Implementing Cisco MPLS

MPLS v3.0; 5 Days, Instructor-led

About this course

The Implementing Cisco MPLS (MPLS) v3.0 is a five-day course that is designed to help students prepare for MPLS exam. This update to the course reflects the most-recent developments in network design and technologies, using real-world scenarios to help reinforce the learning of key objectives.

Enterprises and service providers face many challenges in terms of customer demand, including an ongoing need for value-added services. Conventional IP packet forwarding has several limitations, and more and more enterprise and service providers realize that something else is needed. Not only they must be concerned with protecting their existing infrastructure, but they must also find ways to generate new services that are not currently supportable using existing technologies.

Multiprotocol Label Switching (MPLS) is a high-performance method for forwarding packets through a network. MPLS enables routers at the edge of a network to apply simple labels to packets. This practice allows the edge devices to switch packets according to labels, with minimal lookup overhead. MPLS integrates the performance and traffic-management capabilities of data link Layer 2 with the scalability and flexibility of network Layer 3 routing. When used in conjunction with other standard technologies, MPLS gives the ability to support value-added features.

To participate in the hands-on labs in this class, you need to bring a laptop computer with the following:

- Windows 7 or 8.1 or 10 is recommended. Mac OSX 10.6 or greater is supported as well.
- Intel Celeron or better processors are preferred.
- 1 GB or more of RAM
- Browser Requirements: Internet Explorer 10 or greater or Mozilla Firefox. (Safari and Mozilla Firefox for Mac OSX)
- All students are required to have administrator rights to their PCs and cannot be logged in to a domain using any Group Policies that will limit their machine's capabilities.
- If you do not have administrator rights to your PC, you at least need permissions to download, install, and run Cisco Any Connect Client.
- If you are participating in a WebEx event, it is highly recommended to take this class at a location that has bandwidth speeds at a minimum of 1 Mbps bandwidth speeds.
Note: Students registering for this course will be receiving their course kit in a digital format. To be able to view your digital kit you will need to bring a laptop PC and/or a compatible iPad or Android tablet.

Prerequisites

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

- Intermediate to advanced knowledge of Cisco IOS Software configuration
- Configuring and troubleshooting EIGRP, OSPF, IS-IS and BGP
- Skills and knowledge equivalent to those learned in:
  - Interconnecting Cisco Networking Devices v2.0, Part 1 (ICND1 v2.0) and Part 2 (ICND2 v2.0), or
  - Interconnecting Cisco Networking Devices: Accelerated Version 2.0 (CCNAX v2.0)
  - Implementing Cisco IP Routing (ROUTE v2.0)
  - Configuring BGP on Cisco Routers (BGP v4.0)
  - Building Cisco Service Provider Next-Generation Networks Part 1 (SPNGN1) v1.2
  - Building Cisco Service Provider Next-Generation Networks Part 2 (SPNGN2) v1.2
  - Deploying Cisco Service Provider Network Routing (SPROUTE) v1.2
  - Deploying Cisco Service Provider Advanced Network Routing (SPADVROUTE) v1.2

Audience profile

This course is intended primarily for network administrators, network engineers, network managers and systems engineers who would like to implement MPLS and MPLS Traffic Engineering. The secondary audience for this course is intended for network designers and project managers. The course is also recommended to all individuals preparing for MPLS exam.

At course completion

After completing this course, students will be able to:

- Describe the features of MPLS
- Describe how MPLS labels are assigned and distributed
- Configure and troubleshoot frame-mode MPLS on Cisco IOS platforms
- Describe the MPLS peer-to-peer architecture and explain the routing and packet-forwarding model in this architecture
- Configure, monitor, and troubleshoot VPN operations
- Describe how the MPLS VPN model can be used to implement managed services and Internet access
- Describe the various Internet access implementations that are available and the benefits and drawbacks of each model
- Describe the tasks and commands that are necessary to implement MPLS TE
Course Outline

Module 1: MPLS Concepts

Lesson 1: Introducing Basic MPLS Concepts

- Foundations of Traditional IP Routing
- Basic MPLS Features
- Benefits of MPLS
- MPLS Terminology: Label Switch Router
- MPLS Terminology: Label-Switched Path
- MPLS Terminology: Upstream and Downstream
- MPLS Architecture Components
- Architecture of Ingress Edge LSRs
- Architecture of Intermediate LSRs
- Architecture of Egress Edge LSRs
- Summary

Lesson 2: Introducing MPLS Labels and Label Stack

- MPLS Labels
- FEC and MPLS Forwarding
- MPLS Label Format
- MPLS Label Imposition
- MPLS Label Stack
- Summary

Lesson 3: Identifying MPLS Applications

- MPLS Services
- MPLS Unicast IP Routing
- MPLS Multicast IP Routing
- MPLS VPNs
- MPLS Traffic Engineering
- MPLS Quality of Service
- Any Transport over MPLS
- Interactions Between MPLS Services
- Summary

Lesson 4: Module Summary

- References
Lesson 5: Module Self-Check

Module 2: Label Assignment and Distribution

Lesson 1: Discovering LDP Neighbors
- Label-Distributing Protocols
- LDP Neighbor Session Establishment
- LDP Link Hello Message
- LDP Negotiating Label Space
- Discovering LDP Neighbors
- Negotiating LDP Sessions
- Summary

Lesson 2: Introducing Typical Label Distribution in Frame-Mode MPLS
- Propagating Labels Across a Network
- Building Blocks for IP Forwarding
- Using the FIB Table to Forward Packets
- Using LDP to Forward Packets
- Label-Switched Path
- Propagating Labels by Using PHP
- Impact of IP Aggregation on LSPs
- Label Allocation in a Frame-Mode MPLS Network
- Label Distribution and Advertisement
- Receiving Label Advertisement
- Liberal Label Retention
- Further Label Allocation
- Frame-Mode Loop Detection Using the MPLS TTL Field
- Normal TTL Operation
- Disabling TTL Propagation
- Summary

Lesson 3: Introducing Convergence in Frame-Mode MPLS
- MPLS Steady-State Operation
- Link Failure State
- Routing Protocol Convergence After a Link Failure
- MPLS Convergence After a Link Failure
- Link Recovery Actions
- Summary

Lesson 4: Module Summary
- References
Lesson 5: Module Self-Check

Module 3: Frame-Mode MPLS Implementation on Cisco IOS Platforms

Lesson 1: Introducing CEF Switching
- Cisco IOS Platform-Switching Mechanisms
- Using Standard IP Switching
- Cisco Express Forwarding Switching Architecture
- Configuring IP Cisco Express Forwarding
- Monitoring IP Cisco Express Forwarding
- Discovery 1: Verifying CEF Switching
- Summary

Lesson 2: Configuring Frame-Mode MPLS on Cisco IOS Platforms
- MPLS Configuration Tasks
- Configuring the MPLS ID on a Router
- Configuring MPLS on a Frame-Mode Interface
- Discovery 2: Enabling MPLS
- Configuring IP TTL Propagation
- Discovery 3: Change IP TTL Propagation
- Configuring Conditional Label Distribution
- Summary

Lesson 3: Monitoring Frame-Mode MPLS on Cisco IOS Platforms
- Monitoring MPLS
- Monitoring LDP
- Monitoring Label Switching
- Debugging MPLS and LDP
- Summary

Lesson 4: Troubleshooting Frame-Mode MPLS on Cisco IOS Platforms
- Common Frame-Mode MPLS Issues
- Solving LDP Session Startup Issues
- Solving Label Allocation Issues
- Solving Label Distribution Issues
- Solving Packet-Labeling Issues
- Solving Intermittent MPLS Failures
- Solving Packet Propagation Issues
- Summary
Lesson 5: Module Summary

• References

Lesson 6: Module Self-Check

Module 4: MPLS Virtual Private Network Technology

Lesson 1: Introducing Virtual Private Networks

• Basic VPN Overview
• VPN Implementation Models
• Overlay VPN Technologies
• Peer-to-Peer VPN Technologies
• Benefits of VPNS
• Drawbacks of VPNS
• Summary

Lesson 2: Introducing MPLS VPN Architecture

• MPLS VPN Architecture
• PE Router Architecture
• VRF Overview
• Methods of Propagating Routing Information Across the P-Network
• Route Distinguishers
• RD Format
• RD Operation in MPLS VPN
• RD Process Flow
• Route Targets
• RT Operation
• RT and RD Process Flow
• Summary

Lesson 3: Introducing the MPLS VPN Routing Model

• MPLS VPN Routing
• CE Router MPLS VPN Routing
• P Router MPLS VPN Routing
• PE Router MPLS VPN Routing
• Support for Internet Routing
• Routing Tables on PE Routers
• Identifying End-to-End Routing Update Flow
• Summary
Lesson 4: Forwarding MPLS VPN Packets

- End-to-End VPN Forwarding Mechanisms
- VPN Penultimate Hop Popping
- Propagating VPN Labels Between PE Routers
- Effects of MPLS VPNs on Label Propagation
- Effects of MPLS VPNs on Packet Forwarding
- Summary

Lesson 5: Module Summary

- References

Lesson 6: Module Self-Check

Module 5: MPLS VPN Implementation

Lesson 1: Using MPLS VPN Mechanisms of Cisco IOS Platforms

- VRF Table
- Need for Routing Protocol Contexts
- VPN-Aware Routing Protocols
- Using VRF Tables
- Propagating BGP Routes Outbound Example
- Propagating Non-BGP Routes Outbound Example
- Propagating BGP Routes Inbound Example
- Propagating Non-BGP Routes Inbound Example
- Summary

Lesson 2: Configuring an MP-BGP Session Between PE Routers

- Configuring BGP Address Families
- Enabling BGP Neighbors
- Configuring MP-BGP
- Configuring MP-IBGP
- Discovery 4: Configure MP-IBGP
- Summary

Lesson 3: Configuring VRF Tables

- VRF Configuration Tasks
- Creating VRF Tables and Assigning RDs
- Specifying Export and Import RTs
- Discovery 5: Configure the VRF Instances
- Using MPLS VPN IDs
- Summary
Lesson 4: Configuring Small-Scale Routing Protocols Between PE and CE Routers

- Configuring PE-CE Routing Protocols
- Selecting the VRF Routing Context for BGP
- Configuring Per-VRF Static Routes
- Configuring RIP PE-CE Routing
- Discovery 6: Configure RIP as a PE-CE Routing Protocol
- Configuring EIGRP PE-CE Routing
- Discovery 7: Configure EIGRP as a PE-CE Routing Protocol
- Configuring SOO for EIGRP PE-CE Loop Prevention
- Summary

Lesson 5: Monitoring MPLS VPN Operations

- Monitoring VRFs
- Monitoring VRF Routing
- Monitoring MP-BGP Sessions
- Monitoring an MP-BGP VPNv4 Table
- Monitoring Per-VRF Cisco Express Forwarding and LFIB Structures
- Monitoring Labels Associated with VPNv4 Routes
- Identifying MPLS VPN Diagnostic Commands
- Summary

Lesson 6: Configuring OSPF as the Routing Protocol Between PE and CE Routers

- OSPF Hierarchical Model
- OSPF in an MPLS VPN Routing Model
- OSPF Superbackbone OSPF-BGP Hierarchy Issue
- OSPF in MPLS VPNs Goals
- OSPF Superbackbone Route Propagation Example
- OSPF Superbackbone Rules
- OSPF Superbackbone Implementation
- OSPF Superbackbone External Routes
- OSPF Superbackbone Mixing Routing Protocols
- Configuring PE-CE OSPF Routing
- Discovery 8: Configure OSPF as a PE-CE Routing Protocol
- Routing Loops Between MP-BGP and OSPF
- OSPF Down Bit Loop Prevention
- Optimizing of Packet Forwarding Across the MPLS VPN Backbone
- Routing Loops Across OSPF Domains
- OSPF Tag Field Operation
- OSPF Tag Field Usage Guidelines
- OSPF Tag Field Routing Loop Prevention
- Sham Link
- Summary
Lesson 7: Configuring BGP as the Routing Protocol Between PE and CE Routers

- Configuring a Per-VRF BGP Routing Context
- Reasons for Limiting the Number of Routes in a VRF
- Limiting the Number of Prefixes Received from a BGP Neighbor
- Limiting the Total Number of VRF Routes
- Identifying AS-Override Issues
- AS-Override Implementation
- AS-Path Prepending
- Discovery 9: Configure BGP as a PE-CE Routing Protocol
- Identifying the Allow-AS Issue
- Allow-AS-In Implementation
- Implementing SOO for Loop Prevention
- Summary

Lesson 8: Troubleshooting MPLS VPNs

- Identifying Preliminary Steps in MPLS VPN Troubleshooting
- Verifying the Routing Information Flow
- Validating CE-to-PE Routing Information Flow
- Validating PE-to-PE Routing Information Flow
- Validating PE-to-CE Routing Information Flow
- Identifying the Issues When Verifying the Data Flow
- Validating Cisco Express Forwarding Status
- Validating the End-to-End LSP
- Validating the LFIB Status
- MPLS VPN Troubleshooting Command Summary
- Summary

Lesson 9: Module Summary
Lesson 10: Module Self-Check

Module 6: Complex MPLS VPNs

Lesson 1: Introducing Overlapping VPNs

- Participants in Overlapping VPNs
- Typical Overlapping VPN Usages
- Overlapping VPN Routing
- Overlapping VPN Data Flow
- Configuring Overlapping VPNs
- Summary

Lesson 2: Introducing Central Services VPNs

- Central Services VPN
• Central Services VPN Routing
• Central Services VPN Data Flow Model
• Discovery 10: Configure a Central Services VPN
• Central Services VPN and Overlapping VPN Requirements
• Configuring RDs and RTs in a Central Services VPN and Overlapping VPN
• Advanced VRF Features
• Configuring Selective VRF Import
• Configuring Selective VRF Export
• Summary

Lesson 3: Introducing the Managed CE Routers Service

• Managed CE Routers
• VRF Creation and RD Overview
• Configuring Managed CE Routers
• Summary

Lesson 4: Module Summary
Lesson 5: Module Self-Check

Module 7: Internet Access and MPLS VPNs

Lesson 1: Combining Internet Access with MPLS VPNs

• Customer Internet Connectivity Scenarios Overview
• Classical Internet Access
• Multisite Internet Access
• Wholesale Internet Access
• Internet Design Models for Service Providers
• Internet Access Through Global Routing
• Internet Access Through a Separate VPN Service
• Internet Access Through Route Leaking
• Summary

Lesson 2: Implementing Internet Access in the MPLS VPN Environment

• Classical Internet Access for a VPN Customer
• Implementing Classical Internet Access for a VPN Customer
• Using Separate Subinterfaces
• Implementing Internet Access from Every Customer Site
• Internet Access as a Separate VPN
• Redundant Internet Access
• Implementing Wholesale Internet Access
• Separate Internet Access Benefits and Limitations
• Running an Internet Backbone in a VPN: Benefits and Limitations
• Summary
Lesson 3: Module Summary
Lesson 4: Module Self-Check

Module 8: MPLS Traffic Engineering Overview

Lesson 1: Introducing MPLS Traffic Engineering Components

- Traffic Engineering Concepts
- Traffic Engineering Motivations
- Business Drivers for Traffic Engineering
- Congestion Avoidance and Traffic Engineering
- Traffic Engineering with a Layer 2 Overlay Model
- Traffic Engineering with a Layer 2 Overlay Model: Example
- Drawbacks of the Layer 2 Overlay Solution
- Layer 3 Routing Model Without Traffic Engineering
- Traffic Engineering with a Layer 3 Routing Model
- Traffic Engineering with the MPLS TE Model
- MPLS TE Traffic Tunnels
- Traffic Tunnels: Attributes
- Link Resource Attributes
- Constraint-Based Path Computation
- Example of Constraint-Based Path Computation (Bandwidth)
- MPLS TE Process
- Role of RSVP in Path Setup Procedures
- Path Setup and Admission Control with RSVP
- Forwarding Traffic to a Tunnel
- Autoroute
- Autoroute Example
- Summary

Lesson 2: MPLS Traffic Engineering Operations

- Attributes Used by Constraint-Based Path Computation
- MPLS TE Link-Resource Attributes
- MPLS TE Link Resource Attributes: Maximum Bandwidth and Maximum Reservable Bandwidth
- MPLS TE Link-Resource Attributes: Link-Resource Class
- MPLS TE Link-Resource Attributes: Constraint-Based Specific Link Metric (Administrative Weight)
- MPLS TE Tunnel Attributes
- MPLS TE Tunnel Attributes: Traffic Parameter and Path Selection and Management
- MPLS TE Tunnel Attributes: Tunnel Resource Class Affinity
- MPLS TE Tunnel Attributes: Adaptability, Priority, Pre-emption
- MPLS TE Tunnel Attributes: Resilience
- Implementing TE Policies with Affinity Bits
- Using Affinity Bits in TE Policies
- Propagating MPLS TE Link Attributes with Link-State Routing Protocol
Lesson 3: Configuring MPLS Traffic Engineering on Cisco IOS Platforms

- Constraint-Based Path Computation
- Constraint-Based Path Computation: Path Selection
- Example of Constraint-Based Path Computation (Resource Affinity)
- Path Setup
- RSVP Usage in Path Setup
- Hop-by-Hop Path Setup with RSVP
- Tunnel and Link Admission Control
- Path Rerouting
- Path Reoptimization
- Path Rerouting: Link Failure
- Assigning Traffic to Traffic Tunnels
- Using Static Routing to Assign Traffic to Traffic Tunnel
- Autoroute
  - Autoroute: Path Selection Rules
  - Autoroute: Default Metric
  - Autoroute: Relative and Absolute Metric
  - Forwarding Adjacency
  - Forwarding Adjacency Traffic Flows
- Summary

Lesson 4: Monitoring Basic MPLS TE on Cisco IOS Platforms

- Monitoring MPLS TE Tunnels
  - show ip rsvp interface Command
  - show mpls traffic-eng tunnels brief Command
  - Monitoring MPLS TE
  - show mpls traffic-eng autoroute Command
  - show ip cef Command
- Summary
Lesson 5: Module Summary
Lesson 6: Module Self-Check

Lab Outline

Challenge 1: Implement the Service Provider's and Customer's IP Addressing and IGP Routing
  • Implement the Service Provider IP Addressing and IGP Routing Protocol

Challenge 2: Implement the Core MPLS Environment in the Service Provider Network
  • Implement the Core MPLS Environment in the Service Provider Network

Challenge 3: Implement EIGRP Based VPNs
  • Implement EIGRP Based VPNs

Challenge 4: Implement OSPF Based MPLS VPNs
  • Implement OSPF Based MPLS VPNs

Challenge 5: Implement BGP Based MPLS VPNs
  • Implement BGP Based MPLS VPNs

Challenge 6: Implement MPLS Traffic Engineering
  • Implement MPLS Traffic Engineering