Domain Name**	**Skill Objectives/Job Tasks**
13.00	Implement high availability	
13.02		Implement and troubleshoot routing redundancy (Layer 3 high availability) (BFD, multi homing, and MPLS TE FRR)
13.03		Implement topology redundancy (link layer redundancy and Flex Link)
Domain 15	**Domain Name**	**Skill Objectives/Job Tasks**
15.00	Implement and troubleshoot VPN technologies	

15.01		Design, implement, and troubleshoot Layer 3 MPLS VPN, address family, and MP-BGP
15.05		Implement and troubleshoot AToM

Course Flow Diagram

This section illustrates the flow of the course.

	AM	PM
Day 1	Course Introduction Module 1: Service Provider Connectivity with BGP	Module 2: Scale Service Provider Network
Day 2	Module 3: Secure and Optimize BGP	Module 3 (cont.) Module 4: Multicast Overview
Day 3	Module 4 (cont.)	Module 5: Intradomain and Interdomain Multicast Routing
Day 4	Module 5 (cont.)	Module 5 (cont.)
Day 5	Module 6: Service Provider IPv6 Transition Implementations	Module 6 (cont.)

Required Classroom Environment

Room setup, layout, logistics, and equipment:

The course requires a typical classroom for instructor-led training delivery of Cisco training (for example, whiteboard, projector, Internet access, sufficient seating with tables).

Instructor Certification Requirements

Credentials to teach this version of the course are:

- Be a Cisco CCSI certified instructor in good standing
- Attend the SPADVROUTE v1.2 Train-the-Trainer (TTT) session (live or on-demand), or an SPADVROUTE v1.2 course delivered by a certified instructor
- Pass the 642-885 SPADVROUTE exam at the instructor cut score rate
- Be CCNP SP certified

General Information

This topic provides a high-level description of the lab environment.

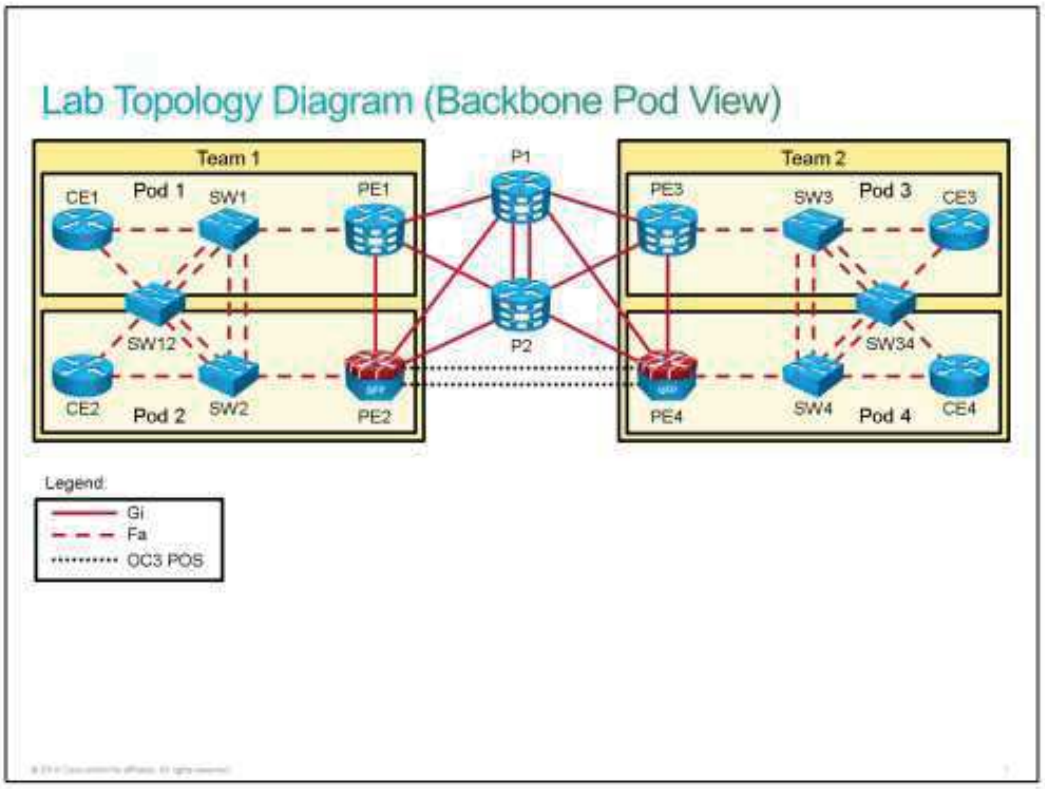
Laboratory Topology (Delivery)

This lab topology consists of two teams and four pods, with each team using two pods. Two students will usually configure one pod. Each pod has one switch and two routers. Two pods may share one additional switch, which is not used in this course. All teams share the same core routers (P1 and P2).

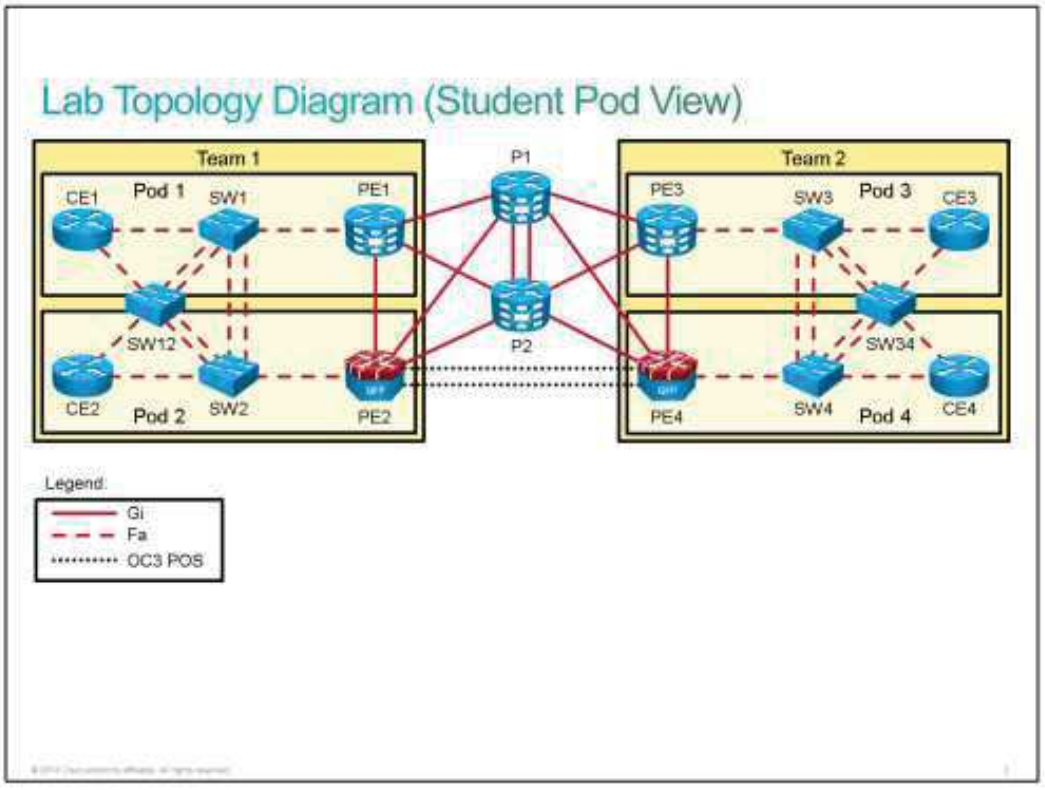
The CE routers in both pods are running Cisco IOS Software. The first pod within a team (pod 1 or 3) will work on PE routers running Cisco IOS XR Software, and the second pod within the same team (pod 2 or 4) will work on PE routers running Cisco IOS XE Software.

Laboratory Topology

Lab Topology Diagram (Backbone Pod View)



Lab Topology Diagram (Student Pod View)



Laboratory Equipment

These tables list the recommended equipment to support the lab activities. These tables assume a class size of eight students.

Description	Manufacturer	Part Number	Total Quantity
CE router: ISR 2901	Cisco	CISCO2901/K9	4
PE router running Cisco IOS XR: ASR 9006 with route processor and line card (with SFPs)	Cisco	ASR-9006-AC A9K-RSP-4G A9K-40GE-L	2
PE router running Cisco IOS XE: ASR 1001	Cisco	ASR1001-2XOC3POS	2
Switch: ME-3400E-24TS-M	Cisco	ME340x-METROACCESSK9-M	6
P1 router running Cisco IOS XR: ASR 9006 with route processor and line card (with SFPs)	Cisco	ASR-9006-AC A9K-RSP-4G A9K-40GE-L	1
P2 router running Cisco IOS XR: ASR 9001 with route processor and line card (with SFPs)	Cisco	ASR-9001-S	1

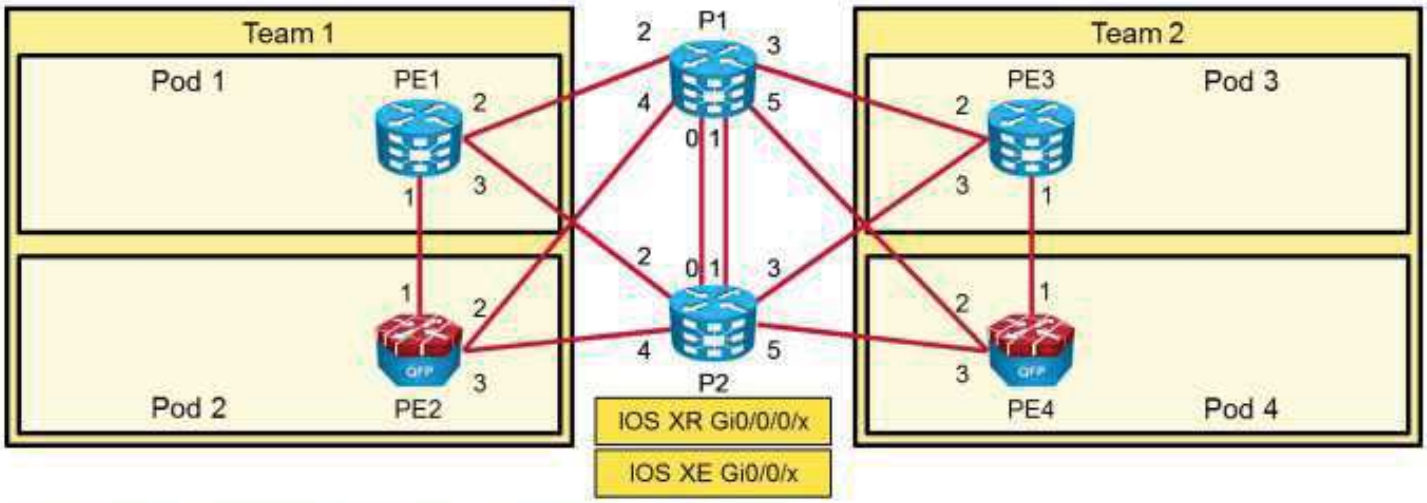
Software List

Description	Mfr.	Part Number	Total Quantity	Notes
Cisco IOS Software, ME340x Software , Version 12.2(60)EZ3, RELEASE SOFTWARE (fc2)	Cisco	ME340x-METROACCESSK9-M	6	me340x-metroaccessk9-mz.122-60.EZ3.bin
Cisco IOS Software, C2900 Software, Version 15.3(3)S2, RELEASE SOFTWARE (fc1)	Cisco	C2900-UNIVERSALK9-M	4	c2900-universalk9-mz.SPA.153-3.S2.bin
Cisco IOS Software, IOS-XE Software, Version 15.3(3)S, RELEASE SOFTWARE (fc1)	Cisco	X86_64_LINUX_IOSD-UNIVERSALK9-M	2	asr1001-universalk9.03.02.00.S.153-3.S.bin
Cisco IOS XR Software, Version 5.1.1	Cisco		4	ASR9K-iosxr-5.1.1.tar

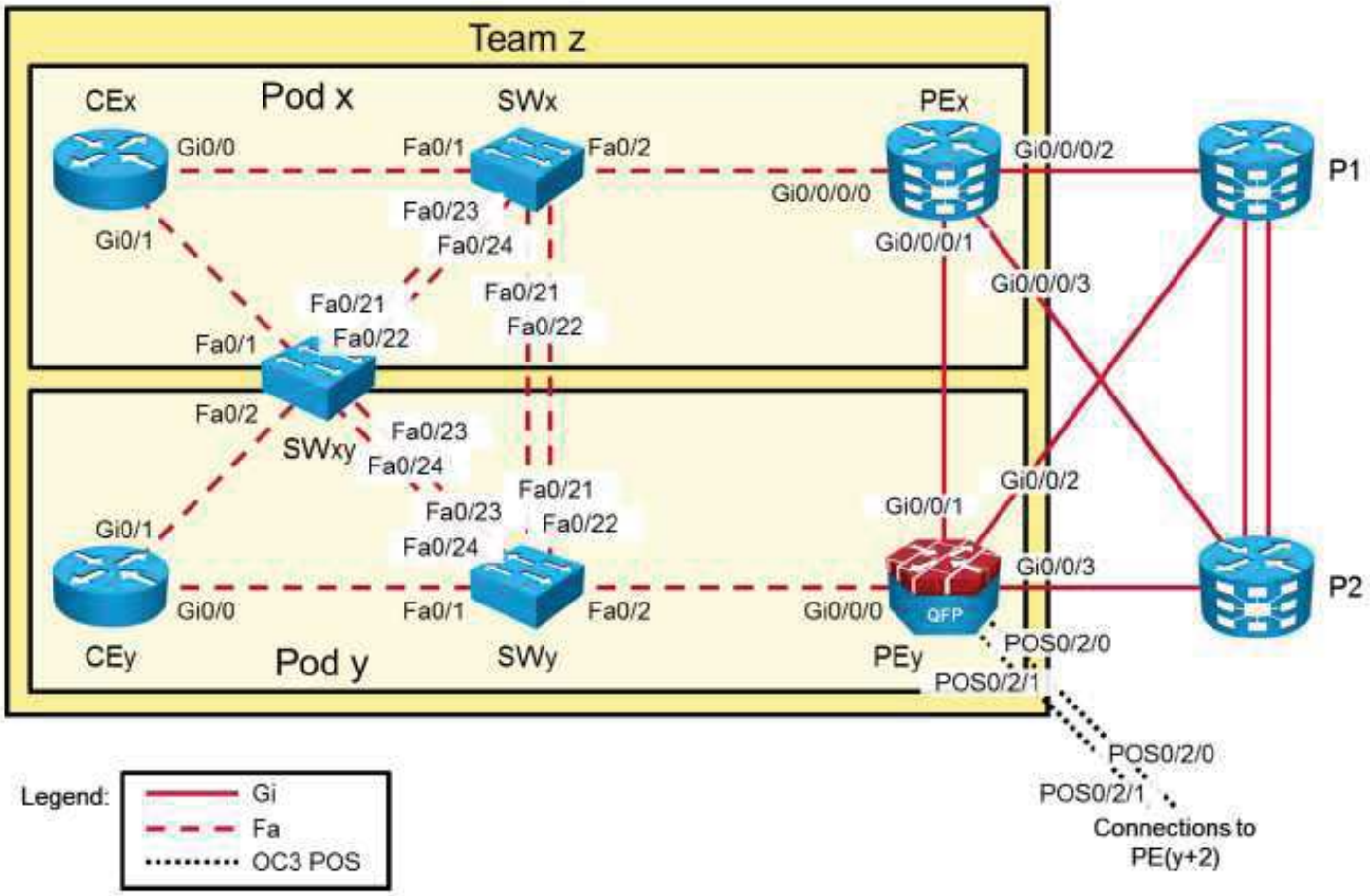
Initial Lab Build

This topic contains the information required to interconnect lab equipment.

The following figure shows core lab interface identification:



The following figure shows the pod lab interface identification:



General Lab Setup

This topic details the procedure to set up and configure the lab equipment at the beginning of each class.

Notes on Delivery Lab Equipment

On the Cisco IOS XR Software routers (Cisco ASR 9006 and Cisco ASR 9001), it is recommended to install all single-package PIEs that are included in the TAR file. It is required to install at least asr9k-mini-px-5.1.1 and asr9k-mpls-px-5.1.1 packages.

On the PE router running Cisco IOS XR (ASR 9006), PIE archive asr9k-mgbl-px.pie-5.1.1 must be located on disk0.

Development Lab Equipment Requirements

This section details the resources and requirements needed to develop and test the course labs.

Required Materials Laboratory Topology (Development)

Lab equipment for the development should be the same as the lab equipment for the delivery. The requirement is to have at least two development pods. The developer pod consist of two teams.

Notes on Development Lab Equipment

Lab development requires two developer pods or four teams. The pods can be remotely available to the developers. For the review, the pods must be remotely available for Cisco TEC reviewers to review the labs in a live environment.

The software and hardware list is the same as for production pods.

Course Management

Course Description

Deploying Cisco Service Provider Advanced Network Routing (SPADVROUTE) v1.2 is a course that provides network engineers and technicians with the knowledge and skills necessary to implement and support a service provider network.

The course focuses on using Cisco routers that are typically found in the service provider network and on various technologies that are used to offer different services to customers. Upon completing this course learners will be able to configure, verify, and troubleshoot advanced BGP configuration, IP multicasting, and IPv6 transition mechanisms.

The course also includes classroom activities with remote labs that are useful to gain practical skills on deploying Cisco IOS/IOS XE and Cisco IOS XR features to operate and support service provider network.

Full Title of Course	Deploying Cisco Service Provider Advanced Network Routing
Course Order Code	SPADVROUTE
Course Version Number	1.2
New Course?	no
Replaces	1.01

Curricula

The course is used in the following curricula, certifications, specializations, and learning maps:

Certifications:

- Cisco Certified Network Professional Service Provider (CCNP SP)

Curricula, specializations, and learning maps:

- N/A

Course Goal and Objectives

This topic describes the course goal and objectives.

Upon completing this course, you will be able to meet these objectives:

- Configure the service provider network to support multiple BGP connections with customers and other autonomous systems
- Describe common routing and addressing scalability issues in the service provider network
- Describe available BGP tools and features to secure and optimize the BGP routing protocol in a service provider environment
- Introduce IP multicast services and the technologies that are present in IP multicasting
- Introduce PIM-SM as the most current scalable IP multicast routing protocol
- Describe service provider IPv6 transition implementations

Target Audiences

This section specifies the primary and secondary target audiences of this course by job roles and notes the relevance to each job role.

Primary target audience:

- This course is intended primarily for network administrators, network engineers, network managers and systems engineers who would like to implement IP routing in service provider environments.

Secondary target audience:

- This course is intended for network designers and project or program managers. This course is also recommended to all individuals preparing for CCNP SP certification.

Target Theaters and Locales

The primary target theater for the course is:

- Americas

The secondary target theater is:

- EMEAR

The tertiary theater is:

- AJPC

Prerequisite Skills and Knowledge

This section lists the skills and knowledge that learners must possess to benefit fully from the course. It includes recommended Cisco learning offerings that the learners may complete to benefit fully from this course

The knowledge and skills that a learner must have before attending this course are as follows:

- Intermediate to advanced knowledge of Cisco IOS/IOS XE and Cisco IOS XR Software configuration
- Skills and knowledge equivalent to those learned in:
  - *Building Cisco Service Provider Next-Generation Networks, Part 1* (SPNGN1) v1.2 course
  - *Building Cisco Service Provider Next-Generation Networks, Part 2* (SPNGN2) v1.2 course
  - *Deploying Cisco Service Provider Network Routing* (SPROUTE) v1.2 course

Course Differences (Delta) Information

This section provides a summary of the most significant differences between the previous version, SPADVROUTE v1.01, and this one, SPADVROUTE v1.2.

Executive Summary

Overview

The course structure stays exactly as it is, what is added is an update to the latest software. There are new technologies added and EOL technologies are removed. All printouts in the student guide and labs are updated to reflect latest software versions.

Course Objectives

This table shows new features added to the course:

Module/Lesson/Lab	New Feature
SPADVROUTE modules and labs	Outputs updated with latest IOS/XE/XR versions.
SPADVROUTE labs	Steps added in the verification sections. Answer key added to each step.
SPADVROUTE Module 1 Lesson 1	Topics "Multihomed Customer Connectivity" and "Routing Schemes" text added.
SPADVROUTE Module 5 Lesson 1	Topics divided: "PIM-SM Neighbor Discovery", "PIM-SM Forwarding", "PIM-SM Joining", and "PIM-SM Registering"
SPADVROUTE Module 5 Lesson 1	Topics divided: "Enable PIM-SM", "Static RP", and "Finding PIM Neighbors and Checking RP Information"
SPADVROUTE Module 5 Lesson 2	Topics divided: "DF Election Process", "DF Election Messages", "Initial Election", "Winning the Election as DF", and "DF Loses Path to the RP"
SPADVROUTE Module 5 Lesson 3	Topics divided: "Multicast Service Provider Requirements", "MSDP Protocol", and "MSDP Concepts"
SPADVROUTE Module 5 Lesson 3	Topic "MSDP SA Message Processing" merged with topic "Steps to Process SA Messages"
SPADVROUTE Module 5 Lesson 3	Topics divided: "Configuring MSDP" and "Verifying MSDP"
SPADVROUTE Module 5 Lesson 4	Topic "PIMv2 BSR Advertisement Process" merged with topic "BSR Process"
SPADVROUTE Module 6 Lesson 1	Topics divided: "MLD Configuring" and "MLD Verifying"

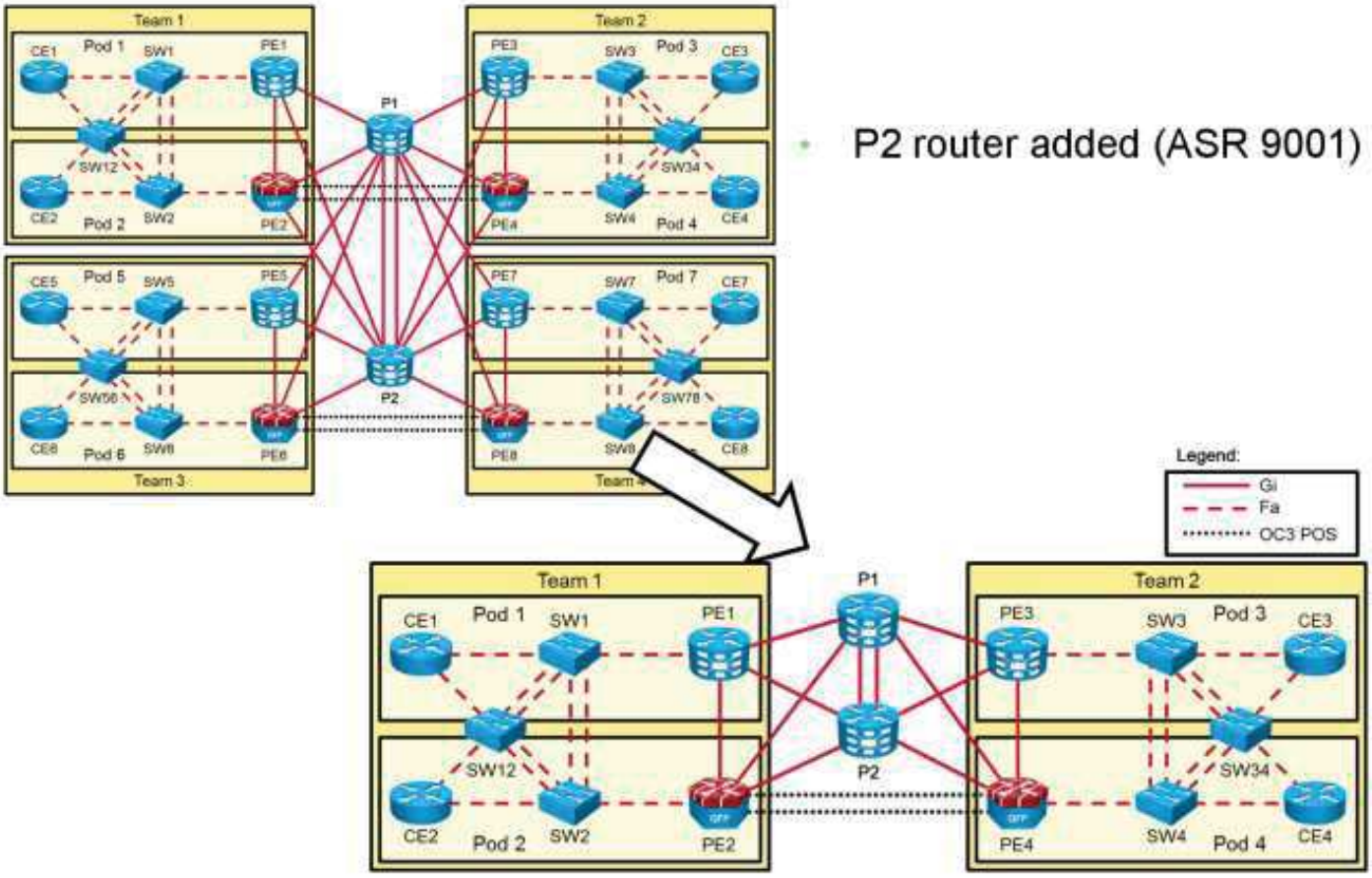
Lab Equipment Changes

This table provides a comparison of the lab equipment.

Devices	Description
CE routers (Cisco 2901): CE1, CE2, CE3, CE4	Upgraded software to Cisco IOS 15.3.3M(ED))
Pod switches (ME3400E): SW1, SW2, SW3, SW4	Upgraded software to Cisco IOS 12.2(60)EZ3(ED))
Shared switches (ME3400E): SW12, SW34	Upgraded software to Cisco IOS 12.2(60)EZ3(ED))
PE1/PE3 (ASR9006)	Upgraded software to Cisco IOS XR 5.1.1
PE2/PE4 (ASR1001)	Upgraded software to Cisco IOS XE 15.3(3)S2/3.10.2S)
P1 (ASR9006)	Upgraded software to Cisco IOS XR 5.1.1
P2 (ASR9001)	Upgraded software to Cisco IOS XR 5.1.1

Lab Topology Changes

These figures provide a comparison of the lab topologies.



- P2 router added (ASR 9001)

Configuration Files Summary

This topic details the course configuration files, which provide information about the starting condition of each lab

Configuration Filename	Comments
SPADVROUTE12_CE1_initial.txt	Initial configuration for CE1.
SPADVROUTE12_CE2_initial.txt	Initial configuration for CE2.
SPADVROUTE12_CE3_initial.txt	Initial configuration for CE3.
SPADVROUTE12_CE4_initial.txt	Initial configuration for CE4.
SPADVROUTE12_SW1_initial.txt	Initial configuration for SW1.
SPADVROUTE12_SW2_initial.txt	Initial configuration for SW2.
SPADVROUTE12_SW3_initial.txt	Initial configuration for SW3.
SPADVROUTE12_SW4_initial.txt	Initial configuration for SW4.
SPADVROUTE12_SW12_initial.txt	Initial configuration for SW12.
SPADVROUTE12_SW34_initial.txt	Initial configuration for SW34.
SPADVROUTE12_PE1_initial.txt	Initial configuration for PE1.
SPADVROUTE12_PE2_initial.txt	Initial configuration for PE2.
SPADVROUTE12_PE3_initial.txt	Initial configuration for PE3.
SPADVROUTE12_PE4_initial.txt	Initial configuration for PE4.
SPADVROUTE12_P1_initial.txt	Initial configuration for P1.
SPADVROUTE12_P2_initial.txt	Initial configuration for P2.

Course Instruction Details

Instructor Certification Requirements

Credentials to teach this version of the course are:

- Be a Cisco CCSI certified instructor in good standing
- Attend the SPADVROUTE v1.2 Train-the-Trainer (TTT) session (live or on-demand), or an SPADVROUTE v1.2 course delivered by a certified instructor
- Pass the 642-885 SPADVROUTE exam at the instructor cut score rate
- Be CCNP SP certified

Required Classroom Environment

Room setup, layout, logistics, and equipment:

The course requires a typical classroom for instructor-led training delivery of Cisco training (for example, whiteboard, projector, Internet access, sufficient seating with tables).

Detailed Course Flow

The course schedule specifies the recommended teaching time for each lesson, lab, and activity. Optionally, indicate breaks and starting and ending times for each day.

Day 1: Service Provider Connectivity with BGP, Scale Service Provider Network		
	8:30–9:00 (0830–0900)	Course Introduction
	9:00–10:00 (0900–1000)	Lesson 1-1: Defining Customer-to-Provider Connectivity Requirements
	10:00–10:15 (1000–1015)	Break
	10:15–12:15 (1015–1215)	Lesson 1-2: Connecting a Customer to Service Provider
	12:15 –1:15 (1215–1315)	**Lunch**
	1:15 –2:00 (1315–1400)	Lesson 2-1: Scaling BGP in Service Provider Networks
	2:00–3:30 (1400–1530)	Lesson 2-2: Introducing BGP Route Reflectors and Confederations
	3:30–3:45 (1530–1345)	Break
	3:45–4:45 (1545–1645)	Lab 1: Implement BGP Route Reflectors
	4:45 (1645)	**Day ends**
Day 2: Secure and Optimize BGP, Multicast Overview		
	8:00–8:30 (0800–0830)	**Review of Day 1**
	8:30–10:00 (0830–1000)	Lesson 3-1: Implementing Advanced BGP Operations
	10:00–10:15 (1000–1015)	Break
	10:15–11:15 (1015–1115)	Lab 2: Implement BGP Security Options
	11:15–12:30 (1115–1230)	Lesson 3-2: Improving BGP Convergence
	12:30 –1:30 (1230–1330)	**Lunch**
	1:30–2:45 (1330–1445)	Lesson 3-3: Improving BGP Configuration Scalability
	2:45–4:15 (1445–1615)	Lab 3: Improve BGP Scalability
	4:15–4:30 (1615–1630)	Break
	4:30–6:00 (1630–1800)	Lesson 4-1: Introducing IP Multicast
	6:00 (1800)	**Day ends**

Day 3: Multicast Overview, Intradomain and Interdomain Multicast Routing		
	8:00–8:30 (0800–0830)	**Review of Day 2**
	8:30–10:00 (0830–1005)	Lesson 4-2: Defining Multicast Distribution Trees and Forwarding
	10:00–10:15 (1000–1015)	Break
	10:15–11:15 (1015–1115)	Lesson 4-3: Defining Multicast on the LAN
	11:15–11:45 (1115–1145)	Lab 4: Implement Layer 2 and Layer 3 Multicast
	11:45–12:45 (1145–1245)	**Lunch**
	12:45–1:30 (1245–1330)	Lesson 4-4: Populating the Mroute Table
	1:30 –3:45 (1330–1545)	Lesson 5-1: Introducing PIM-SM Protocol
	3:45–4:00 (1545–1600)	Break
	4:00–5:00 (1600–1700)	Lab 5: Enable and Optimize PIM-SM
	5:00 (1700)	**Day ends**
Day 4: Intradomain and Interdomain Multicast Routing		
	8:00–8:30 (0830–0830)	**Review of Day 3**
	8:30–9:30 (0830–0930)	Lesson 5-2: Implementing PIM-SM Enhancements
	9:30–9:45 (0930–0945)	Break
	9:45–11:00 (0945–1100)	Lab 6: Implement PIM-SM Enhancements
	11:00–12:30 (1100–1230)	Lesson 5-3: Implementing Interdomain IP Multicast
	12:30–1:30 (1230–1330)	**Lunch**
	1:30 –3:00 (1330–1500)	Lesson 5-4: Identifying Rendezvous Point Distribution Solutions
	3:00–3:15 (1500–1515)	Break
	3:15–4:15 (1515–1615)	Lab 7: Implement Rendezvous Point Distribution

	4:15 (1615)	**Day ends**
Day 5: Service Provider IPv6 Transition Implementations		
	8:00–8:30 (0800–0830)	**Review of Day 4**
	8:30–10:30 (0830–1030)	Lesson 6-1: Introducing IPv6 Services
	10:30–10:45 (1030–1045)	Break
	10:45–11:30 (1045–1130)	Lab 8: Implement a DHCPv6 Server with Prefix Delegation
	11:30–12:00 (1130–1200)	Lab 9: Implement IPv6 Multicasting
	12:00–1:00 (1200–1300)	**Lunch**
	1:00–3:00 (1300–1500)	Lesson 6-2: Defining IPv6 Transition Mechanisms
	3:00–3:15 (1500–1515)	Break
	3:15–4:00 (1515–1600)	Lab 10: Implement Tunnels for IPv6
	4:00–4:30 (1600–1630)	Lesson 6-3: Deploying IPv6 in the Service Provider Network
	4:30–5:30 (1630–1730)	**Wrap-up**

Course Evaluation

Curriculum Evaluation

Effectiveness of the course will be evaluated at these Levels of Kirkpatrick's performance evaluation.

- Level 1: Reaction to the course
  - Course effects: This assessment level gauges learner satisfaction, that is, feedback from participants regarding their levels of satisfaction with the offering. This assessment will consist of the Cisco standard program evaluation and will be completed by the learner.
  - Course evaluation: Required (via MTM).
- Level 2: Learning retained
  - Course effects: This assessment level tests for learner achievement following a portion, or all, of an instructional offering. The strategy for learner assessment calls for the use of written tests in support of the instructional program. Written tests will be administered in accordance with L@C standards through proctored certification exams. This assessment will consist of the laboratory exercises and the Cisco Certification Exam.
  - Course evaluation: Required.
- Level 3: Performance changes after the course
  - Course effects: N/A
  - Course evaluation: N/A
- Level 4: Results on the job, after the course
  - Course effects: N/A
  - Course evaluation: N/A

Course Outlines

High Level Course Outline

This subtopic provides an overview of how the course is organized. The course contains these components:

- Module 1: Service Provider Connectivity with BGP
- Module 2: Scale Service Provider Network
- Module 3: Secure and Optimize BGP
- Module 4: Multicast Overview
- Module 5: Intradomain and Interdomain Multicast Routing
- Module 6: Service Provider IPv6 Transition Implementations
- Hardware Lab 1: Implement BGP Route Reflectors
- Hardware Lab 2: Implement BGP Security Options
- Hardware Lab 3: Improve BGP Scalability
- Hardware Lab 4: Implement Layer 2 and Layer 3 Multicast
- Hardware Lab 5: Enable and Optimize PIM-SM
- Hardware Lab 6: Implement PIM-SM Enhancements
- Hardware Lab 7: Implement Rendezvous Point Distribution
- Hardware Lab 8: Implement a DHCPv6 Server with Prefix Delegation
- Hardware Lab 9: Implement IPv6 Multicasting
- Hardware Lab 10: Implement Tunnels for IPv6

Detailed Course Outline

This in-depth outline of the course structure lists each module, lesson, and topic.

Course Introduction

The Course Introduction provides learners with the course objectives and prerequisite learner skills and knowledge. The Course Introduction presents the course flow diagram and the icons that are used in the course illustrations and figures. This course component also describes the curriculum for this course, providing learners with the information that they need to make decisions regarding their specific learning path.

- Overview
- Course Goal and Objectives
- Course Flow
- Additional References
- Your Training Curriculum

Module 1: Service Provider Connectivity with BGP

Objective: Describe different connectivity types and routing options between a service provider and a customer

Lesson 1: Defining Customer-to-Provider Connectivity Requirements

Objective: Define the requirements to connect customer networks to the Internet in a service provider environment

This lesson includes these topics:

- Cisco IP NGN Architecture
- Customer-to-Service Provider Connectivity Types
- Single-Homed Customer Connectivity
- Dual-Attached Customer Connectivity
- Multihomed Customer Connectivity
- Routing Schemes
- Single-Homed Customer Routing Schemes
- Dual-Attached Customer Routing Schemes
- Multihomed Customer Routing Schemes
- Addressing and AS Number Allocation
- Single-Homed Customer IP Addressing Schemes
- Dual-Attached Customer IP Addressing and AS Number Schemes
- Multihomed Customer IP Addressing and AS Number Schemes

Lesson 2: Connecting a Customer to a Service Provider

Objective: Describe a service provider-aided routing policy using BGP in multihomed scenarios using a primary and a backup path

This lesson includes these topics:

- Implementing Customer Connectivity Using Static Routing
- Single-Homed Customer Using Static Routing and a Single IP Address
- Single-Homed Customer Using Static Routing and Multiple IP Addresses
- Dual-Attached Customers Using Static Routing in a Primary and Backup Scenario
- Dual-Attached Customers Using Static Routing in a Load-Balancing Scenario
- Connecting a Dual-Attached Customer to a Single Service Provider
- Conditional BGP Advertising
- BGP Configurations on the Service Provider PE Router
- Removing a Private AS Number

- Dual-Attached Customers Using BGP
- Service Provider Migrations Using Local AS
- Dual-Attached Customers Using BGP in a Primary and Backup Scenario
- Dual-Attached Customers Using BGP in a Load-Balancing Scenario
- Connecting a Multihomed Customer to Multiple Service Providers
- Customer-Implemented BGP Routing Policies in a Primary and Backup Scenario
- Customer-Implemented BGP Routing Policies in a Load-Balancing Scenario
- Service Provider-Aided BGP Routing Policy in a Primary and Backup Scenario

Module 2: Scale Service Provider Network

Objective: Describe routing and addressing issues that may arise in a typical service provider network

Lesson 1: Scaling BGP in Service Provider Networks

Objective: Describe common routing and addressing scalability issues in service provider networks

This lesson includes these topics:

- Cisco IP NGN Infrastructure Layer
- Service Provider Network Routing Protocols
- Route Propagation in Service Provider Networks
- Route Information Exchange Between Service Providers
- Route Information Exchange with Customers
- BGP Next-Hop Resolution with IGP
- Scaling BGP Routing
- Scaling Addressing in Service Provider Core Networks
- BGP Policy Accounting

Lesson 2: Introducing BGP Route Reflectors and Confederations

Objective: Describe the function of route reflectors and confederations in a BGP environment, and list the steps needed to implement BGP route reflectors

This lesson includes these topics:

- BGP Route Reflectors and BGP Confederations
- BGP Split-Horizon Rule
- Steps of Route Propagation in a Route Reflector-Enabled Network
- Redundant Route Reflectors
- Route Reflector Clusters
- Additional Loop-Prevention Mechanism
- Network Design with BGP Route Reflectors
- Hierarchical Route Reflectors
- Implementing BGP Route Reflectors
- BGP Confederations Overview
- AS Path Propagation Within BGP Confederation
- Intraconfederation EBGP Session Properties

Hardware Lab 1: Implement BGP Route Reflectors

This activity includes these tasks:

- Verify the Existing BGP Sessions
- Configure a Route Reflector and Internal BGP Session
- Restrict Route Propagation to a Client

Module 3: Secure and Optimize BGP

Objective: Describe and use BGP tools and features that are available to secure and optimize the BGP routing protocol in a service provider environment

Lesson 1: Implementing Advanced BGP Operations

Objective: Implement BGP security and optimization options

This lesson includes these topics:

- Cisco IP NGN Infrastructure Layer
- Threats in Service Provider Environments
- BGP Countermeasures Overview
- BGP Route Limiting
- BGP Neighbor Authentication
- BGP TTL Security Check
- Control Plane Policing
- BGP Neighbor Authentication, TTL Security, and CoPP Configuration
- Remote-Triggered Black-Hole Filtering
- Destination-Based RTBH
- Source-Based RTBH
- Cisco Nonstop Forwarding
- Cisco Nonstop Routing
- BGP NSF and NSR Configuration
- BGP Process Restart
- Summary

Hardware Lab 2: Implement BGP Security Options

This activity includes these tasks:

- Implement BGP Neighbor Authentication Using Passwords
- Implement BGP Neighbor Authentication Using Key Chains
- Enable BGP TTL Security Check
- Enable CoPP
- Enable RTBH Filtering

Lesson 2: Improving BGP Convergence

Objective: Improve convergence in BGP networks using different features

This lesson includes these topics:

- BGP Route-Dampening Overview
- Configuring BGP Route Dampening
- Verifying BGP Route Dampening
- BGP Convergence
- BGP Processes
- Improving BGP Convergence
- Distributed BGP
- PMTU Discovery
- PMTU Increasing Input Queue Depth
- PMTU Discovery, Hold Queue, and Distributed BGP Configurations
- BGP Prefix Independent Convergence
- Bidirectional Forwarding Detection for BGP
- BGP Timers and Intervals
- Summary

Lesson 3: Improving BGP Configuration Scalability

Objective: Configure BGP to limit the number of prefixes that are received from a neighbor and describe how to use BGP peer and configuration templates and how to use route dampening to minimize the impact of unstable routes

This lesson includes these topics:

- BGP Peer Groups Overview
- BGP Peer Groups as Performance Tool
- BGP Peer Groups Configuration
- BGP Peer Groups Limitation
- BGP Dynamic Update Groups
- BGP Peer Templates Overview
- BGP Configuration Templates
- BGP Configuration Templates Inheritance
- Configuring BGP Configuration Templates
- BGP Configuration Templates Verification
- BGP Peer Templates
- BGP Peer Templates Inheritance

- BGP Peer Templates Configuration
- BGP Peer Templates Verification
- Summary

Hardware Lab 3: Improve BGP Scalability

This activity includes these tasks:

- Implement the BGP Configuration and Peer Templates
- Limit the Number of Prefixes Received from a BGP Neighbor
- Improve BGP Convergence by Changing the BGP Scan and Advertisement Interval
- Implement BGP Route Dampening

Module 4: Multicast Overview

Objective: Understand IP multicast services and the technologies that are present in IP multicasting

Lesson 1: Introducing IP Multicast

Objective: List various types of IP multicast applications and explain their requirements

This lesson includes these topics:

- IP Multicast Benefits and Caveats
- Multicast Operations High-Level Overview
- Multicast Advantages and Disadvantages
- Multicast Application Types
- IP Multicast Group Address
- IP Multicast Basic Addressing
- RFC 2770 and SSM Addressing
- Multicast Session Directory
- IP Multicast Service Model
- Functions of a Multicast Network
- Multicast Source and Receivers
- Multicast Protocols
- Multicast Forwarding and RPF Check
- Multicast Scoping

Lesson 2: Defining Multicast Distribution Trees and Forwarding

Objective: Explain how protocols are building the IP multicast distribution tree, and review the functions and methods that are performed within the IP multicast-enabled network in order to ensure the delivery path from multicast sources to receivers

This lesson includes these topics:

- RPF Check
- Types of Multicast Distribution Trees
- Multicast Distribution Tree Identification
- Multicast Protocols Overview
- PIM Dense Mode and Sparse Mode High-Level Overview
- Intradomain Multicast Routing Protocols
- Interdomain Multicast Routing Protocols
- Multicast High-Availability Options
- Multicast NSF with Stateful Failover

- PIM Triggered Joins
- IGMP Overview
- IGMPv1 Overview
- IGMPv2 Overview
- IGMPv3 Overview
- Summary

Lesson 3: Defining Multicast on the LAN

Objective: Identify IP multicast issues on a data link layer

This lesson includes these topics:

- Mapping Multicast IP Addresses to MAC Addresses
- Layer 2 Multicast Frame Switching
- Implementing IGMP
- IGMP join-group and static-group
- IGMPv3 Host Stack Feature
- Configuring IGMP Snooping
- IGMP Fast-Leave in a Switch
- PIM Snooping

Hardware Lab 4: Implement Layer 2 and Layer 3 Multicast

This activity includes these tasks:

- Enable IGMP and MLD
- Verify IGMP Snooping

Lesson 4: Populating the Mroute Table

Objective: Explain the purpose of the multicast route table and routing protocol supported for mroute table population

This lesson includes these topics:

- The Mroute Table
- Multiprotocol BGP
- MP-BGP Capability Negotiation
- MP-BGP Multicast Configuration
- MP-BGP Multicast Verification

Module 5: Intradomain and Interdomain Multicast Routing

Objective: Implement intradomain and interdomain multicast routing in the service provider environment

Lesson 1: Introducing PIM-SM Protocol

Objective: Describe the principles of operation of PIM-SM and explain various control mechanisms in maintaining the distribution tree

This lesson includes these topics:

- PIM-SM in the Cisco IP NGN Infrastructure Layer
- PIM-SM Shared Tree Join
- PIM-SM Sender Registration
- PIM-SM SPT Switchover
- PIM-SM Packets
- PIM-SM State Information
- PIM-SM State Maintenance
- Multicast Routing Table
- PIM-SM OIL Rules
- PIM-SM State Flags
- PIM-SM Neighbor Discovery
- PIM-SM Forwarding
- PIM-SM Joining
- PIM-SM Registering
- PIM-SM Registering: Receiver Joins First Scenario
- PIM-SM Registering: Source Starts First Scenario
- PIM-SM Registering: Receivers Along the SPT Scenario
- PIM-SM SPT Switchover Overview
- PIM-SM SPT Switchover Process
- PIM-SM Shared Tree Pruning Overview
- PIM-SM Pruning Shared Tree Process
- PIM-SM SPT Pruning Overview
- PIM-SM Pruning SPT Process
- Enable PIM-SM
- Static RP
- Finding PIM Neighbors and Checking RP Information
- Troubleshooting PIM-SM Guidelines
- Summary

Hardware Lab 5: Enable and Optimize PIM-SM

This activity includes these tasks:

- Implement PIM-SM
- Shared Tree Formation—Receivers
- Shared Tree Formation—Sources
- Switching to the SPT

Lesson 2: Implementing PIM-SM Enhancements

Objective: Describe SSM, PIM-SM bidirectional mode, and IGMPv3

This lesson includes these topics:

- Source Specific Multicast
- SSM Scenario
- SSM with IGMPv3
- SSM Mapping
- Configuring SSM
- Bidirectional PIM
- Bidirectional PIM Sources and Receivers
- Bidirectional PIM Traffic Flow
- Forwarding and Tree Building Process
- DF Election Process
- DF Election Messages
- Initial Election
- Winning the Election as DF
- DF Loses Path to the RP
- DF Dies and Other Metric Changes
- Configuring Bidirectional PIM

Hardware Lab 6: Implement PIM-SM Enhancements

This activity includes these tasks:

- Implement PIM-SSM

Lesson 3: Implementing Interdomain IP Multicast

Objective: Implement MSDP in the interdomain environment

This lesson includes these topics:

- Service Provider Multicast Requirements
- GLOP—Static Allocation of 233/8
- SSM Role in Interdomain IP Multicast
- MSDP Role in Interdomain IP Multicast
- Multicast Service Provider Requirements
- MSDP Protocol
- MSDP Concepts
- MSDP Neighbor Relationship
- MSDP Messages
- MSDP SA Message Processing
- MSDP SA Message Origination
- MSDP MD5 Password Authentication
- Configuring MSDP
- Verifying MSDP

Lesson 4: Identifying Rendezvous Point Distribution Solutions

Objective: Introduce the need for dynamic RP information distribution, and list mechanisms for dynamic RP distribution

This lesson includes these topics:

- Static RP Disadvantages
- Dynamic RP Discovery Mechanisms
- RP Placement
- Auto-RP
- Auto-RP Candidate RPs
- Auto-RP Mapping Agents
- Auto-RP Other Routers
- Auto-RP Configuration
- Auto-RP Troubleshooting
- Auto-RP Scoping
- Securing Auto-RP Using a Boundary
- PIMv2 Bootstrap Router
- PIMv2 BSR Candidate RPs

- PIMv2 BSRs
- PIMv2 BSR Election
- Other PIMv2 BSR Routers
- PIMv2 BSR Advertisement Process
- PIMv2 BSR Configuration
- PIMv2 BSR Verification
- PIMv2 BSR Troubleshooting
- BSR Hop-by-Hop Flooding
- Constraining BSR Messages
- Anycast RP
- Anycast RP Example
- Anycast RP Configuration
- Anycast RP Configuration Guidelines

Hardware Lab 7: Implement Rendezvous Point Distribution

This activity includes these tasks:

- Enable OSPF Routing
- Enable BSR
- Enable Anycast RP

Lesson 5: Module Summary

Module 6: Service Provider IPv6 Transition Implementations

Objective: Transition IPv6 implementations in a typical provider network (P-network)

Lesson 1: Introducing IPv6 Services

Objective: Describe DNS and DHCP support for IPv6 and support for QoS and multicast in the IPv6 network

This lesson includes these topics:

- Multicast in the Cisco IP NGN Infrastructure Layer
- IPv6 Multicast Address Format
- IPv6 Multicast Address Scope
- IPv6 Solicited-Node Multicast Address Format
- IPv6 Multicast Address with a Global Scope
- IPv4 vs. IPv6 Multicast Comparison
- PIMv6 Overview
- Embedding the RP Address in an IPv6 Multicast Address
- IPv6 Multicast Routing Configuration
- IPv6 Multicast Listener Discovery
- MLDv1 Messages
- MLDv1 General Query Message
- MLDv1 Report Message
- MLDv1 Done Message
- MLDv1 Address-Specific Query Message
- MLDv2 Protocol
- MLD Access Groups and Group Limits
- MLD Configuration
- MLD Verification
- MLD Join-Group and Static-Group
- MLD Snooping
- DNS and DHCPv6 in the Cisco IP NGN Infrastructure Layer
- DNS IPv6 Support
- Dynamic DNS
- DHCPv6 Operations
- DHCPv6 Server Router Configuration
- DHCPv6 Lite Operation (Stateless DHCPv6)
- DHCPv6 Prefix Delegation

- DHCPv6 Verification
- QoS in the Cisco IP NGN Infrastructure Layer
- IPv6 Header Fields Used for QoS
- IPv6 Traffic Class Field
- IPv6 Flow Label Field
- IPv6 QoS Configuration
- Cisco IOS Software Features
- Cisco IOS IPv6 Telnet and SSH Server and Client Support
- Cisco IOS IPv6 Tools
- Cisco Discovery Protocol Support for IPv6
- Cisco Express Forwarding for IPv6
- IP Service Level Agreement (SLA) for IPv6
- Configuring IP SLA

Hardware Lab 8: Implement a DHCPv6 Server with Prefix Delegation

This activity includes these tasks:

- Configure a Prefix Delegation DHCPv6 Server and Client
- Configure DHCPv6 Lite Server

Hardware Lab 9: Implement IPv6 Multicasting

This activity includes these tasks:

- Create a New Loopback Interface and Verify Connectivity
- Implement IPv6 Multicast Using Embedded RPs

Lesson 2: Defining IPv6 Transition Mechanisms

Objective: Describe IPv6 transition mechanisms and which methods are most effective in the service provider network

This lesson includes these topics:

- Dual Stack, CGN, and NAT64
- Dual-Stack Operations Overview
- Dual-Stack Considerations
- Dual Stack with Carrier-Grade NAT
- NAT444
- Carrier-Grade NAT on Cisco Routers

- NAT64
- DNS64
- Stateless NAT64
- Stateful NAT64
- Stateless versus Stateful NAT64 Comparison
- Stateful NAT64 Configuration on ASR 1000
- Static, Stateful NAT64 Configuration on ASR 1000
- IPv6 Tunneling Mechanisms
- Manually Configured Tunnels
- GRE Tunnels
- 6in4 Tunnels
- 6in4 Tunnel Configuration
- 6to4 Automatic Tunnels
- 6to4 Considerations
- 6to4 Configuration
- 6RD Automatic Tunnels
- 6RD Considerations
- 6RD Configuration

Hardware Lab 10: Implement Tunnels for IPv6

This activity includes these tasks:

- Configure a Static IPv6-in-IPv4 Tunnel
- Configure Dynamic 6RD Tunnels

Lesson 3: Deploying IPv6 in the Service Provider Network

Objective: Describe the deployment strategies that service providers are facing when deploying IPv6

This lesson includes these topics:

- IPv6 Service Provider Deployment
- Dual-Stack Option
- Dual Stack Pros and Cons
- Tunneling of IPv6 in IPv4
- Tunneling of IPv6 in IPv4 Pros and Cons
- Key Service Provider Strategies
- IPv6 Services
- IPv6 Address Allocation

- IPv6 Address Selection Guidelines
- IPv6 Broadband Access Services
- FTTH Access Architecture
- DSL Access Architecture
- Cable Access Architecture

Lab Setup

General Information

This topic provides a high-level description of the lab environment.

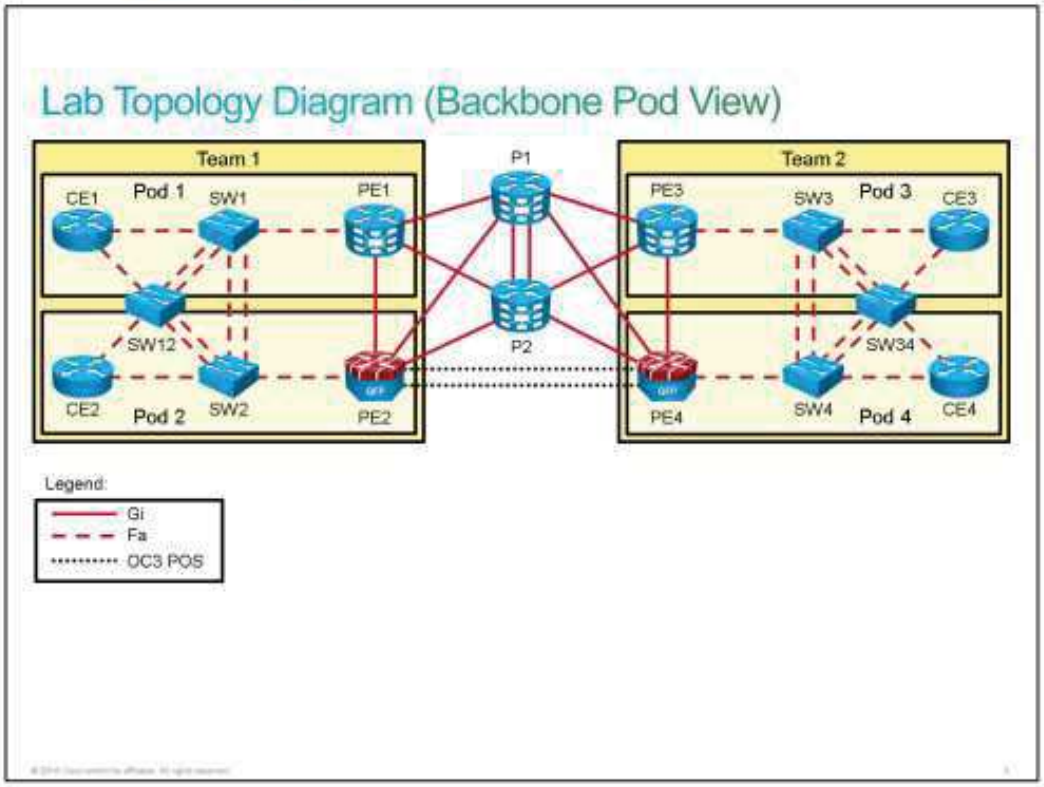
Laboratory Topology (Delivery)

This lab topology consists of two teams and four pods, with each team using two pods. Two students will usually configure one pod. Each pod has one switch and two routers. Two pods may share one additional switch, which is not used in this course. All teams share the same core routers (P1 and P2).

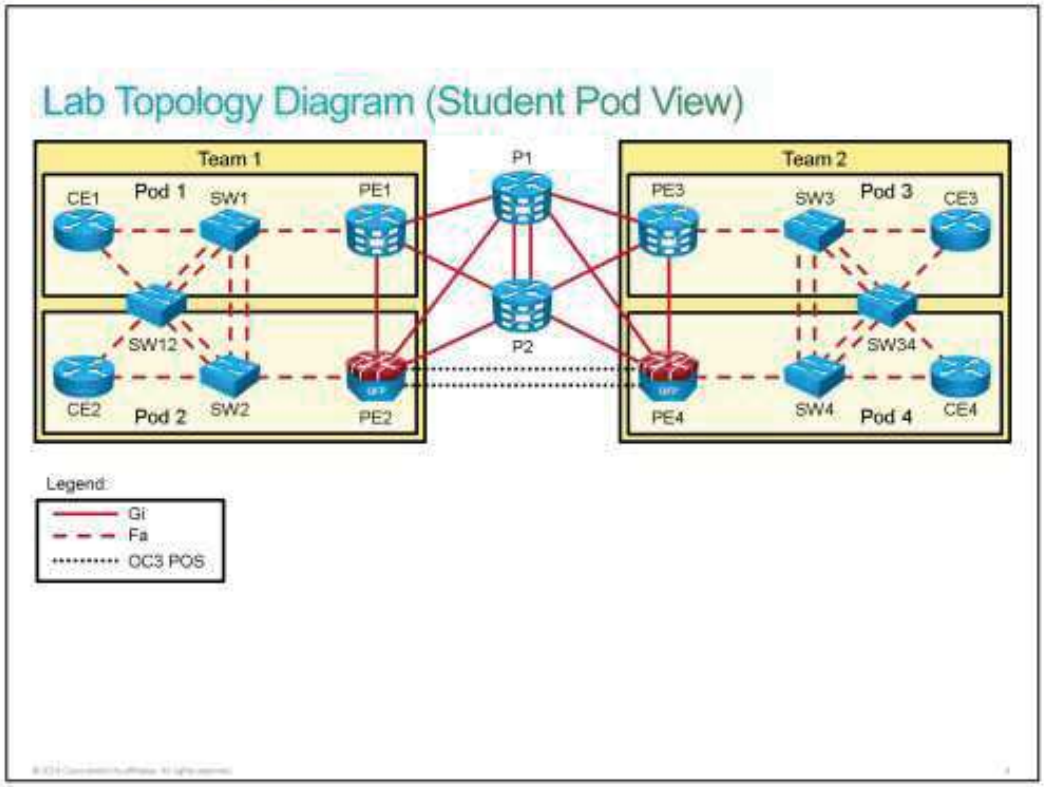
The CE routers in both pods are running Cisco IOS Software. The first pod within a team (pod 1 or 3) will work on PE routers running Cisco IOS XR Software, and the second pod within the same team (pod 2 or 4) will work on PE routers running Cisco IOS XE Software.

Laboratory Topology

Lab Topology Diagram (Backbone Pod View)



Lab Topology Diagram (Student Pod View)



Laboratory Equipment

These tables list the recommended equipment to support the lab activities. These tables assume a class size of eight students.

Description	Manufacturer	Part Number	Total Quantity
CE router: ISR 2901	Cisco	CISCO2901/K9	4
PE router running Cisco IOS XR: ASR 9006 with route processor and line card (with SFPs)	Cisco	ASR-9006-AC A9K-RSP-4G A9K-40GE-L	2
PE router running Cisco IOS XE: ASR 1001	Cisco	ASR1001-2XOC3POS	2
Switch: ME-3400E-24TS-M	Cisco	ME340x- METROACCESSK9-M	6
P1 router running Cisco IOS XR: ASR 9006 with route processor and line card (with SFPs)	Cisco	ASR-9006-AC A9K-RSP-4G A9K-40GE-L	1
P2 router running Cisco IOS XR: ASR 9001 with route processor and line card (with SFPs)	Cisco	ASR-9001-S	1

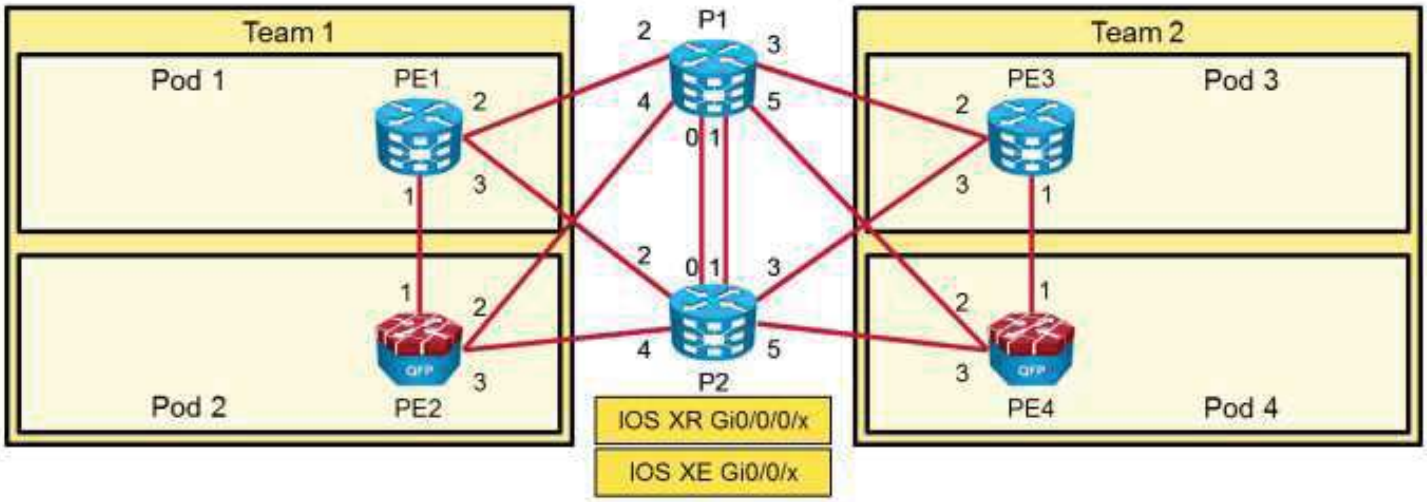
Software List

Description	Mfr.	Part Number	Total Quantity	Notes
Cisco IOS Software, ME340x Software , Version 12.2(60)EZ3, RELEASE SOFTWARE (fc2)	Cisco	ME340x-METROACCESSK9-M	6	me340x-metroaccessk9-mz.122-60.EZ3.bin
Cisco IOS Software, C2900 Software, Version 15.3(3)S2, RELEASE SOFTWARE (fc1)	Cisco	C2900-UNIVERSALK9-M	4	c2900-universalk9-mz.SPA.153-3.S2.bin
Cisco IOS Software, IOS-XE Software, Version 15.3(3)S, RELEASE SOFTWARE (fc1)	Cisco	X86_64_LINUX_IOSD-UNIVERSALK9-M	2	asr1001-universalk9.03.02.00.S.153-3.S.bin
Cisco IOS XR Software, Version 5.1.1	Cisco		4	ASR9K-iosxr-5.1.1.tar

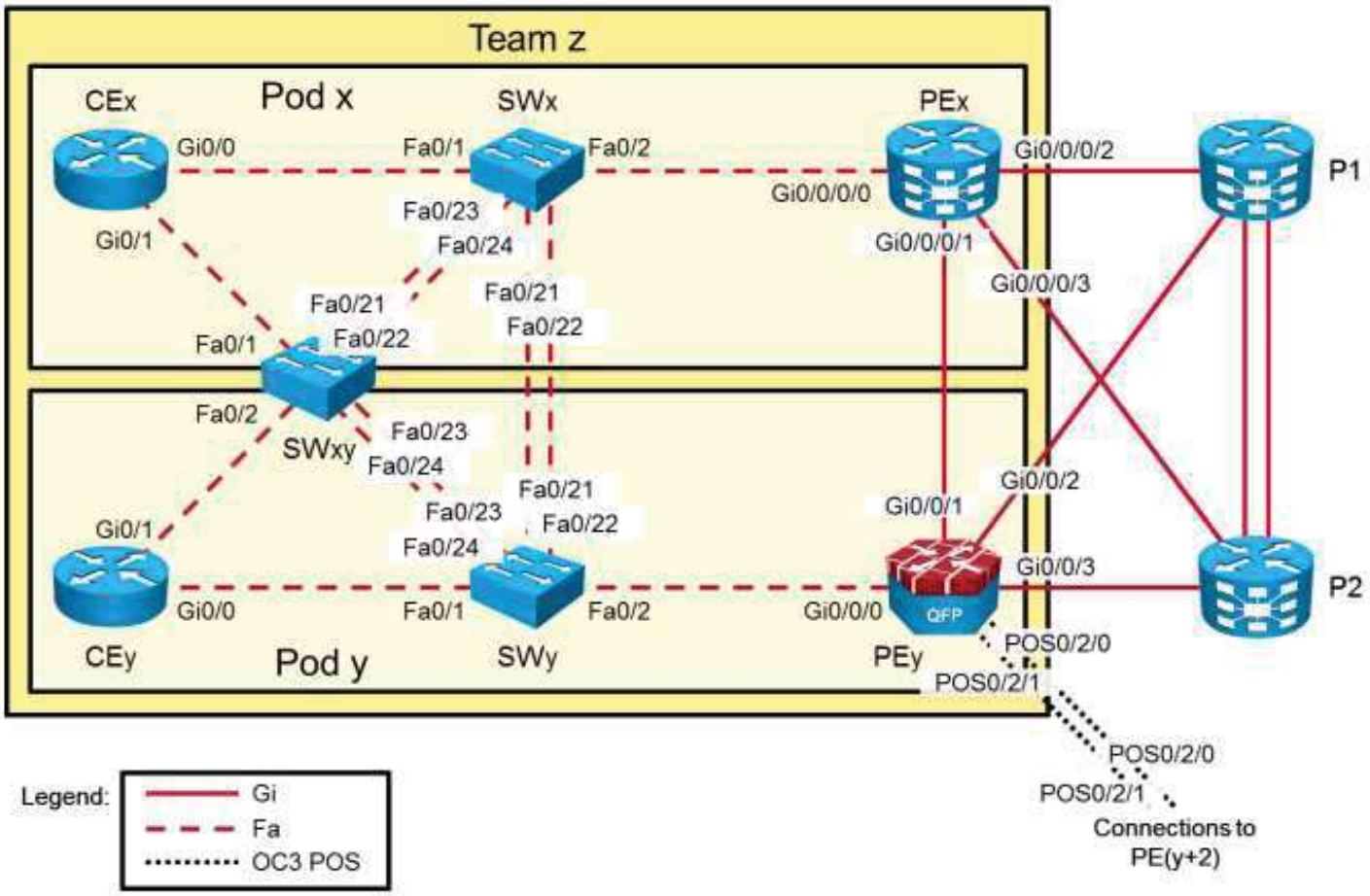
Initial Lab Build

This topic contains the information required to interconnect lab equipment.

The following figure shows core lab interface identification:



The following figure shows the pod lab interface identification:



General Lab Setup

This topic details the procedure to set up and configure the lab equipment at the beginning of each class.

Notes on Delivery Lab Equipment

On the Cisco IOS XR Software routers (Cisco ASR 9006 and Cisco ASR 9001), it is recommended to install all single-package PIEs that are included in the TAR file. It is required to install at least asr9k-mini-px-5.1.1 and asr9k-mpls-px-5.1.1 packages.

On the PE router running Cisco IOS XR (ASR 9006), PIE archive asr9k-mgbl-px.pie-5.1.1 must be located on disk0.

Configuration Files Summary

This topic details the course configuration files, which provide information about the starting condition of each lab

Configuration Filename	Comments
SPADVROUTE12_CE1_initial.txt	Initial configuration for CE1.
SPADVROUTE12_CE2_initial.txt	Initial configuration for CE2.
SPADVROUTE12_CE3_initial.txt	Initial configuration for CE3.
SPADVROUTE12_CE4_initial.txt	Initial configuration for CE4.
SPADVROUTE12_SW1_initial.txt	Initial configuration for SW1.
SPADVROUTE12_SW2_initial.txt	Initial configuration for SW2.
SPADVROUTE12_SW3_initial.txt	Initial configuration for SW3.
SPADVROUTE12_SW4_initial.txt	Initial configuration for SW4.
SPADVROUTE12_SW12_initial.txt	Initial configuration for SW12.
SPADVROUTE12_SW34_initial.txt	Initial configuration for SW34.
SPADVROUTE12_PE1_initial.txt	Initial configuration for PE1.
SPADVROUTE12_PE2_initial.txt	Initial configuration for PE2.
SPADVROUTE12_PE3_initial.txt	Initial configuration for PE3.
SPADVROUTE12_PE4_initial.txt	Initial configuration for PE4.
SPADVROUTE12_P1_initial.txt	Initial configuration for P1.
SPADVROUTE12_P2_initial.txt	Initial configuration for P2.

Lab Addressing

Loopback IP Addressing

Device Name	Device Role	Lo0 IPv4 Address	Lo0 IPv6 Address
CEx CEy	Cisco 2900 pod router	10.x.10.1/32 10.y.10.1/32	2001:db8:10:x:10::1/128 2001:db8:10:y:10::1/128
PEx PEy	Cisco ASR 9000 or Cisco ASR 1000 pod router	10.x.1.1/32 10.y.1.1/32	2001:db8:10:x:1::1/128 2001:db8:10:y:1::1/128
SWx SWy	Cisco ME340x pod switch	10.x.0.1/32 10.y.0.1/32	2001:db8:10:x:0::1/128 2001:db8:10:y:0::1/128
SWxy	Cisco ME340x pod switch not used in the service provider courses	10.xy.0.1/32	2001:db8:10:xy:0::1/128
P1	Cisco ASR 9006 core router	10.0.1.1/32	2001:db8:10:0:1::1/128
P2	Cisco ASR 9001 core router	10.0.2.1/32	2001:db8:10:0:2::1/128

Pod IP Addressing

Device	Interface	IPv4 Address	IPv6 Address
CEx	Gi0/0	192.168.10x.x1/24	2001:db8:192:168:10x::x1/80
CEy	Gi0/0	192.168.10y.y1/24	2001:db8:192:168:10y::y1/80
P1		192.168.x1.1/24	2001:db8:192:168:x1::1/80
		192.168.y1.1/24	2001:db8:192:168:y1::1/80
P2		192.168.x2.2/24	2001:db8:192:168:x2::2/80
		192.168.y2.2/24	2001:db8:192:168:y2::2/80
PE2	POS0/2/0	192.168.211.20/24	2001:db8:192:168:211::20/80
	POS0/2/1	192.168.212.20/24	2001:db8:192:168:212::20/80
PE4	POS0/2/0	192.168.211.40/24	2001:db8:192:168:211::40/80
	POS0/2/1	192.168.212.40/24	2001:db8:192:168:212::40/80
PEx	Gi0/0/0/0	192.168.10x.x0/24	2001:db8:192:168:10x::x0/80
	Gi0/0/0/1	192.168.1xy.x0/24	2001:db8:192:168:1xy::x0/80
	Gi0/0/0/2	192.168.x1.x0/24	2001:db8:192:168:x1::x0/80
	Gi0/0/0/3	192.168.x2.x0/24	2001:db8:192:168:x2::x0/80
PEy	Gi0/0/0	192.168.10y.y0/24	2001:db8:192:168:10y::y0/80
	Gi0/0/1	192.168.1xy.y0/24	2001:db8:192:168:1xy::y0/80
	Gi0/0/2	192.168.y1.y0/24	2001:db8:192:168:y1::y0/80
	Gi0/0/3	192.168.y2.y0/24	2001:db8:192:168:y2::y0/80

Core IP Addressing

Device	Device IP Address	Peer	Peer IP Address
P1	192.168.1.1/24 2001:db8:192:168:1::1/80	P2	192.168.1.2/24 2001:db8:192:168:1::2/80
	192.168.2.1/24 2001:db8:192:168:2::1/80		192.168.2.2/24 2001:db8:192:168:2::2/80

Lab Details

Hardware Lab 1: Implement BGP Route Reflectors

This topic details the lab activity for Hardware Lab 1: Implement BGP Route Reflectors.

In this lab activity, you will configure a backbone router (P2) to act as a redundant route reflector. You will also configure an additional IBGP session between the PE router in your pod and the redundant route reflector (P2). Your instructor already configured P1 as a route reflector for the pod PE routers.

Note	Students from two different pods work as a team. The CE routers in both pods are running Cisco IOS Software. The first pod in the team will work on the PE router that is running Cisco IOS XR Software, and the second pod in the same team will work on the PE router that is running Cisco IOS XE Software. Students in the same team should coordinate their activities.

Hardware Lab 2: Implement BGP Security Options

This topic details the lab activity for Hardware Lab 2: Implement BGP Security Options.

In this lab activity, you will first configure BGP neighbor authentication between the CE, PE, and P1 routers. You will also enable a BGP TTL security check between the same routers. You will also configure CoPP on the CE router. Finally, you will implement source-based RTBH filtering by using the P1 router as an RTBH triggering router.

Note	Students from two different pods work as a team. The CE routers in both pods are running Cisco IOS Software. The first pod in the team will work on the PE router that is running Cisco IOS XR Software, and the second pod in the same team will work on the PE router that is running Cisco IOS XE Software. Students in the same team should coordinate their activities.

Hardware Lab 3: Improve BGP Scalability

This topic details the lab activity for Hardware Lab 3: Improve BGP Scalability.

In this activity, you will first migrate an existing BGP configuration for EBGP neighbors to a template-based configuration. Then you will limit the number of prefixes that can be received from a BGP neighbor. You will also improve BGP convergence by changing the BGP scan and advertisement interval. Finally, you will implement BGP route dampening. All configurations will be performed on the PE router.

Students from two different pods work as a team. The CE routers in both pods are running Cisco IOS Software. The first pod in the team will work on the PE router that is running Cisco IOS XR Software, and the second pod in the same team will work on the PE router that is running Cisco IOS XE Software. Students in the same team should coordinate their activities.

Hardware Lab 4: Implement Layer 2 and Layer 3 Multicast

This topic details the lab activity for Hardware Lab 4: Implement Layer 2 and Layer 3 Multicast.

In this lab activity, you will implement and verify the operation of IGMP and MLD and you will observe multicast flooding on the LAN when IGMP snooping is implemented.

Note	Students from two different pods work as a team. The CE routers in both pods are running Cisco IOS Software. The first pod in the team will work on the PE router that is running Cisco IOS XR Software, and the second pod in the same team will work on the PE router that is running Cisco IOS XE Software. Students in the same team should coordinate their activities.

Hardware Lab 5: Enable and Optimize PIM-SM

This topic details the lab activity for Hardware Lab 5: Enable and Optimize PIM-SM.

Complete this lab activity to practice what you learned in the related module.

In this lab activity, you will enable multicast on the router in your team. The P1 router is preconfigured to act as an RP for your multicast traffic. You will configure receivers for multicast traffic on the CE and PE router. The other pod CE router will act as a multicast source.

Note	Students from two different pods work as a team. The CE routers in both pods are running Cisco IOS Software. The first pod in the team will work on the PE router that is running Cisco IOS XR Software, and the second pod in the same team will work on the PE router that is running Cisco IOS XE Software. Students in the same team should coordinate their activities.

You will work on different Cisco routers that are running Cisco IOS (c2900), Cisco IOS XE (asr1001), and Cisco IOS XR (asr9k) Software. After completing this activity, you will be able to meet these objectives:

- Implement multicast routing, PIM-SM, and manual RP configuration
- Observe shared tree formation
- Observe the switchover from the shared tree to the SPT

Hardware Lab 6: Implement PIM-SM Enhancements

This topic details the lab activity for Hardware Lab 6: Implement PIM-SM Enhancements.

In this lab activity, you will configure and monitor PIM-SSM on the CE and PE routers.

Note	Students from two different pods work as a team. The CE routers in both pods are running Cisco IOS Software. The first pod in the team will work on the PE router that is running Cisco IOS XR Software, and the second pod in the same team will work on the PE router that is running Cisco IOS XE Software. Students in the same team should coordinate their activities.

You will work on different Cisco routers that are running Cisco IOS (c2900), Cisco IOS XE (asr1001), and Cisco IOS XR (asr9k) Software. After completing this activity, you will be able to meet this objective:

- Implement and monitor PIM-SSM

Hardware Lab 7: Implement Rendezvous Point Distribution

This topic details the lab activity for Hardware Lab 7: Implement Rendezvous Point Distribution.

In this activity, you will use PIM-SM. Avoiding the configuration of static RP information, you will choose the standard bootstrap mechanism to verify the redundant setup of BSR routers and RPs.

You also will configure two RPs with the same IP address, sharing the same range of groups. This action will create the Anycast RP solution that will require a simple MSDP configuration.

Note	Students from two different pods work as a team. The CE routers in both pods are running Cisco IOS Software. The first pod in the team will work on the PE router that is running Cisco IOS XR Software, and the second pod in the same team will work on the PE router that is running Cisco IOS XE Software. Students in the same team should coordinate their activities.

Hardware Lab 8: Implement a DHCPv6 Server with Prefix Delegation

This topic details the lab activity for Hardware Lab 8: Implement a DHCPv6 Server with Prefix Delegation.

In this lab activity, you will configure the PE router to act as a prefix delegation DHCPv6 server. You will configure the PE router to delegate a prefix to the CE router. You will then configure the CE router interface with an IPv6 address from the delegated prefix. You will also configure the CE router to act as a DHCPv6 Lite server, with DNS server IP address options obtained from the PE router. This scenario is valid, where the service provider would assign a prefix to a CE router using prefix delegation, and the CE router would then advertise the prefix to LAN endpoints to enable stateless autoconfiguration.

This lab exercise will be performed only in the pod with Cisco IOS XE router.

Note	Students from two different pods work as a team. The CE routers in both pods are running Cisco IOS Software. The first pod in the team will work on the PE router running Cisco IOS XR Software, and the second pod in the same team will work on the PE router running Cisco IOS XE Software. Students in the same team should coordinate their activities.

Hardware Lab 9: Implement IPv6 Multicasting

This topic details the lab activity for Hardware Lab 9: Implement IPv6 Multicasting.

In this lab activity, you will first implement IPv6 multicast using embedded RPs. Your pod CE router will act as the multicast receiver, and the other pod CE router will act as the multicast source. Your pod PE router will act as the RP.

Note	Students from two different pods work as a team. The CE routers in both pods are running Cisco IOS Software. The first pod in the team will work on the PE router running Cisco IOS XR Software, and the second pod in the same team will work on the PE router running Cisco IOS XE software. Students in the same team should coordinate their activities.

Hardware Lab 10: Implement Tunnels for IPv6

This topic details the lab activity for Hardware Lab 10: Implement Tunnels for IPv6.

In this lab activity, you will first establish a static IPv6-in-IPv4 tunnel between two CE routers in different pods in the same team. Then you will deploy 6RD tunnels and configure a 6RD CE router and 6RD Border Relay.

Note	Students from two different pods work as a team. The CE routers in both pods are running Cisco IOS Software. In this activity, students will work on CE routers. Students from both pods will work on the PE router from the second pod only. Students in the same team should coordinate their activities.

