TestOut

Lesson Plans

Building Scalable Cisco Internetworks

(Exam 642-901 BSCI)

Version 2.0

The lessons only experience can teach

Table of Contents

Course Overview

This course prepares students for Exam BSCI 642-901: Building Cisco Scalable Internetworks. It focuses on using advanced IP addressing and routing strategies to employ scalability on Cisco routers.

Module 0 – Introduction

This module introduces the students to the router simulator, which is a learning tool used to complete the simulations throughout the course. An overview of static and dynamic routing as well as classful and classless routing is presented. Students will also be introduced to routing protocol concepts.

Module 1 – EIGRP

This module discusses the functions, configuration, authentication, verification, and troubleshooting of Enhanced Interior Gateway Routing Protocol (EIGRP).

Module 2 – OSPF

This module examines the functions, configuration, authentication, verification, and troubleshooting of Open Shortest Path First (OSPF) routing. Students will become familiar with single-area and multi-area OSPF routing concepts.

Module 3 – IS-IS

In this module students will learn about Intermediate System to Intermediate System (IS-IS). They will learn the role of IS-IS, components associated with IS-IS, configuration, and verification of IS-IS.

Module 4 – Routing Protocol-Independent Features

This module teaches the students about route redistribution, controlling route information through route filtering, and configuring Dynamic Host Configuration Protocol (DHCP) services.

Module 5 – IP Multicast

This module discusses concepts about IP Multicast, Protocol Independent Multicast (PIM), and configuring IP Multicast routing.

Module 6 – IPv6

This module examines the need for IPv6, IPv6 addressing concepts, configuring IPv6 OSPF routing, and interoperation of IPv6 and IPv4.

Module 7 – BGP

In this module students will learn about the functions of Border Gateway Protocol (BGP). They will learn how to configure a router as an internal or external BGP neighbor and configure BGP path selection.

Practice Exams

In Practice Exams students will have the opportunity to test themselves and verify that they understand the concepts and are ready to take the certification exam.

Section 0.1: Introduction

Summary

This section introduces the student to the TestOut router simulator, which is used in most of the lab exercises throughout the course. Students will become familiar with the:

- Process to complete labs
- Elements of the Lab Report box
- Device console
- Icons used to represent network devices and connections

Before you start this course, you should have completed the following course(s) or have equivalent networking experience:

- Cisco Exam 640-802 OR
- Cisco Exam 640-822 AND Exam 640-816

Time

About 5 minutes

Section 0.2: Static and Dynamic Routing Overview

Summary

This section provides an overview of static and dynamic routing. Static routing is an addressing method in which IP configuration information must be built and updated manually on each host by an administrator. Concepts covered about static routing include:

- When to use static routing
- Drawbacks to static routing
- Common types of static routes
    - Default route
    - Floating

Dynamic routing is an addressing method that senses changes in the network topology and responds accordingly without administrator involvement. Concepts covered about dynamic routing include:

- Role of dynamic routers
- Role of dynamic addresses
- Common routing protocols
    - Border Gateway Protocol (BGP)
    - Enhanced Interior Gateway Routing Protocol (EIGRP)
    - Intermediate System-to-Intermediate System (IS-IS)
    - Open Shortest Path First (OSPF)
    - Routing Information Protocol (RIP)

Students will learn how to:

- Use static route configuration commands to create a static route.

Lecture Focus Questions:

- Under which circumstances would you choose static routing over dynamic routing?
- What is the main purpose of a floating static route?
- What are the advantages of using On-Demand Routing (ODR)?

Time

About 10 minutes

Section 0.3: Classful and Classless Routing Overview

Summary

This section provides an overview of classful and classless routing.

- Classful addresses are IP addresses that use the default subnet mask.
- Classless addresses are those that use a custom mask value to separate the network and host portion of the IP address.
- The differences between classful and classless routing are presented.

Students will learn how to:

- Select protocols which require manual summarization.

Lecture Focus Questions:

- What is the major limitation of a classful routing environment?
- How does classless routing improve upon classful routing?
- Which routing protocols support classless routing?

Time

About 7 minutes

Section 0.4: Routing Protocols Introduction

Summary

This section introduces routing protocol concepts. Students will become familiar with:

- *Distance vector* is a routing protocol in which routers send their routing tables at regular intervals to neighboring routers and routers modify their tables based on information received from their neighbors.
    - Routers are susceptible to a routing loop
    - Methods to minimize a routing loop include:
        - Split horizon
        - Split horizon with poison reverse
        - Triggered updates
        - Hold-downs
    - Advantages of using a distance vector method
    - Disadvantages of using a distance vector method
- *Link-State routing* is a routing protocol in which routers broadcast Link-State Packets (LSPs) to all routers in a network or specific area of a network only when there is a change.
    - Link-state protocol process
    - Advantages of using the link-state method over distance vector method
    - Possible problems with the link-state method
        - Requires greater CPU and memory capability
        - Generates a high amount of traffic during initial configuration
        - Delay or loss of LSPs
- *Hybrid routing* is a combination of the distance vector protocol and the link-state protocol.
    - Enhanced Interior Gateway Routing Protocol (EIGRP) is a well-known hybrid routing protocol.

Lecture Focus Questions:

- What causes bridging loops when you are using the distance vector routing protocol?
- Why is the term *routing by rumor* used to refer to distance vector routing?
- When using link-state routing what methods can be used to remedy the effects of inconsistent LSP information?
- In hybrid routing, where is routing information sent after a topology change?
- What is the only routing protocol that is currently considered a hybrid?

Time

About 10 minutes

Section 1.1: EIGRP

Summary

This section discusses the Enhanced Interior Gateway Routing Protocol (EIGRP). EIGRP is a Cisco-proprietary balanced hybrid routing protocol that combines the best features of distance vector and link-state routing. Concepts covered about EIGRP include:

- Features of EIGRP
- EIGRP processes
- EIGRP packets and messages:
  - Hello
  - Query
  - Reply
  - Update
  - Acknowledge (ACK)
  - Goodbye
- EIGRP packet details:
  - Retransmit Time-Out (RTO)
  - Smooth Round Trip Time (SRTT)
  - Split Horizon and Poison Reverse
  - Stub routing
- EIGRP tables:
  - Neighbor table
  - Topology table
  - Routing table
- Diffusing Update Algorithm Link-state (DUAL) computes route information using:
  - Advertised Distance (AD)
  - Feasible Distance (FD)
  - Successor
  - Feasible Successor

Students will learn how to:

- Given a scenario, calculate the Feasible Distance and the Feasible Successor.

Building Scalable Cisco Internetworks Objectives

- 101. Explain the functions and operations of EIGRP (e.g., DUAL).

Lecture Focus Questions:

- How does EIGRP minimize network bandwidth usage for routing updates?
- Under what circumstances are hello packets sent every 5 seconds or every 60 seconds?

- How do the two types of EIGRP tables differ (e.g. neighbor table vs. topology table)?
- What is the purpose of DUAL and what elements does it use to perform this function?

Time

About 30 minutes

Number of Exam Questions

6 questions

Section 1.2: EIGRP Configuration

Summary

In this section students will learn EIGRP configuration concepts.

- Conditions that must be met for an EIGRP router to share information with a neighbor.
  - Both routers must be configured with the same AS number.
  - Both routers are on the same subnet with the same subnet mask.
  - If used, authentication checks must pass.
  - Metric values (K values) must match on both routers.

- Configure EIGRP by using commands to:
  - Define an EIGRP process with an Autonomous System (AS) number.
  - Identify a network that participates in the route process.
  - Turn off automatic route summarization.
  - Configure a summary address on the specified interface.
  - Configure the bandwidth to be used by EIGRP on an interface in kbps.
  - Configure the percentage of bandwidth that may be used by an EIGRP AS on an interface.
  - Configure a router as an EIGRP stub.
  - Modify the stub routing configuration.
  - Create a default route within EIGRP.

Students will learn how to:

- Given a scenario, configure and verify classful EIGRP routing.
- Given a scenario, configure routers to share classless routing information using EIGRP.
- Configure and verify EIGRP summary addresses on a specified interface.
- Configure EIGRP stub routing on a specified router.

Building Scalable Cisco Internetworks Objectives

- 102. Configure EIGRP routing. (e.g., Stub Routing, authentication, etc.)

Lecture Focus Questions:

- What is the purpose of the Autonomous System (AS) number?
- How do you run multiple instances of EIGRP on the same router?
- Why would you add the wild card bit mask to the **network** command?
- What conditions must match on both EIGRP routers for them to share information?

- By default, EIGRP packets can consume a maximum of 50 percent of the link bandwidth, how does EIGRP know the actual bandwidth on the link?

Time

About 50 minutes

Lab/Activity

- Configure Classful EIGRP Routing
- Configure Classless EIGRP Routing
- Configure EIGRP Summary Addresses
- Configure EIGRP Stub Routing

Number of Exam Questions

15 questions

Section 1.3: EIGRP Authentication

Summary

This section examines EIGRP Authentication. Students will become familiar with how to configure EIGRP authentication by using commands to:

- Enable MD5 authentication in EIGRP packets on the specified interface.
- Enable authentication of EIGRP packets and specify the name of the authentication key chain from which the key will be obtained for this interface.
- Identify a specific key chain and enter the key chain's configuration mode.
- Identify the key number.
- Configure the key-string (password) used to authenticate sent and received EIGRP packets.
- Cause the key-string to be stored and displayed in encrypted form.
- Confirm that an interface is receiving or rejecting packets from EIGRP adjacent neighbors.

Students will learn how to:

- Configure MD5 authentication for routers running EIGRP.

Building Scalable Cisco Internetworks Objectives

- 102. Configure EIGRP routing. (e.g., Stub Routing, authentication, etc.)

Lecture Focus Questions:

- Why is simple password authentication vulnerable to passive attacks?
- When configuring md5 authentication, what is the purpose of the key chain?
- What authentication values must match for routers to exchange EIGRP update packets?

Time

About 15 minutes

Lab/Activity

- Configure EIGRP Authentication

Number of Exam Questions

3 questions

Section 1.4: EIGRP Verification and Troubleshooting

Summary

This section provides commands that can be used for EIGRP verification and troubleshooting. Students will learn commands that can be used to display:

- EIGRP configuration information.
- Interfaces that are sending and receiving EIGRP updates.
- The metric used by EIGRP to calculate the Feasible Distance (FD).
- The IP address and local interface of neighbor routers.
- The number EIGRP hello, update, query, reply, and acknowledgment packets which have been sent and received.
- The contents of the topology table for EIGRP.

Students will learn how to:

- Use **show** commands to display router information.
- Use the **show ip route** and **show ip protocols** commands to troubleshoot and verify router information.
- Use **ping** to verify connectivity between routers.

Building Scalable Cisco Internetworks Objectives

- 103. Verify or troubleshoot EIGRP routing configurations.

Lecture Focus Questions:

- Which command can you use to identify why specific routes can't be seen in the routing table?
- Which show command will you use to verify that two routers are configured with the same autonomous system number?
- From the **sh ip eigrp topology** command output, what does S in front of the route indicate?

Time

About 40 minutes

Lab/Activity

- Find EIGRP Information
- Troubleshoot EIGRP 1
- Troubleshoot EIGRP 2

Number of Exam Questions

19 questions

Section 2.1: OSPF Overview

Summary

This section provides an overview of Open Shortest Path First (OSPF), a link-state protocol commonly used in IP networking. Concepts discussed include:

- How OSPF works and the elements involved in the process
- OSPF forces a two-layer hierarchy based on areas. Two-layer hierarchy details include:
  - The role of Area 0 or backbone area
  - The role of regular or non-backbone areas
  - Benefits provided
    - Minimized routing tables
    - Minimized effort to update and propagate topological changes within areas
    - Summarization
    - LSA flooding is stopped at the area boundary
- Details about using OSPF
- OSPF packets:
  - Type 1 packets are hello packets
  - Type 2 packets are Database Description (DBD) packets
  - Type 3 are Link-State Request (LSR) packets
  - Type 4 packets are Link-State Update (LSU) packets
  - Type 5 packets are Link-State Acknowledgement (LSAck) packets
- Details about OSPF packets:
  - All OSPF packets are directly encapsulated into an IP payload.
  - OSPF packets do not use TCP or UDP.
  - Because TCP is not implemented, OSPF defines its own route for acknowledgement that uses LSAcks.
- All OSPF packets begin with the same header format, which includes the following fields:
  - Version number
  - Type
  - Packet length
  - Router ID
  - Area ID
  - Checksum
  - Authentication type
  - Packet-dependent data
- Conditions for two routers to become OSPF neighbors
- Adjacent neighbor router states:
  - Down
  - Init
  - 2-way
  - Exstart

    - Exchange
    - Full
- Environments that OSPF establishes adjacencies in:
    - Peer-to-peer
    - Multi-access (multi)
- Router roles:
    - Designated Router (DR)
    - Backup Designated Router (BDR)
    - DROTHER
- OSPF recognizes the following types of networks:
    - Point-to-point
    - Broadcast
- Non-Broadcast Multiple Access (NBMA) networks:
    - In the star topology
    - In the full-mesh topology
    - In the partial-mesh topology
- Cisco recognizes the following types of additional NBMA networks:
    - NBMA Non-Broadcast
    - NBMA Point-t-Multipoint
    - NBMA Broadcast
    - NBMA point-to-multipoint with none-broadcast
    - NBMA point-to-point

Building Scalable Cisco Internetworks Objectives

- 201. Explain the functions and operations of multiarea OSPF.

Lecture Focus Questions:

- Which steps does OSPF use to select the best path in the routing database?
- What conditions must be met for two routers to become OSPF neighbors?
- What happens when a Designated Router (DR) on a LAN fails and then regains service?
- What are the major differences between an OPSF point-to-point and a broadcast network type?

Time

About 40 minutes

Number of Exam Questions

7 questions

Section 2.2: Single-area OSPF Configuration

Summary

This section presents commands and details for configuring single-area OSPF. Students will become familiar with the commands to:

- Enter configuration mode for OSPF for the specified process ID.
- Identify the networks that participate in OSPF routing.
- Configure the router ID for the OSPF process.
- Set the OSPF priority number for the specified interface.
- Sets an IP address for a loopback interface.
- Configure the OSPF network type to a type other than the default given the medium.
- Configure OSPF neighbors on routers that interconnect to non-broadcast networks.
- Specify a cost for the neighbor.

Students will learn how to:

- Configure routers to share routing information using OSPF.
- Run OSPF for area 0 on all interfaces of a specified router.
- Configure specified routers as the Designated Router (DR) and Backup Designated Router (BDR).

Building Scalable Cisco Internetworks Objectives

- 202. Configure multiarea OSPF routing. (e.g., Stub, NSSA, authentication, etc.)

Lecture Focus Questions:

- What happens when the **area id** is different between routers?
- What happens when the **process id** is different between routers?
- What would you do to ensure that a router never becomes the Designated Router (DR) or Backup Designated Router (BDR)?

Time

About 50 minutes

Lab/Activity

- Configure Single-area OSPF Routing
- Exploring OSPF Routing
- Configure Designated and Backup Designated Routers

Number of Exam Questions

10 questions

Section 2.3: Multi-area OSPF Concepts

Summary

This section discusses multi-area OSPF. Concepts covered include:

- Factors that may cause network performance issues on a large OSPF networks include:
  - Excessive CPU usage due to frequent calculations of the SPF algorithm.
  - Unmanageably large routing tables and LSDBs.
- Hierarchical routing is the process of dividing the network into multiple OSPF areas that are smaller and more manageable. Types of routers used by hierarchical routing include:
  - Internal router
  - Backbone router
  - Area Border Router (ABR)
  - Autonomous System Boundary Router (ASBR)
- Types of LSA traffic generated by OSPF:
  - Type 1 (Router LSA)
  - Type 2 (Network LSA)
  - Type 3 and 4 (Summary LSA)
  - Type 5 (AS external LSA)
  - Type 6 (Multicast OSPF LSA)
  - Type 7 (Defined for Not-So-Stubby areas)
  - Type 8 (External attributes LSA for BGP)
  - Type 9, 10, or 11 (Opaque LSA)
- The process of when an ABR receives summary or external LSAs.
- Route summarization:
  - Inter-area
  - External
- OSPF area types
- Backbone or Area 0
- Stub
- Totally stubby
- Not-So-Stubby Area (NSSA)

Students will learn how to:

- Identify the current domain and forest functional levels.
- Raise the functional levels of domains and forests.

Building Scalable Cisco Internetworks Objectives

- 201. Explain the functions and operations of multiarea OSPF.

Lecture Focus Questions:

- What benefits does hierarchical routing provide for OSPF networks?
- Under what circumstances can a router be more than one router type?
- What is the purpose of OSPF generating traffic based upon different LSA types?
- Why might a large network require summarization?
- What is the difference between a stub area and a totally stubby area?

Time

About 30 minutes

Number of Exam Questions

2 questions

Section 2.4: Multi-area OSPF Configuration

Summary

In this section students will explore configuring multi-area OSPF. Students will become familiar with the commands to:

- Enter the configuration mode for OSPF for the specified process ID.
- Identify the networks that participate in OSPF routing.
- Configure a virtual link to the backbone area.
- Configure route summarization on an Area Border Router (ABR).
- Configure route summarization on an Autonomous System Boundary Router (ASBR).
- Generate a default external route into an OSPF routing domain.

Students will learn how to:

- Configure multi-area OSPF routing.

Building Scalable Cisco Internetworks Objectives

- 202. Configure multiarea OSPF routing. (e.g., Stub, NSSA, authentication, etc.)

Lecture Focus Questions:

- What is another name for the backbone area in a multi-area OSPF configuration?
- In multi-area OSPF configurations, how would you connect the backbone area to other areas?
- Which area ID is used when configuring a virtual link to the backbone area?

Time

About 25 minutes

Lab/Activity

- Configure Multi-area OSPF Routing 1
- Configure Multi-area OSPF Routing 2

Number of Exam Questions

2 questions

Section 2.5: OSPF Stub and NSSA Configuration

Summary

This section discusses the commands for configuring OSPF stub and NSSA routers. Students will become familiar with the commands to:

- Set the routing process as being part of a stub area.
- Stop Type 3, 4, and 5 LSAs sent into a stub area from the ABR, but allow a single default route into the stub area.
- Define an area to be an NSSA.
- Import routes only into the normal areas, but not into the NSSA area on an NSSA Area Border Router (ABR).
- Generate a Type 7 default route into the NSSA area.
- Set the OSPF default metric.
- Set the OSPF metric type for default routes.
- Allow an area to be an NSSA, but not have summary routes injected into it.

Students will learn how to:

- Configure OSPF stub routing and restrict specified LSAs from being sent into an area.

Building Scalable Cisco Internetworks Objectives

- 202. Configure multiarea OSPF routing. (e.g., Stub, NSSA, authentication, etc.)

Lecture Focus Questions:

- How can you configure a router not to send external routes into a stub area?
- How can you configure a router not to send external and summary routes into a stub area?
- To properly configure a stub area, which routers should have the stub command in the routing process?
- How can you generate a default router into a not-so-stubby area?

Time

About 15 minutes

Lab/Activity

- Configure OSPF Stub Routing

Number of Exam Questions

2 questions

Section 2.6: OSPF Authentication

Summary

This section examines configuring neighbor authentication in OSPF to prevent routers from receiving fraudulent route updates and allow routers to participate in routing based on predefined passwords.

- OSPF supports the following methods of authentication:
  - Simple Password Authentication Protocol
  - Message Digest Authentication (MD5)
- Students will become familiar with the commands to:
  - Enable plain-text authentication (i.e., simple password authentication) in OSPF packets on the specified interface.
  - Configure a plain-text password for OSPF authentication.
  - Enable MD5 authentication in OSPF packets on the specified interface.
  - Enable authentication of OSPF packets and specify the key number and password for the interface.
  - Cause the key-string to be stored and displayed in encrypted form.

Building Scalable Cisco Internetworks Objectives

- 202. Configure multiarea OSPF routing. (e.g., Stub, NSSA, authentication, etc.)

Lecture Focus Questions:

- How does neighbor authentication provide security from fraudulent route updates?
- Which of the two authentication methods supported by OSPF is the most secure?
- How can you prevent an authentication key-string from being displayed in plain text within the running configuration file?

Time

About 8 minutes

Number of Exam Questions

1 questions

Section 2.7: OSPF Verification and Troubleshooting

Summary

In this section students will learn about verifying and troubleshooting an OSPF configuration. Concepts covered include:

- Conditions that must be met for two routers to become fully adjacent
- Commands to:
  - Display OSPF configuration information
  - Display OSPF information
  - Display information about neighbor OSPF routers
  - Display interfaces that are running OSPF
  - Display the current state of OSPF virtual links
  - Display the information related to the OSPF database for a specific router
  - Display all routes in the routing table.
  - Display debugging information about hello exchanges, DR selection information, SPF calculation, and errors related to negotiating adjacency
- Error messages that display with the **debug ip ospf events** command:
  - OSPF: mismatched hello parameters from 10.0.0.1
    OSPF: Dead R 20 C 40, Hello R 5 C 5
    Mask R 255.255.255.0 C 255.255.255.0
  - OSPF: hello packet with mismatched E bit
  - Neighbor Down: Dead timer expired

Students will learn to:

- Verify OSPF routing information.
- Troubleshoot and modify OSPF routing configurations appropriately to enable connectivity.

Building Scalable Cisco Internetworks Objectives

- 203. Verify or troubleshoot multiarea OSPF routing configurations.

Lecture Focus Questions:

- What conditions must be met for OSPF routers to be considered fully adjacent neighbors?
- If two adjacent neighbor routers have different OSPF process IDs, will they be able to communicate?
- How can you determine which router is the Designated Router (DR)?

Time

About 35 minutes

Lab/Activity

- Find OSPF Information
- Troubleshoot OSPF 1
- Troubleshoot OSPF 2

Number of Exam Questions

17 questions

Section 3.1: IS-IS

Summary

This section examines Intermediate System to Intermediate System (IS-IS). Concepts covered include:

- The role of IS-IS
- IS-IS terms:
  - Intermediate System (IS)
  - End System (ES)
  - End System to Intermediate System Routing Exchange Protocol (ES-IS)
  - Integrated IS-IS
- Routing components associated with IS-IS
- OSI levels:
  - Level 0
  - Level 1
  - Level 2
  - Level 3
- IS-IS router types:
  - L1 routers
  - L2 routers
  - L1/L2 routers
- Protocol Data Unit (PDU) types:
  - Hello PDU
  - Link-State PDU (LSP)
  - Sequence Number PDU (SNP)
- OSI network-layer addresses identify:
  - Network Service Access Point (NSAP)
    - Initial Domain Part (IDP)
    - Domain-Specific Part (DSP)
  - Network Entity Title (NET)
    - Area address
    - System ID
    - NSEL
- IS-IS network types:
  - Point-to-point
  - Broadcast
- Comparison of IS-IS and OSPF:
  - Similarities
  - Differences

Building Scalable Cisco Internetworks Objectives

- 301. Describe the features and benefits of integrated IS-IS.

Lecture Focus Questions:

- What term is used by OSI to describe a router?
- What term is used by OSI to describe a host?
- Which two network layer protocols are supported by Integrated IS-IS?
- Which type of IS-IS router is equivalent to an ABR in OSPF?
- How are OSPF and IS-IS similar and different?

Time

About 35 minutes

Number of Exam Questions

8 questions

Section 3.2: IS-IS Configuration and Verification

Summary

In this section students will learn about configuring and verifying an IS-IS configuration. Concepts covered include:

- Considerations when planning an IS-SI configuration
- IS-IS router deployment:
  - Manually configure IS-IS router, otherwise it will be a L1/L2 device by default.
  - Manually enable summarization
- Configuring IS-IS with commands to:
  - Enter configuration mode for an IS-IS routing process.
  - Identify the IS-IS Network Entity Title (NET) on the router. A NET is a Network Service Access Point (NSAP) where the last byte is always zero.
  - Configure the routing level for the IS-IS routing process.
  - Configure an IS-IS routing process for IP on an interface and attach an area designator to the routing process.
  - Configure the type of adjacency.
  - Configure the priority of designated routers, or Designated Intermediate Systems (DIS).
  - Configure the value of an IS-IS metric.
  - Create a summary address for IS-IS.
  - Disable the IS-IS protocol so that it cannot form adjacencies on a specified interface.
  - Prevent IS-IS from forming any adjacency on any interface and clears the IS-IS LSP database.
- Verifying IS-IS with commands to:
  - Display all routes in the routing table.
  - Display the current state of the active routing protocol processes.
  - Verify the presence and connectivity of all known routers in all areas.
  - Display the protocol-specific information for each IS-IS routing process in the router.
  - Display ES, IS, and Multi-topology Integrated Intermediate System-to-Intermediate System (M-ISIS) neighbors. The output verifies that the correct adjacencies are established.
- Understanding command output:
  - System ID
  - Subnetwork Point of Attachment (SNPA)
  - Type values:
    - ES
    - IS
    - M-ISIS
    - L1
    - L1L2
    - L2

Students will learn how to:

- Configure IS-IS Intra-area routing.
- Configure IS-IS Inter-area routing.
- Use the appropriate **show** commands to display and verify IS-IS information.

Building Scalable Cisco Internetworks Objectives

- 302. Configure and verify integrated IS-IS.

Lecture Focus Questions:

- What should you consider when planning an IS-IS configuration?
- What could be the problem of leaving an IS-IS router configured as the default Level 1/2 router type?
- How would you verify if IS-IS summarization has been enabled during a deployment?
- Which **show** command can you use to verify the establishment of correct adjacencies?

Time

About 45 minutes

Lab/Activity

- Configure IS-IS Intra-area Routing
- Configure IS-IS Inter-area Routing
- Find IS-IS Information

Number of Exam Questions

5 questions

Section 4.1: Route Redistribution

Summary

This section discusses using route redistribution to connect to different routing domains to exchange and advertise routing information. Concepts covered include:

- Migration to a new protocol involves:
  - Developing a timeline of what changes need to occur.
  - Identifying the edge (the old protocol) and the core (the new protocol).
  - Identifying which routers will be used for redistribution.
  - Testing routers in a lab environment before implementing redistribution to make sure the routers can function with the new protocol.
- Types of route redistribution:
  - One-way redistribution
  - Two-way redistribution
- Route redistribution techniques
- Default values when redistributing into the following protocols:
  - RIP
  - OSPF
  - EIGRP
  - IS-IS
- Items to be aware of:
  - Routing feedback
  - Incompatible routing information
  - Different convergence times
  - Default metric 0 interpreted as infinity
  - Steps to configure a route distribution
- Configuring routing protocol redistribution with commands to:
  - Enter an EIGRP routing process and then redistribute routes into the EIGRP routing process.
  - Enter an OSPF routing process and then redistribute routes into the OSPF routing process.
  - Enter an IS-IS routing process and then redistribute routes into the IS-IS routing process.
  - Force the current routing protocol to use the same metric value for all redistributed routes. This applies to BGP, OSPF, and RIP.
  - Force the EIGRP routing protocol to use the same metric value for all non-EIGRP redistributed routes.
  - Automatically bring the connected networks/subnets into the routing protocol, just as if you had used multiple **network** commands within the routing process.
  - View the redistributed routing process(es) within a specific routing process.
  - Verify the presence of redistributed routes.

Students will learn how to:

- Configure EIGRP and OSPF route redistribution.
- Configure IS-IS and OSPF route redistribution.
- Configure EIGRP and RIP route redistribution.
- Configure EIGRP and IS-IS route redistribution.

Building Scalable Cisco Internetworks Objectives

- 401. Describe, configure or verify route redistribution between IP routing IGPs. (e.g., route-maps, default routes, etc.)

Lecture Focus Questions:

- What circumstances may require you to take advantage of route redistribution?
- What kind of problems can occur when using route redistribution?
- Of the two types of route redistribution, which is the most reliable?
- Why is it important to recognize that the seed metric of different protocols is based upon different elements?
- How can proper redistribution strategies help to eliminate route feedback and routing loops?

Time

About 45 minutes

Lab/Activity

- Configure EIGRP and OSPF Route Redistribution
- Configure IS-IS and OSPF Route Redistribution
- Configure EIGRP and RIP Route Redistribution
- Configure EIGRP and IS-IS Route Redistribution

Number of Exam Questions

6 questions

Section 4.2: Controlling Route Information

Summary

This section provides information about methods and commands to control route information. Concepts covered include:

- Methods to control routing information:
  - Passive interface
  - Default routes
  - Static routes
  - Distribute list
  - Route map
- Configure passive interfaces with commands to:
  - Prevent routing updates from being sent out on an interface, yet the particular subnet on the interface will continue to be advertised to other interfaces and networks.
  - Force all interfaces to become passive where they are not sending routing updates.
- Configure distribute lists with commands to:
  - Filter networks received in updates on a specified interface based on a standard IP access list number. This prevents the processing of certain routes.
  - Filter networks received in updates based on a specified route map.
  - Filter networks sent in updates based on a standard IP access list number.
  - Create an access list which permits all traffic.
  - Create an access list which permits traffic from a specified network.
  - View the distribute list applied to the routing process.
  - Display all access lists that exist on the router.
- Configure road maps with commands to:
  - Define a route map to control where packets are sent and enter the route map configuration mode.
  - Set the position of a new route map in the list of route maps already configured with the same name.
  - Match CLNS information.
  - Match any routes that have their next hop out one of the interfaces specified.
  - Match any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
  - Match any routes that have a next hop router address passed by one of the access lists specified.
  - Match routes that have been advertised by routers and access servers at the address specified by the access lists.
  - Match the minimum and maximum packet lengths.

- Match routes with the metric specified.
- Match routes of specified types.
- Match the source protocol, such as EIGRP, OSPF, or IS-IS.
- Match routes in the routing table that match the specified tags.
- Set the metric value for a routing protocol.
- Set the metric-type for the OSPF and IS-IS routing protocols.
- Specify the next hop to which to route the packet.
- Specify the next hop to which to route the packet, if there is no explicit route for this destination.
- Specify the output interface for the packet. (supported only over point-to-point links.)
- Specify the output interface for the packet if there is no explicit route for the destination.
- Set the precedence value in the IP header.
- Set the routes with the specified tag.
- Delete the specified route map.
- Use a route map to filter the incoming of routes from the source routing protocol to the current routing protocol.
- Filter networks received in updates based a specified route map.
- Identify the route map to use for policy routing on the specified interface.
- Display all route maps configured or only the one specified route map.

Students will learn how to:

- Configure passive interfaces, distribute lists, and route maps.

Building Scalable Cisco Internetworks Objectives

- 401. Describe, configure or verify route redistribution between IP routing IGPs. (e.g., route-maps, default routes, etc.)
- 402. Describe, configure or verify route filtering (i.e., distribute-lists and passive interfaces).

Lecture Focus Questions:

- Under what circumstances would you most likely use passive interface?
- How can you limit EIGRP updates from being sent to a router while still maintaining the neighborship?
- How can default routes help to reduce the use of network resources caused by dynamic routing?
- What is the difference between a distribute list and a route map?
- How do distribute lists and route maps use access lists?

Time

About 75 minutes

Lab/Activity

- Configure a Passive Interface
- Configure a Distribute List 1
- Configure a Distribute List 2
- Configure a Route Map

Number of Exam Questions

8 questions

Section 4.3: DHCP

Summary

In this section students will learn the basics of the Dynamic Host Configuration Protocol (DHCP). Concepts covered include:

- DCHP configuration parameters:
  - Address pool
  - Lease
  - DCHP options
  - Binding
  - Database agent
- The process a DHCP client uses to obtain an IP address:
  - Lease Request
  - Lease Offer
  - Lease Selection
  - IP Lease Acknowledgement
- Allocation methods supported by DHCP:
  - Manual
  - Automatic
  - Dynamic
- Preparation steps for configuring a DHCP server
- Completing the DHCP configuration with commands to:
  - Enable DHCP features on the router.
  - Configure a DHCP server to save automatic bindings on the database agent.
  - Disable DHCP address conflict logging.
  - Exclude addresses from being assigned.
  - Create a DHCP pool. Pools are used to define a range of addresses to assign, as well as create bindings.
  - Identify the subnet address and mask for the address pool.
  - Set the domain name to be delivered to hosts.
  - Identify DNS server addresses delivered to hosts.
  - Identify the default gateway address that will be assigned to hosts.
  - Configure the IP address lease time (in days).
  - Create a binding.
  - Configure a Cisco device, such as a Catalyst switch, to get its IP address from the DHCP server.
  - Execute an immediate renewal or release of a DHCP lease for the specified interface.
  - Enable a DHCP server to selectively ignore and not reply to received Bootstrap Protocol (BOOTP) request packets.
  - Display count information about server statistics and messages sent and received.

    - Display a list of all bindings created on a specific DHCP server.
    - Display information about the DHCP address pools.
    - Display address conflicts found by a DHCP server when addresses are offered to the client.
    - Display DHCP server database agent information.
    - Display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.
- The role of a DHCP Relay Agent
- Details about a DHCP Relay Agent
- Configuring a Cisco router as a DHCP relay agent with commands to:
    - Configure an interface to forward UPD broadcasts, including BOOTP and DHCP, via IP unicast, to the specified DHCP server address.
    - Control which broadcast packets and protocols are forwarded from the relay agent.

Students will learn how to:

- Configure a router as a DHCP server.
- Configure a server to always receive the same IP address through DHCP.
- Configure an interface to request an IP address through DHCP.
- Configure a router as a DHCP Relay Agent.

Building Scalable Cisco Internetworks Objectives

- 403. Describe and configure DHCP services (e.g., Server, Client, IP helper address, etc.).

Lecture Focus Questions:

- What is the difference between automatic and dynamic address allocation?
- When you are creating a DHCP manual binding, what are you permanently binding together?
- Which devices can be configured to act as DHCP relay agents?
- Under what circumstances will the *giaddr* field be zero?
- What is the purpose of option 82 in the DHCP packet?

Time

About 50 minutes

Lab/Activity

- Configure a DHCP Server
- Configure DHCP Manual Bindings
- Configure a DHCP Relay Agent

Number of Exam Questions

16 questions

Section 5.1: IP Multicast

Summary

This section provides an overview of IP Multicast. Concepts covered include:

- The role of multicast
- Advantages of multicast
- Disadvantages of multicast
- Protocols used by multicast to locate and transmit multicast traffic:
    - Session Description Protocol (SDR)
    - Internet Group Management Protocol (IGMP)
    - Cisco Group Management Protocol (CGMP)
    - Distance Vector Multicast Routing Protocol (DVMRP)
- Address subranges for:
    - Glop Addresses that are reserved for statically defined addresses
    - Reserved Link Local Addresses
    - Globally Scoped Addresses
    - Limited Scope Addresses
- Mapping Multicast IPs to MAC Addresses

Building Scalable Cisco Internetworks Objectives

- 601. Describe IP Multicast (e.g., Layer-3 to Layer-2 mapping, IGMP, etc.).

Lecture Focus Questions:

- When would you choose to use multicast over broadcast transmission?
- Which packet distribution model is best for a video distribution scenario?
- What services does IGMP Snooping provide?
- Which multicast protocol is most commonly used as a multicast switching solution?
- What is the multicast address range available for Internet use with multicast groups?

Time

About 30 minutes

Number of Exam Questions

8 questions

Section 5.2: Protocol Independent Multicast (PIM)

Summary

This section discusses using Protocol Independent Multicast (PIM). Concepts covered include:

- Terms used in relation to PIM:
  - Distribution tree
    - Source distribution trees
    - Shared distribution trees
  - Reverse Path Forwarding (RPF)
  - PIM Source Specific Multicast (PIM-SSM)
- Rendezvous Point (RP) concepts:
  - Auto-RP
  - Bootstrap Router (BSR)
  - Multicast Source Discovery Protocol (MSDP)
  - Anycast RP
  -
- Multicast modes that PIM uses:
  - PIM Sparse Mode (PIM-SM)
  - PIM Dense Mode (PIM-DM)
  - PIM Sparse-Dense mode
  - Bidirectional PIM
  - PIM Source Specific Multicast (PIM-SSM)

Building Scalable Cisco Internetworks Objectives

- 602. Describe, configure, or verify IP multicasting routing (i.e., PIM Sparse-Dense Mode).

Lecture Focus Questions:

- What is the difference between PIM Sparse mode and PIM Sparse-Dense mode?
- What is the purpose of the PIM group modes?
- In what situation would you select source distribution trees over shared distribution trees?

Time

About 15 minutes

Number of Exam Questions

6 questions

Section 5.3: IP Multicast Routing Configuration

Summary

In this section students will learn about the commands used to configure IP multicast routing. Concepts covered include:

- Configuring IP multicast routing with commands to:
  - Enable IP multicast routing.
  - Enable PIM Sparse mode on the specified interface.
  - Enable PIM Dense mode on the specified interface.
  - Enable PIM Sparse-Dense mode on the specified interface, where the interface is treated as in either sparse mode or dense mode of operation, depending on which mode the multicast group operates in.
  - Send Rendezvous Point (RP) announcements out all PIM-enabled interfaces for Auto-RP configurations.
  - Configure the router to be an RP mapping agent.
  - Configure an interface on the router to join the specified group.
  - Send Rendezvous Point (RP) announcements out all PIM-enabled interfaces for static RP configurations.
- Verifying IP multicast routing with commands to:
  - Display all the entries in the multicast routing (mroute) table, and verify that the mroute table is being populated properly.
  - Display information about interfaces configured for PIM.
  - Display the PIM neighbors.
  - Display the multicast groups with receivers that are directly connected to the router and that were learned through the Internet Group Management Protocol (IGMP).
- Understanding command outputs:
  - Address
  - Ver/Mode
    - SD = Sparse-Dense mode
    - S = Sparse mode
    - D = Dense mode
  - Nbr Count
  - Designated Router (DR)

Building Scalable Cisco Internetworks Objectives

- 602. Describe, configure, or verify IP multicasting routing (i.e., PIM Sparse-Dense Mode).

Lecture Focus Questions:

- How can you configure a Rendezvous Point (RP) in PIM SM?

- What will happen if you do not configure a Rendezvous Point (RP) in PIM Sparse-Dense Mode?
- What do the asterisk(*), S and G in the multicast routing table stand for?
- What is the difference between the discovery of PIM neighbors using PIMv1 and PIMv2?

Time

About 25 minutes

Number of Exam Questions

4 questions

Section 6.1: IPv6

Summary

This section discusses the need for IPv6 and the features it provides. Concepts covered include:

- Issues with IPv4 addresses
- Features of the IPv6 standard:
  - Geographic assignment of addresses
  - Efficient route summarization
  - No need for Network Address Translation (NAT) or Port Address Translation (PAT)
  - Native Internet Protocol Security (IPSec)
  - Header improvements
  - Extension headers
  - Built-in Quality of Service (QoS)
  - Flow label
  - Large address space
  - Stateless and stateful address configuration
  - Neighbor node interaction

Building Scalable Cisco Internetworks Objectives

- 701. Describe IPv6 addressing operations.

Lecture Focus Questions:

- Why was it necessary to implement IPv6?
- What is the strategy for assigning an IPv6 address?
- Why is NAT not needed in an IPv6 environment?
- In a stateless address configuration, how are link-local addresses assigned?

Time

About 10 minutes

Section 6.2: IPv6 Addressing

Summary

This section discusses using IPv6 addressing. Concepts covered include:

- The format of an IPv6 address
- IPv6 address types:
  - Reserved
  - Multicast
  - Unicast
    - Global unicast
    - Link-local
    - Unique-local
  - Anycast
  - Loopback
  - Unspecified
  - Default route
- Subdividing the 64-bit prefix
- Sample assignments of IPv6 addresses for:
  - Regional Internet Registry (RIR)
  - Internet Service Provider (ISP)
  - Site
  - Subnet ID
- Interface IDs
- Methods to configure IPv6 configuration information on a host:
  - Static full assignment
  - Static partial assignment
  - Stateless autoconfiguration
  - DHCPv6
- The process a host uses on start up to configure the IPv6 address for each interface
- Configuring IPv6 addresses with commands to:
  - Configure a global IPv6 address with an interface identifier (ID) in the low-order 64 bits of the IPv6 address.
  - Configure a link-local address on the interface that is used instead of the link-local address that is automatically configured when IPv6 is enabled on the interface.
  - Add an IPv6 anycast address to the specified interface.
  - Verify that IPv6 addresses are configured correctly for the specified interface and validate the IPv6 status.
  - Display a brief summary of IPv6 status and configuration for each interface.

Students will learn how to:

- Implement IPv6 on a network by configuring IPv6 addresses on the interfaces.

Building Scalable Cisco Internetworks Objectives

- 701. Describe IPv6 addressing operations.

Lecture Focus Questions:

- How many bits of data does each quartet represent in an IPv6 address?
- How do you properly abbreviate an IPv6 address?
- What two 64-bit parts are contained in an IPv6 address, and what does each part represent?
- What is the difference between an anycast address and an unicast address?
- What is the function of the local loopback address?
- Why do broadcast addresses not exist in an IPv6 environment?
- Which prefix of an IPv6 address may be used to represent a continent?

Time

About 50 minutes

Number of Exam Questions

13 questions

Section 6.3: IPv6 OSPF Routing

Summary

This section explores using IPv6 OSPF routing. Concepts covered include:

- Changes made to OSPFv2 to accommodate IPv6 with OSPFv3:
  - Default Router ID
  - Multicast addresses
  - LSA types renamed:
    - Type 3 is now intra-area prefix LSA for ABRs.
    - Type 4 is now intra-area router LSA for ASBRs.
  - LSA types added:
    - Type 8 is a link LSA from link-locals.
    - Type 9 is an intra-area prefix to describe the network.
  - Commands
  - Graceful restarts
- Functions of OSPF for IPv6:
  - Shortest Path First (SPF) Throttling
  - Load balancing
  - IPsec authentication
  - Secure socket states
- Configuring IPv6 OSPF routing with commands to:
  - Enable the forwarding of IPv6 unicast packets.
  - Enable OSPF for IPv6 router configuration.
  - Configure the IPv6 router ID for the specified routing process.
  - Enable OSPFv3 for IPv6 on the specified interface.
  - Remove all IPv6 routing protocol entries from the IPv6 routing table.
  - Clear the OSPF database, have it repopulated, and then perform the shortest path first (SPF) algorithm.
  - Display the current contents of the IPv6 routing table.
  - Display the parameters and current state of the active IPv6 routing protocol processes.
  - Display output similar to the **show ip interface** command, but for IPv6-specific information.
  - Display IPv6 Neighbor Discovery (ND) cache information for OSPF on a per-interface basis.

Students will learn how to:

- Configure IPv6 OSPF unicast routing between subnets.

Building Scalable Cisco Internetworks Objectives

- 703. Describe, configure, or verify OSPF routing with IPv6 addressing.

Lecture Focus Questions:

- Which major OSPFv2 changes accommodate IPv6 in OSPFv3?
- What is the main difference between the commands used with OSPF in IPv4 and those used in IPv6?
- How does OSPFv3 handle IPv6 authentication?
- How many IPv6 address prefixes can be configured on a single interface?

Time

About 25 minutes

Number of Exam Questions

5 questions

Section 6.4: IPv6 and IPv4 Interoperation

Summary

This section examines strategies and commands for interoperation of IPv6 and IPv4. Concepts covered include:

- Strategies for deploying IPv6:
  - Dual stack
  - Tunneling
    - Manually configured tunnel
    - 6-to-4 tunneling
    - Intra-site Automatic Tunnel Addressing Protocol (ISATAP)
    - Teredo tunneling
    - Generic Routing Encapsulation (GRE) Tunneling
  - Network Address Translation-Protocol Translation (NAT-PT)
- Configuring IPv6 tunneling with commands to:
  - Enter configuration mode for the tunnel interface.
  - Configure a global IPv6 address with an interface identifier (ID) in the low-order 64 bits of the IPv6 address.
  - Set the source address for a tunnel interface.
  - Set the destination address for a tunnel interface.
  - Configure a static tunnel interface to encapsulate IPv6 over an IPv4 link.
  - Set IPv6 automatic tunneling mode using a 6to4 address.
  - Set IPv6 automatic tunneling mode using an IPv4-compatible IPv6 address.
  - Set IPv6 automatic tunneling mode as Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) to connect IPv6 hosts within IPv4 networks.
  - Enable OSPF routing for IPv6 on the tunnel interface.
  - Display the current contents of the IPv6 routing table.
  - Display IPv6 Neighbor Discovery (ND) cache information for OSPF on a per-interface basis.
  - Display the information for each tunnel running IPv6.
  - Display the information for the tunnel interface.

Building Scalable Cisco Internetworks Objectives

- 702. Describe IPv6 interoperation with IPv4.

Lecture Focus Questions:

- What factors might be involved in an IPv4 to IPv6 migration?
- How does dual stack provide communication with both IPv4 and IPv6 hosts?
- What is the difference between tunneling and NAT-PT?
- What limitations does ISATAP have for IPv6 implementation?

- Which IPv6 tunneling methods work through NAT?
- What is the only method possible to enable an IPv6-only host to communicate with an IPv4-only host?

Time

About 30 minutes

Number of Exam Questions

11 questions

Section 7.1: BGP

Summary

This section provides information about the Border Gateway Protocol (BGP). Concepts covered include:

- The terms related to BGP:
  - Autonomous System (AS)
  - Interior Gateway Protocol (IGP)
  - Exterior Gateway Protocol (EGP)
- The role of BGP
- The role of BGP-4
- BGP concepts:
  - Autonomous System Numbers
  - Modes of operation
    - Internal BGP (iBGP)
    - External BGP (eBGP)
  - Transit AS peering
  - Nontransit AS peering
  - Mutihoming
  - Route aggregation
- Optimal environments to employ BGP
- Suboptimal environments to employ BGP
- Multiprotocol BGP
- BGP address families:
  - Internet Protocol version 4 (IPv4)
  - Internet Protocol version 6 (IPv6)
  - Connectionless Network Service (CLNS)
  - Virtual Private Network Version 4 (VPNv4)
  - Layer 2 Virtual Private Networks (L2VPN)
- Implementation of BGP:
  - Neighbor/peer model
    - BGP speaker
    - BGP peer
    - BGP peer group
  - eBGP neighbors
  - iBGP neighbors
  - full-mesh iBGP
- Messages to communicate between devices:
  - Open
  - Keepalive
  - Update
  - Notification
- BGP states:

    - Idle
    - Connect
    - Active
    - OpenSent
    - OpenReceive
    - Established
- Updating after a BGP policy configuration change occurs by performing a session reset:
    - Hard reset
    - Soft reset
    - Route refresh
- Disabled synchronization facts
- Enabled synchronization facts

Building Scalable Cisco Internetworks Objectives

- 501. Describe the functions and operations of BGP.

Lecture Focus Questions:

- Why is BGP the protocol used between Internet Service Providers (ISPs)?
- What allows for the configuration of BGP policies on a per-address family basis?
- What are the BGP address families?
- What types of messages does BGP use to communicate between devices?
- When performing a session reset, what is the difference between a hard reset and a soft reset?
- Why has the BGP synchronization rule been disabled by default?

Time

About 30 minutes

Number of Exam Questions

5 questions

Section 7.2: BGP Configuration

Summary

This section discusses configuring Internal BGP (iBGP) and External BGP (eBGP). Concepts covered include:

- Configuring BGP routing using commands to:
  - Create a loopback interface and assign an IP address to the interface.
  - Create a BGP routing process with a specified autonomous system number.
  - Configure the neighboring device with a specified autonomous system.
  - To specify the source IP address contained in the BGP packets.
  - Specify which networks to advertise if they are in the IP routing table.
  - Create a static route. For BGP, this is primarily used to reach the eBGP neighbor.
  - Configure eBGP multi-hop with a Time to Live (TTL) value.
  - Configure the next-hop attribute.
  - Create a peer group.
  - Configure a neighbor to be a member of a peer group.
  - Enable Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers.
  - Create an aggregate (or summary) entry in the BGP table.
- Verifying BGP routing using commands to:
  - Display entries in the BGP routing table.
  - Display the neighbor BGP connections.
  - Display BGP neighbor information.
- Understanding command output:
  - Status code
    - s – The table entry is suppressed.
    - d – The table entry is dampened.
    - h – The table entry is history.
    - * -- The table entry is valid.
    - > -- The table entry is the best entry to use for that network.
    - i – The table entry was learned via an internal BGP (iBGP) session.
    - r – When BGP tries to install the bestpath prefix into Routing Information Base (RIB), RIB might reject the BGP route.
  - Next Hop
  - Path

Students will learn how to:

- Configure a router as an internal BGP (iBGP) neighbor.
- Configure a router as an external BGP (eBGP) neighbor.

Building Scalable Cisco Internetworks Objectives

- 502. Configure or verify BGP operation in a non-transit AS (e.g., authentication).

Lecture Focus Questions:

- Why is it a good design strategy to configure loopback addresses before configuring internal BGP?
- What is the main difference between configuring internal BGP (iBGP) and configuring external BGP (eBGP)?
- Which additional configuration is needed to use a loopback address in eBGP?
- What are the rules for creating a password when you enable MD5 authentication between two BGP peers on a TCP connection?
- Which commands are used to troubleshoot and verify BGP operations by displaying details of BGP routing?

Time

About 30 minutes

Lab/Activity

- Configure Internal BGP (iBGP)
- Configure External BGP (eBGP) 1
- Configure External BGP (eBGP) 2

Number of Exam Questions

13 questions

Section 7.3: BGP Path Selection

Summary

This section provides information about BGP path selection. The following concepts are covered.

- BGP attribute definitions:
  - Well-known attributes
    - Well-known mandatory
    - Well-known discretionary
  - Optional attributes
    - Optional transitive
    - Optional nontransitive
- Industry-standard attributes:
  - AS path (type code 2)
  - Next-hop (type code 3)
  - Origin (type code 1)
  - Local preference (type code 5)
  - Community (type code 8)
  - MultiExist-Discriminator (MED) (type code 4)
  - Weight
- The process of path selection
- Configuring and verifying BGP path selection using commands to:
  - Assign a weight to a multihomed connection when there are two IPs.
  - Prepend an arbitrary autonomous system path string to BGP routes to influence inbound BGP path selection.
  - Set the MED metric attribute to influence inbound BGP path selection.
  - Set the local preference attribute to influence outbound path selection.
  - Enforce the MED comparison between all paths, regardless of the autonomous system from which the paths are received.
  - Specify that a community's attribute should be sent to a BGP neighbor.
  - Reset BGP connections using hard or soft reconfiguration.
  - Display all the BGP paths in the database.

Students will learn how to:

- Configure BGP path selection.

Building Scalable Cisco Internetworks Objectives

- 503. Configure BGP path selection (i.e., Local Preference, AS Path, Weight or MED attributes).

Lecture Focus Questions:

- What is the order of the first five attributes used for BGP path selection?
- When is the local preference attribute used?
- If two paths exist to the same destination and each path has a different weight, will the preferred path have the higher weight value?
- How can you enforce the comparison of the MED values for all paths?

Time

About 30 minutes

Number of Exam Questions

3 questions

Practice Exams

Summary

This section provides information to help prepare students to take the exam and to register for the exam.

Students will also have the opportunity of testing their mastery of the concepts presented in this course to reaffirm that they are ready for the certification exam. For example, all questions that apply to **Objective 100. Implement EIGRP operations** are grouped together and presented in practice exam ***100. Implement EIGRP operations, All Questions***. Students will typically take about 60-90 minutes to complete each of the following practice exams.

100. Implement EIGRP operations, All Questions (44 questions)
200. Implement multiarea OSPF operations, All Questions (43 questions)
300. Describe integrated IS-IS, All Questions (13 questions)
400. Implement Cisco IOS routing features, All Questions (29 questions)
500. Implement BGP for enterprise ISP connectivity, All Questions (21 questions)
600. Implement multicast forwarding, All Questions (18 questions)
700. Implement IPv6, All Questions (29 questions)

The *Certification Practice Exam* consists of 60 questions that are randomly selected from the above practice exams. Each time the Certification Practice Exam is accessed different questions may be presented. The Certification Practice Exam has a time limit of 90 minutes -- just like the real certification exam. A passing score of 95% should verify that the student has mastered the concepts and is ready to take the real certification exam.