

MPLS ENT Course Outline

BGP

1. BGP Overview
 - Session Establishment
 - Path Attributes
 - Route Processing
 - Basic Configuration
 - Monitoring and Troubleshooting
2. BGP Transit Autonomous Systems
 - Working with a Transit AS
 - Interacting with IBGP and EBGP in a Transit AS
 - Forwarding Packets in a Transit AS
 - Configuring a Transit AS
 - Monitoring and Troubleshooting IBGP in a Transit AS
3. Route Selection Using Policy Controls
 - Multihomed BGP Networks
 - Employing AS Path Filters
 - Filtering with Prefix Lists
 - Outbound Route Filtering
 - Applying Route Maps as BGP Filters
 - Implementing Changes in BGP Policy
4. Route Selection Using Attributes
 - BGP Route Selection with Weights
 - BGP Local Preference
 - AS-Path Prepending
 - BGP Multi-Exit Discriminator (MED)
 - Addressing BGP Communities
5. Customer-to-Provider Connectivity with BGP
 - Customer-to-Provider Connectivity Requirements
 - Implementing Customer Connectivity Using Static Routes
 - Connecting a Multihomed Customer to Single or Multiple Service Providers
6. Scaling Service Provider Networks
 - Scaling IGP and BGP in Service Provider Networks
 - Designing Networks and Route Reflectors
 - Configuring and Monitoring Route Reflectors
 - Configuring and Monitoring Confederations
7. Optimizing BGP Scalability
 - Improving BGP Convergence
 - Limiting the Number of Prefixes Received from a BGP Neighbor
 - Implementing BGP Peer Groups
 - BGP Route Dampening

Labs

Lab 1: Network Setup

- Establish physical connectivity between routers
- Configure IP addressing
- Enable an Interior Routing Protocol
- Verify routing

Lab 2: Configuring EBGP Peerings

- Create two EBGP peerings
 - Advertise networks into BGP
 - Redistribute your IGP into BGP
 - Examine the effects of BGP auto-summarization
 - Summarize routes to your neighbour
- Lab 3: Configuring IBGP Peerings
- Configure an IBGP peering with another edge router
 - Peering with loopback interfaces
 - Examine effect of BGP synchronization
 - Discover BGP next-hop behavior
 - Examine the effects of multihoming on path selection
- Lab 4: Using AS-Path Filters and Regular Expressions
- Filter updates to external routers
 - Manipulate path selection using AS-path filters and regular expressions
- Lab 5: Using Prefix Lists
- Filter advertised AS routes using prefix lists
- Lab 6: Soft Reconfiguration and Route Refresh
- Monitor and verify the actions of BGP Route Refresh
 - Configure BGP soft inbound reconfiguration
- Lab 7: Configuring the Weight Attribute
- Configure a second BGP peering for each router
 - Set a weight value for routes received from each EBGP neighbor
 - Monitor the resulting path choice
- Lab 8: Configuring the Local Preference Attribute
- Use the Local Preference attribute to control BGP path selection
- Lab 9: AS-Path Prepending
- Configure AS-Path Prepending to make one path into your AS look more attractive than the other
- Lab 10: Configuring the Multi-Exit Discriminator (MED) Attribute
- Use the MED attribute to influence the BGP path selection by routers in neighboring systems
- Lab 11: Using the Community Attribute
- Configure the community attribute in setting local preference BGP policies
- Lab 12: Becoming a Service Provider
- Configure your AS as a service provider
 - Configure full-mesh IBGP
 - Determine appropriate filters for routing updates to and from your customer
 - Configure and apply filters
- Lab 13: Using Route Reflectors
- Configure a hierarchical route reflector structure
 - Examine the effects of route reflectors on routing updates
- Lab 14: Using Confederations
- Divide your AS into confederations
 - Configure intra- and inter-confederation peerings
 - Configure peering with external neighbors
 - Examine the effects of confederation on routing updates
- Lab 15: Monitoring and Tuning BGP Resource Use
- Examine the effects of BGP session establishment and route updates on router resources
 - Examine how timers speed BGP convergence
 - Set a maximum prefix value
- Lab 16: Using Peer Groups

- Place neighboring BGP routers into peer groups
- Apply policy configuration to peer groups

Lab 17: Using Route Dampening

- Configure and apply route dampening to external peers
- Monitor the results when that peer's routes flap

MPLS

Module 1: MPLS Features

Lesson 1: Describing Basic MPLS Concepts

- Provide an overview of MPLS forwarding, features, and benefits
- Define MPLS terminology
- Describe the main components of the MPLS architecture

Lesson 2: Describing MPLS Labels and Label Stack

- Describe the features and format of MPLS labels
- Describe where MPLS labels are imposed in an IP packet
- Describe the features of an MPLS label stack

Lesson 3: Identifying MPLS Applications

- Describe the various services that are used with MPLS
- Describe the features of MPLS unicast and multicast IP routing
- Describe MPLS use in VPNs
- Describe MPLS use in TE environments
- Describe MPLS use in QoS environments
- Describe AToM
- Identify the interactions that occur between various MPLS services

Module 2: Label Assignment and Distribution

Lesson 1: Discovering LDP Neighbors

- Describe several varieties of protocols that distribute labels
- Describe how LDP sessions are established between adjacent neighbors
- Describe how LDP neighbors are discovered
- Describe the process of LDP session negotiation between LDP neighbors

Lesson 2: Describing Typical Label Distribution in Frame-Mode MPLS

- Describe how labels are propagated across a network
- Describe the function of LSPs
- Describe the function of PHP
- Describe the impact that IP aggregation has on LSPs
- Describe how labels are allocated in a frame-mode MPLS network
- Describe how MPLS labels are distributed and advertised in a frame-mode network
- Describe how frame-mode loops are detected

Lesson 3: Describing Convergence in Frame-Mode MPLS

- Describe the MPLS steady-state environment
- Describe what happens in the routing tables when a link failure occurs
- Describe routing protocol convergence after a link failure
- Describe frame-mode MPLS convergence after a link failure
- Describe IP and MPLS convergence actions after a link failure has been resolved

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

Lesson 1: Using Cisco Express Forwarding Switching

- Describe the various switching mechanisms used by Cisco IOS platforms
- Describe the function of standard IP switching on Cisco IOS platforms
- Describe the architecture of Cisco Express Forwarding switching

- Configure IP Cisco Express Forwarding switching
- Monitor IP Cisco Express Forwarding switching

Lesson 2: Configuring Frame-Mode MPLS on Cisco IOS Platforms

- Describe the MPLS configuration tasks
- Configure the MPLS ID on a router
- Configure MPLS on a frame-mode interface
- Configure a label-switching MTU
- Configure IP TTL propagation
- Configure conditional label distribution

Lesson 3: Monitoring Frame-Mode MPLS on Cisco IOS Platforms

- Describe how to monitor MPLS
- Describe how to monitor LDP
- Describe how to monitor label switching
- Describe how to debug MPLS and LDP

Lesson 4: Troubleshooting Frame-Mode MPLS on Cisco IOS Platforms

- Identify the common issues that arise in MPLS networks
- Solve LDP session startup issues
- Solve label allocation issues that can arise in MPLS networks
- Solve label distribution issues that can arise in MPLS networks
- Solve packet-labeling issues that can arise in MPLS networks
- Solve intermittent MPLS failures
- Solve packet propagation issues in MPLS networks

Module 4: MPLS VPN Technology

Lesson 1: Introducing Virtual Private Networks

- Provide an overview of virtual private networks
- Identify the two major VPN implementation models
- Describe the benefits and drawbacks of each type of VPN model

Lesson 2: Introducing MPLS VPN Architecture

- Describe the MPLS VPN architecture
- Describe the different methods of propagating routing information across the provider network
- Describe the features of RDs
- Describe the features of RTs

Lesson 3: Introducing the MPLS VPN Routing Model

- Describe the routing requirements for MPLS VPNs
- Describe how IPv4 is used to provide support for existing Internet routing
- Identify the routing tables implemented in the PE router to support MPLS VPNs
- Describe the end-to-end flow of routing updates in an MPLS VPN

Lesson 4: Forwarding MPLS VPN Packets

- Describe the end-to-end MPLS VPN forwarding mechanisms
- Describe the operation of PHP in an MPLS VPN environment
- Describe how labels are propagated between PE routers
- Describe the effects of MPLS VPNs on label propagation
- Describe the effects of MPLS VPNs on packet forwarding

Module 5: MPLS VPN Implementation

Lesson 1: Using MPLS VPN Mechanisms of Cisco IOS Platforms

- Describe the characteristics of a VRF table
- Describe the need for routing protocol contexts
- Describe the characteristics of VPN-aware routing protocols
- Describe how VRF tables are used
- Describe the outbound BGP route propagation process in an MPLS VPN implementation
- Describe the outbound non-BGP route propagation process in an MPLS VPN implementation

- Describe the inbound route propagation process in an MPLS VPN implementation

Lesson 2: Configuring VRF Tables

- Identify the tasks that are required to configure a VRF table
- Create a VRF table and assign RDs
- Specify export and import RTs
- Describe the optional use of VPN IDs
- Assign an interface to a VRF table
- Describe a typical Cisco IOS configuration that enables VRFs

Lesson 3: Configuring an MP-BGP Session Between PE Routers

- Configure BGP address families
- Describe the requirements for enabling BGP neighbors in an MPLS VPN environment
- Identify the process steps involved in configuring MP-BGP in an MPLS VPN environment
- Configure MP-IBGP in an MPLS VPN environment
- Configure MP-BGP community propagation in an MPLS VPN environment
- Disable IPv4 route exchange in an MPLS VPN environment

Lesson 4: Configuring Small-Scale Routing Protocols Between PE and CE Routers

- Identify the requirements for configuring PE-CE routing protocols
- Select the VRF routing context for BGP on the PE router
- Configure per-VRF static routes
- Configure a RIP PE-CE routing session
- Configure an EIGRP PE-CE routing session

Lesson 5: Monitoring MPLS VPN Operations

- Monitor VRF information
- Monitor VRF routing
- Monitor MP-BGP sessions
- Monitor an MP-BGP VPNv4 table
- Monitor per-VRF Cisco Express Forwarding and LFIB structures
- Monitor labels associated with VPNv4 routes
- Identify the command syntax that is used with other MPLS VPN monitoring commands

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

- Describe the features of the OSPF hierarchical model
- Describe the propagation of OSPF customer routes across the MPLS VPN backbone
- Describe how an MPLS VPN is implemented as an OSPF superbackbone
- Configure a PE-CE OSPF routing session
- Describe how the OSPF down bit is used to address the route loop issue
- Describe how packet forwarding is optimized across the MPLS VPN backbone
- Describe how the OSPF tag field is used to address the root loop issue
- Describe the features of a sham link
- Configure a sham link

Lesson 7: Configuring BGP as the Routing Protocol Between PE and CE Routers

- Configure a per-VRF BGP routing context
- Explain the reason for limiting the number of routes in a VRF
- Describe how to limit the number of prefixes received from a BGP neighbor
- Describe how to limit the total number of VRF routes
- Identify the issues encountered when a customer wants to reuse the same AS number on several sites
- Identify the issues encountered when a customer site links two VPNs
- Implement SOO for loop prevention

Lesson 8: Troubleshooting MPLS VPNs

- Identify the preliminary steps in MPLS VPN troubleshooting
- Identify the issues that you should consider when verifying the routing information flow

in an MPLS VPN

- Describe the process used to validate CE-to-PE routing information flow
- Describe the process used to validate PE-to-PE routing information flow
- Describe the process used to validate PE-to-CE routing information flow
- Identify the issues that you should consider when verifying the data flow in an MPLS VPN
- Describe how to validate Cisco Express Forwarding status
- Describe how to validate the end-to-end ILSP
- Describe how to validate the LFIB status

Module 6: Complex MPLS VPNs

Lesson 1: Introducing Overlapping VPNs

- Identify the participants in overlapping VPNs
- Identify typical overlapping VPN usages
- Describe the routing update flow in an overlapping VPN
- Describe the data flow in an overlapping VPN
- Configure overlapping VPNs

Lesson 2: Using Advanced VRF Import and Export Features

- Identify advanced VRF features
- Configure selective VRF imports
- Configure selective VRF exports

Module 7: Internet Access and MPLS VPNs

Lesson 1: Combining Internet Access with MPLS VPNs

- Describe common customer Internet connectivity scenarios
- Identify the two major design models for combining Internet access with MPLS VPN services
- Describe the benefits and drawback of Internet access through global routing
- Describe the benefits and drawback of Internet access in a separate VPN
- Describe the disadvantages of providing Internet access through route leaking

Module 8: MPLS TE Overview

Lesson 1: Introducing Traffic Engineering Concepts

- Identify the concepts behind TE
- Identify the major business drivers for implementing TE
- Identify congestion avoidance and how TE can reduce some congestion-avoidance issues
- Identify how TE is implemented using a Layer 3 model
- Identify how TE is implemented using the MPLS-TE model

Lesson 2: Configuring MPLS Traffic Engineering on Cisco IOS Platforms

- Identify the tasks that are required to implement MPLS TE
- Enable device-level MPLS TE support
- Enable MPLS TE support in an OSPF environment
- Enable MPLS TE on an interface
- Create and configure a traffic tunnel
- Enable traffic tunnels with autoroute

Implementing QoS v2.3

- Introduction to QoS
 - Understanding the Need for QoS
 - Understanding QoS
 - Implementing QoS

- The Building Blocks of QoS
 - Identifying Models for Implementing QoS
 - Understanding the Integrated Services Model
 - Understanding the Differentiated Services Model
 - Identifying QoS Mechanisms
- Introduction to MQC and Cisco AutoQoS
 - Introducing Modular QoS CLI
 - Introducing Cisco AutoQoS VoIP
 - Introducing Cisco AutoQoS for the Enterprise
- Classification and Marking
 - Understanding Classification and Marking
 - Using MQC for Classification
 - Using MQC for Class-Based Marking
 - Using NBAR for Classification
 - Configuring QoS Preclassify
 - Configuring QoS Policy Propagation via BGP
 - Configuring LAN Classification and Marking
 - Understanding QoS in the Life of a Packet
- Congestion Management
 - Introducing Queuing
 - Understanding Queuing Implementations
 - Configuring FIFO and WFQ
 - Configuring CBWFQ and LLQ
 - Configuring LAN Congestion Management
- Congestion Avoidance
 - Introducing Congestion Avoidance
 - Introducing RED
 - Configuring Class-Based Weighted RED
 - Configuring Explicit Congestion Notification
- Traffic Policing and Shaping
 - Understanding Traffic Policing and Shaping
 - Configuring Class-Based Policing
 - Configuring Class-Based Shaping
 - Configuring Class-Based Shaping on Frame Relay Interfaces
 - Frame Relay Voice-Adaptive Traffic Shaping and Fragmentation
- Link Efficiency Mechanisms
 - Understanding Link Efficiency Mechanisms
 - Configuring Class-Based Header Compression
 - Configuring Link Fragmentation and Interleaving
- QoS Best Practices
 - Understanding Traffic Classification Best Practices
 - Deploying End-to-End QoS