



Lesson Plans

Implementing Secure Converged Wide Area Networks

(Exam 642-825 ISCW)

Version 2.0

Table of Contents

Course Overview	2
Section 0.1: Introduction.....	3
Section 1.1: Common Network Attacks	4
Section 1.2: Attack Mitigation.....	5
Section 1.3: Vulnerable Router Services and Interfaces.....	6
Section 1.4: Secure Router Management and Reporting	8
Section 1.5: AAA.....	10
Section 2.1: Firewall and ACL Overview.....	11
Section 2.2: Firewall Configuration.....	12
Section 2.3: Firewall Verification.....	13
Section 2.4: Intrusion Detection and Prevention Systems	14
Section 2.5: IPS Configuration	15
Section 3.1: Remote Connectivity Overview.....	17
Section 3.2: Cable	18
Section 3.3: Digital Subscriber Line (DSL).....	19
Section 3.4: DSL Configuration	20
Section 3.5: DSL Verification and Troubleshooting	21
Section 4.1: IPsec Components and Features	22
Section 4.2: Site-to-Site IPsec VPN.....	23
Section 4.3: Generic Routing Encapsulation (GRE) over IPsec.....	24
Section 4.4: Site-to-Site VPN and GRE Tunnel Verification.....	25
Section 4.5: Cisco Easy VPN.....	26
Section 4.6: IPsec High Availability.....	27
Section 5.1: MPLS	28
Section 5.2: MPLS Configuration.....	29
Section 5.3: MPLS VPN Technology.....	30
Practice Exams.....	31

Course Overview

This course prepares students for Exam ISCW 642-825: Implementing Secure Converged Wide Area Networks. It focuses on securing remote access and VPN client configuration.

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.

Module 1 – Attacks, Mitigation, and Device Hardening

This module discusses common network attacks and the mitigations for each type of attack, hardening vulnerable router services and interfaces, and tools to provide secure router management and reporting. Students will learn about configuring Authentication, Authorization, and Accounting (AAA) services for Cisco routers.

Module 2 – Firewalls and Intrusion Prevention

This module examines firewall and ACL technology including firewall configuration and verification. It also discusses Intrusion detection and prevention system, and configuring an Intrusion Prevention System (IPS) with the Security Device Manager (SDM).

Module 3 – Remote Connectivity

In this module students will learn about remote connectivity. This module provides an overview of remote connectivity, cable technologies, and Digital Subscriber Line (DSL) technologies, including configuring, verifying and troubleshooting DSL.

Module 4 – IPsec

This module teaches the students about IPsec. Elements discussed include the components and features of IPsec, using Site-to-Site IPsec VPNs, combining Generic Routing Encapsulation (GRE) with IPsec, and verifying IPsec/GRE Tunnel configurations. The module also includes information about configuring Cisco Easy VPN solutions and providing high availability using IPsec failovers and IPsec VPN WAN backup.

Module 5 – Multiprotocol Label Switching (MPLS)

This module discusses concepts about using MPLS to forward packets through a network and configuring MPLS. It also discusses configuring an MPLS VPN configuration.

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 1.1: Common Network Attacks

Summary

This section discusses common network attacks. Concepts covered include:

- Reconnaissance attacks.
- Access attacks.
- Denial of service attacks.
- Malware attacks.
- Application layer attacks.
- Management protocol attacks.

Implementing Secure Converged Wide Area Networks Objectives:

- 401. Describe and mitigate common network attacks (i.e., Reconnaissance, Access, and Denial of Service).
- 402. Describe and mitigate Worm, Virus, and Trojan Horse attacks.
- 403. Describe and mitigate application-layer attacks (e.g., management protocols).

Lecture Focus Questions:

- Which type of attack uses ping sweeps and port scanning?
- What is another name for the master device used in a Denial of Service attack?
- Port redirection is a form of which type of attack?
- What are the differences between a worm, virus, and Trojan horse?
- Which SNMP versions transport important data in clear text?

Time

About 40 minutes

Number of Exam Questions

16 questions

Section 1.2: Attack Mitigation

Summary

This section discusses mitigation for common network attacks. Mitigation methods for the following attacks are covered:

- Reconnaissance attack
- Password attack
- DoS and DDoS attack
- IP spoofing
- Malware attack
- Application attack

Implementing Secure Converged Wide Area Networks Objectives:

- 401. Describe and mitigate common network attacks (i.e., Reconnaissance, Access, and Denial of Service).
- 402. Describe and mitigate Worm, Virus, and Trojan Horse attacks.
- 403. Describe and mitigate application-layer attacks (e.g., management protocols).

Lecture Focus Questions:

- What are the steps to mitigate a worm attack?
- What is the result of turning off ICMP ECHO replies?
- RFC 3704 outlines how to mitigate which type of attack?
- How can SYN flood attacks be mitigated?
- Which security implementation will mitigate the effects of a Man-in-the-middle attack?

Time

About 25 minutes

Number of Exam Questions

10 questions

Section 1.3: Vulnerable Router Services and Interfaces

Summary

In this section students will learn about how to lock down and harden vulnerable router services and interfaces. Concepts covered include:

- Using and configuring AutoSecure.
- Using the Cisco Router and Security Device Manager (SDM).

Students will learn how to:

- Implement interactive and non-interactive AutoSecure .
- Prepare a router for Cisco Router and Security Device Manager (SDM) access.
- Conduct a security audit and fix various vulnerabilities.
- Implement One-step Lockdown.

Implementing Secure Converged Wide Area Networks Objectives:

- 501. Describe, Configure, and verify AutoSecure/One-Step Lockdown implementations (i.e., CLI and SDM).

Lecture Focus Questions:

- On which planes does AutoSecure focus?
- Which mode of AutoSecure will implement an AAA login policy?
- What is the default AutoSecure mode?
- Which security vulnerabilities are addressed with the non-interactive mode of AutoSecure?
- The Cisco Router and Security Device Manager (SDM) uses wizards for which types of features?
- The SDM is an alternative to which type of device management interface?
- Which privilege level is necessary to use the SDM?
- Which vulnerabilities are addressed by AutoSecure but not by One-Step Lockdown?

Time

About 50 minutes

Lab/Activity

- Configure AutoSecure 1
- Configure AutoSecure 2
- Conduct a Security Audit
- Implement a One-step Lockdown

Number of Exam Questions

7 questions

Section 1.4: Secure Router Management and Reporting

Summary

This section examines tools for secure router management and reporting. Concepts covered include:

- The secure flow of information between management hosts and managed devices.
- Configuring login enhancements.
- Using the Role-based CLI Access to define views.
- Using the IOS Resilient Configuration feature to secure and maintain a working copy of the running configuration file.
- Using the Secure Shell (SSH) feature to make a secure, encrypted connection to a Cisco router.
- Implementing syslog message logging.
- Using Simple Network Management Protocol (SNMP) to provide a message format for communication between SNMP managers and agents.
- Using Network Time Protocol (NTP) to time-synchronize a network of machines.

Students will learn how to:

- Enable device login enhancements.
- Configure IOS resiliency for the running configuration file and IOS image.

Implementing Secure Converged Wide Area Networks Objectives:

- 504. Describe and configure IOS secure management features (e.g., SSH, SNMP, SYSLOG, NTP, Role-Based CLI, etc.)

Lecture Focus Questions:

- What is quiet mode and how is it enabled?
- How is a superview created?
- What is the difference between a root view user and a user with a privilege level of 15?
- What service must be enabled before configuring role-based views?
- Which feature protects against malicious attempts to erase the contents of persistent storage, such as NVRAM and flash?
- How is SNMPv3 different than prior SNMP versions?
- Which types of authentication are available with NTP?

Time

About 80 minutes

Lab/Activity

- Configure Login Enhancement
- Configure IOS Resiliency

Number of Exam Questions

11 questions

Section 1.5: AAA

Summary

This section provides details about using AAA services to allow systematic and scalable access security.

Students will learn how to:

- Use the SDM to enable AAA services for privilege EXEC mode access.
- Use the CLI to create a default login and AAA server policy for VTY access.

Implementing Secure Converged Wide Area Networks Objectives:

- 502. Describe, configure, and verify AAA for Cisco Routers.

Lecture Focus Questions:

- Which authentication protocols are used in AAA?
- What are the differences between TACACS+ and RADIUS?
- How can a user have a successful login even if all authentication methods fail?
- Which AAA CLI keyword creates a default policy applied to all lines and interface?

Time

About 40 minutes

Lab/Activity

- Configure AAA Services with CLI 1
- Configure AAA Services with CLI 2
- Configure AAA Services with SDM

Number of Exam Questions

11 questions

Section 2.1: Firewall and ACL Overview

Summary

This section provides an overview of firewall and ACL technology. Concepts covered include:

- Firewall zones and operations.
- Components of the Cisco IOS firewall feature set.
- Types of Access Control Lists (ACLs).
- Applying a Cisco IOS Firewall.

Implementing Secure Converged Wide Area Networks Objectives:

- 503. Describe and configure threat and attack mitigation using ACLs.
- 601. Describe the functions and operations of Cisco IOS Firewall (e.g., Stateful Firewall, CBAC, etc.).

Lecture Focus Questions:

- What is typically found in a DMZ?
- How are packet filtering and stateful packet filtering different?
- What four components comprise the Cisco IOS firewall feature set?
- How does the CBAC identify returning traffic?
- What are the differences between standard and extended ACLs?
- In general, which direction should ACLs be applied?

Time

About 35 minutes

Number of Exam Questions

7 questions

Section 2.2: Firewall Configuration

Summary

This section presents information about configuring the firewall. Concepts covered include:

- Configuring the firewall through the CLI.
- Implementing the IOS firewall and ACLs.
- Using SDM to implement a complex IOS Firewall configuration.

Students will learn how to:

- Use the CLI to configure and apply ACLs .
- Use the SDM to configure the Cisco IOS Firewall.

Implementing Secure Converged Wide Area Networks Objectives:

- 503. Describe and configure threat and attack mitigation using ACLs.
- 602. Configure Cisco IOS Firewall with SDM.

Lecture Focus Questions:

- How does the **established** keyword affect TCP traffic received at the router?
- What is the result of using the **no ip inspect** privileged EXEC command?
- What types of firewall wizards are available in the SDM?
- Which SDM firewall wizard is used to select multiple outside interfaces?
- Which SDM firewall wizard is used to create a DMZ or custom application security policy?

Time

About 60 minutes

Lab/Activity

- Configure a Firewall with CLI 1
- Configure a Firewall with CLI 2
- Configure a Firewall with SDM 1
- Configure a Firewall with SDM 2

Number of Exam Questions

19 questions

Section 2.3: Firewall Verification

Summary

This section discusses how to verify a firewall configuration after it has been created. Concepts covered include:

- SDM Firewall configuration verification strategies.
- CLI Firewall configuration verification strategies.

Students will learn how to:

- Use the SDM and CLI to verify basic and advanced firewall configurations.

Implementing Secure Converged Wide Area Networks Objectives:

- 603. Verify Cisco IOS Firewall configurations (i.e., IOS CLI configurations, SDM Monitor).

Lecture Focus Questions:

- Which SDM icon indicates an inspection policy?
- With the SDM, how can you determine if the firewall is active?
- Which interface will have ACLs blocking traffic sourced from subnets specified in RFC 1918?
- Which CLI command will identify the source and destination IP addresses of current firewall inspection sessions?
- In a basic IOS firewall configuration, will originating traffic have ACLs or IP inspection rules applied, or both?

Time

About 30 minutes

Lab/Activity

- Verify a Firewall Configuration with SDM 1
- Verify a Firewall Configuration with SDM 2
- Verify a Firewall Configuration with CLI

Number of Exam Questions

8 questions

Section 2.4: Intrusion Detection and Prevention Systems

Summary

In this section students will explore using intrusion detection and prevention systems to protect the network by monitoring frames on the network in real time. Concepts covered include:

- The role of an Intrusion Detection System (IDS).
- The role of an Intrusion Protection System (IPS).
- The role of Signatures and Signature Definition Files (SDFs).

Implementing Secure Converged Wide Area Networks Objectives:

- 701. Describe the functions and operations of IDS and IPS systems (e.g., IDS/IPS signatures, IPS Alarms, etc.)

Lecture Focus Questions:

- How can an IDS respond to detected attacks?
- Where is the IPS located?
- Which protocols are used by IPS clients and servers to exchange messages?
- What is the difference between signature-based and anomaly-based attack detection?
- What is a honey pot?
- Which one of the four categories of signatures uses regular expression pattern matching?
- What determines which SDF can be implemented for the IPS?

Time

About 30 minutes

Number of Exam Questions

14 questions

Section 2.5: IPS Configuration

Summary

This section discusses configuring IPS. When configuring IPS with the SDM, use the following main components:

- The IPS Rule wizard in the **Create IPS** window
- The IP Policies in the **Edit IPS** window
- The Global Settings in the **Edit IPS** window
- The Signatures in the **Edit IPS** window

Students will learn how to:

- Implement and verify IPS configurations.

Implementing Secure Converged Wide Area Networks Objectives:

- 702. Configure Cisco IOS IPS using SDM.

Lecture Focus Questions:

- Running the IPS wizard allows you to specify which three things?
- Which SDM screen disables or enables IPS on an interface?
- Which SDM screen can change the location and type of SDF?
- How can you identify an edited, enabled, or disabled signature?
- Given default IPS settings, what will happen to traffic that cannot be inspected?
- What CLI command will show IPS configurations not listed in the running configuration file?
- By default, which signatures will be used if the IPS cannot find or load the specified SDF?
- What are the four Alarm Severity categories?
- Which event action blocks the attacker's source IP address completely?

Time

About 35 minutes

Lab/Activity

- Configure IPS 1
- Configure IPS 2
- Verify an IPS Configuration

Number of Exam Questions

9 questions

Section 3.1: Remote Connectivity Overview

Summary

This section examines using remote connectivity to provide data and voice solutions to teleworkers. Concepts covered include:

- Requirements for remote connectivity.
- Considerations for designing a teleworker environment.
- Common remote site connection topologies include.

Lecture Focus Questions:

- Enterprise solutions for remote connectivity address which requirements?
- What are the most common remote connection topologies?

Time

About 5 minutes

Section 3.2: Cable

Summary

In this section students will learn about cable technology. Concepts covered include:

- Cable technology terms.
- Cable systems standards.
- The benefits and drawbacks of cable technology.
- HFC network connectivity.
- Cable Modem (CM) initialization.

Implementing Secure Converged Wide Area Networks Objectives:

- 101. Describe Cable (HFC) technologies.

Lecture Focus Questions:

- What are the advantages of HFC over coaxial cable networks?
- What is the headend, downstream, and upstream in an HFC network?
- Which frequencies are used in downstream and upstream communication?
- What are the steps for CM initialization?
- Which HFC device is located at the headend?

Time

About 25 minutes

Number of Exam Questions

4 questions

Section 3.3: Digital Subscriber Line (DSL)

Summary

This section examines Digital Subscriber Line (DSL) technologies. Concepts covered include:

- Deploying Digital Subscriber Line (DSL).
- Variants of DSL.
- Deploying ADSL.

Implementing Secure Converged Wide Area Networks Objectives:

- 102. Describe xDSL technologies.

Lecture Focus Questions:

- Where is the DSLAM located in a DSL network?
- Which DSL variant is used as a replacement for T1 lines?
- In which ways is CAP different than DMT?
- How is bandwidth optimized within DMT?
- Which ADSL encapsulation method requires host-based software?
- Which PPPoE discovery packet is sent to a server to indicate needed services?

Time

About 35 minutes

Number of Exam Questions

5 questions

Section 3.4: DSL Configuration

Summary

This section discusses configuring DSL. Concepts covered include:

- Configuring a PPPoE client router.
- Configuring a PPPoA client router.

Students will learn how to:

- Implement PPPoE client configurations.

Implementing Secure Converged Wide Area Networks Objectives:

- 103. Configure ADSL (i.e., PPPoE or PPPoA).
- 104. Verify basic teleworker configurations.

Lecture Focus Questions:

- What is the MTU on a PPPoE dialer and Ethernet interface?
- How is the IP address supplied to the dialer interface?
- What keyword performs authentication on incoming calls to the PPPoE client?
- What service is used to translate between inside and outside IP addresses in a PPPoE or PPPoA configuration?
- Which interface should be specified in the default route of a PPPoE client?
- What is the default operating mode for a PPPoA configuration?
- Where is the dialer pool membership specified in a PPPoA configuration?

Time

About 35 minutes

Lab/Activity

- Configure PPPoE 1
- Configure PPPoE 2

Number of Exam Questions

5 questions

Section 3.5: DSL Verification and Troubleshooting

Summary

This section provides information about verifying and troubleshooting DSL client configurations. Concepts covered include:

- DSL layers in which a connection failure can occur.
- Verifying and troubleshooting PPPoE and PPPoA client configurations.
- Understanding in the command output.

Students will learn how to:

- Verify PPPoE client configurations.
- Verify PPPoA client configurations.

Implementing Secure Converged Wide Area Networks Objectives:

- 103. Configure ADSL (i.e., PPPoE or PPPoA).
- 104. Verify basic teleworker configurations.

Lecture Focus Questions:

- Which elements contribute to a Layer 1 failure?
- If the MTU is incorrectly configured for PPPoE, which layer will fail?
- Which PPP negotiation phase will fail if the two devices cannot agree on upper-layer protocols to use?
- Which CLI command will display negotiated PPP options?
- Which layer is affected when the ATM interface is down?

Time

About 25 minutes

Lab/Activity

- Verify DSL Client Configurations

Number of Exam Questions

5 questions

Section 4.1: IPsec Components and Features

Summary

In this section students will learn about features and components of IP Security (IPsec) used to provide secure transmission over unprotected IP networks. Concepts covered include:

- IP Security (IPsec).
- Internet Key Exchange (IKE).
- Security Association (SA).
- Encapsulating Security Payload (ESP)
- IPsec encryption methods.
- Public Key Infrastructure (PKI) environment.

Implementing Secure Converged Wide Area Networks Objectives:

- 301. Describe the components and operations of IPsec VPNs and GRE Tunnels.

Lecture Focus Questions:

- Which encryption types and hash algorithms are available in IPsec?
- What are the differences between ESP and AH?
- In which phase does IKE establish a secure, unidirectional IPsec session to secure data?
- How are the main and aggressive IKE modes different?
- When is a transform set used?
- Which VPN mode encapsulates the original IP header along with all the data within the packet with a new external IP header?
- Which encryption method is known as public key encryption?
- What standard is used for certificates in a PKI environment?

Time

About 65 minutes

Number of Exam Questions

18 questions

Section 4.2: Site-to-Site IPsec VPN

Summary

This section provides an overview of using IPsec to secure data transfers between Site-to-Site VPNs. Concepts covered include:

- Lifecycle of a site-to-site IPsec VPN.
- Configuring the Site-to-Site VPN with IPsec.

Students will learn how to:

- Use the SDM to configure Site-to-Site VPNs.

Implementing Secure Converged Wide Area Networks Objectives:

- 302. Configure a site-to-site IPsec VPN/GRE Tunnel with SDM (i.e., preshared key).

Lecture Focus Questions:

- What are the five steps in the lifecycle of a Site-to-Site IPsec VPN? Which step transmits data through the tunnel?
- What are the differences between the Quick setup and Site to Site VPN SDM wizards?
- How is interesting traffic identified?
- Where can you specify the VPN mode in the Site to Site VPN SDM wizard?

Time

About 35 minutes

Lab/Activity

- Configure a Site-to-Site IPsec VPN 1
- Configure a Site-to-Site IPsec VPN 2

Number of Exam Questions

4 questions

Section 4.3: Generic Routing Encapsulation (GRE) over IPsec

Summary

This section discusses combining Generic Routing Encapsulation (GRE) with IPsec to create a system with effective tunneling capabilities and strong security. Concepts covered include:

- The role of GRE.
- Features of GRE.
- Configuring a GRE tunnel using SDM.

Students will learn how to:

- Use the SDM to configure GRE over IPsec VPNs.

Implementing Secure Converged Wide Area Networks Objectives:

- 302. Configure a site-to-site IPsec VPN/GRE Tunnel with SDM (i.e., preshared key).

Lecture Focus Questions:

- How are GRE tunnel endpoints different than IPsec Site-to-Site VPN tunnel endpoints?
- Which topology is used in a GRE tunnel configuration?
- What GRE tunnel feature allows both encrypted and unencrypted connections?

Time

About 25 minutes

Lab/Activity

- Configure GRE over IPsec

Number of Exam Questions

4 questions

Section 4.4: Site-to-Site VPN and GRE Tunnel Verification

Summary

In this section students will learn commands that can be used to verify Site-to-Site VPNs and GRE tunnels. Concepts covered include:

- Using SDM to view valuable information about IPsec VPNs.
- Using CLI commands to verify or debug the configuration of Site-to-Site IPsec VPNs or GRE tunnels.
- Understanding the command output:

Students will learn how to:

- Use the SDM to verify Site-to-Site VPN configurations.
- Use the CLI to verify GRE over IPsec configurations.

Implementing Secure Converged Wide Area Networks Objectives:

- 303. Verify IPsec/GRE Tunnel configurations (i.e., IOS CLI configurations).

Lecture Focus Questions:

- Which SDM screen verifies transform set information?
- Where can you determine which ACL that identifies interesting traffic for IPsec encryption?
- Where is the crypto map identified in the running configuration file?
- What is the purpose of the **tunnel source** command on a tunnel interface?

Time

About 20 minutes

Lab/Activity

- Verify Site-to-Site IPsec VPN Information
- Verify GRE over IPsec Information

Number of Exam Questions

7 questions

Section 4.5: Cisco Easy VPN

Summary

This section discusses using Easy VPN to reduce administrative overhead and centralize management by supporting a group-based policy control. Concepts covered include:

- The role of Easy VPN.
- Configuring an Easy VPN server solution.
- Configuring an Easy VPN client solution.

Implementing Secure Converged Wide Area Networks Objectives:

- 305. Describe and configure Cisco Easy VPN solutions using SDM.

Lecture Focus Questions:

- In which step does the server initiate user authentication in the Easy VPN process?
- What is the purpose of XAuth?
- What are the Easy VPN Client authentication options?
- In which circumstances is Reverse Route Injection (RRI) used?

Time

About 40 minutes

Number of Exam Questions

9 questions

Section 4.6: IPsec High Availability

Summary

This section discusses providing high availability using IPsec stateless failover, IPsec stateful failover, and IPsec VPN WAN backup. Concepts covered include:

- IPsec stateless failover
- Configuration of an IPsec backup peer.
- Stateful failover in IPsec.
- Configuring IPsec stateful failover.
- IPsec VPN backup solutions for WAN connections.

Students will learn how to:

- Configure stateless and stateful failover.

Implementing Secure Converged Wide Area Networks Objectives:

- 304. Describe, configure, and verify VPN backup interfaces.

Lecture Focus Questions:

- How often are periodic DPD messages sent?
- In a stateless failover configuration, what will occur if a router has traffic to send to the peer and the peer does not respond?
- How can the time limit be adjusted before DPD tears down a primary VPN and fails over to the backup VPN?
- Which protocols are used in stateful failover?
- Which protocols provide gateway redundancy?
- What two methods back up a typical WAN link with an IPsec VPN?

Time

About 45 minutes

Number of Exam Questions

9 questions

Section 5.1: MPLS

Summary

This section discusses using Multiprotocol Label Switching (MPLS), a high-performance method for forwarding packets through a network, to provide high performance, traffic management, scalability and flexibility. Concepts covered include:

- The role of MPLS.
- The role of an MPLS label.
- The role of Label Switch Routers (LSRs) within MPLS operations.

Implementing Secure Converged Wide Area Networks Objectives:

- 201. Describe the components and operation of Frame-Mode MPLS (e.g., packet-based MPLS VPNs).

Lecture Focus Questions:

- How is the FIB updated?
- What will occur if a CEF-enabled router receives a packet that does not have a route in the FIB?
- CEF manages which two MPLS planes?
- In which plane is the Label Information Base (LIB) found? In which plane is the Label Forwarding Information Base (LFIB) found?
- What is the purpose of Label Distribution Protocol (LDP)?
- What are the four fields of the MPLS label header?
- What is the purpose of a Layer 2 header Protocol ID (PID) field?
- Which device imposes a label in an MPLS-enabled network?
- Which device in an MPLS-enabled network uses PHP?

Time

About 50 minutes

Number of Exam Questions

7 questions

Section 5.2: MPLS Configuration

Summary

This section explores configuring MPLS. Concepts covered include:

- Provider Edge (PE) MPLS configuration details.
- Configuring MPLS on the PE router.
- Understanding command output.

Students will learn how to:

- Implement CEF and MPLS on a PE router.
- Configure a P device to handle MPLS packets.

Implementing Secure Converged Wide Area Networks Objectives:

- 202. Configure and verify Frame-Mode MPLS.

Lecture Focus Questions:

- What is the default label distribution protocol?
- What MTU configuration should be provided on interfaces which send and receive packets with two MPLS labels?
- What is the purpose of the LPD MPLS router ID?
- How can CEF be disabled on a single interface?
- Which CLI command displays outgoing interface and next hop IP address information for MPLS-labeled packets?

Time

About 20 minutes

Lab/Activity

- Configure MPLS 1
- Configure MPLS 2

Number of Exam Questions

5 questions

Section 5.3: MPLS VPN Technology

Summary

This section examines using MPLS VPN technology to create a private path through an MPLS cloud for a particular customer's routes. Concepts covered include:

- Understanding MPLS VPN architecture.
- Configuring an MPLS VPN.
- Verifying MPLS VPN information on a PE router.
- Viewing and understanding command output.

Implementing Secure Converged Wide Area Networks Objectives:

- 201. Describe the components and operation of Frame-Mode MPLS (e.g., packet-based MPLS VPNs).

Lecture Focus Questions:

- Which MPLS enabled devices are aware of MPLS VPN configurations?
- Which protocol is used to transmit the global IP routing information to PE routers?
- What is the purpose of an RD?
- How is a VPNv4 address created?
- What are the steps for customer route propagation across the MPLS VPN network?

Time

About 35 minutes

Number of Exam Questions

6 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 basic teleworker services** are grouped together and presented in practice exam **100. Implement basic teleworker services, All Questions**. Students will typically take about 60-90 minutes to complete each of the following practice exams.

- 100. Implement basic teleworker services, All Questions (20 questions)
- 200. Implement Frame-Mode MPLS, All Questions (19 questions)
- 300. Implement a site-to-site IPsec VPN, All Questions (54 questions)
- 400. Describe network security strategies, All Questions (25 questions)
- 500. Implement Cisco Device Hardening, All Questions (46 questions)
- 600. Implement Cisco IOS firewall, All Questions (20 questions)
- 700. Describe and configure Cisco IOS IPS, All Questions (23 questions)

The *Certification Practice Exam* consists of 55 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.