



Lesson Plans

Building Converged Cisco Multilayer Switched Networks

(Exam 642-812 BCMSN)

Version 2.0

Table of Contents

Course Overview	2
Section 0.1: Introduction.....	4
Section 0.2: Multilayer Switching Overview.....	5
Section 0.3: Initial Switch Configuration	6
Section 1.1: VLANs.....	7
Section 1.2: VLAN Trunking	8
Section 1.3: VLAN Trunking Protocol (VTP).....	9
Section 1.4: Verifying and Troubleshooting VLANs.....	11
Section 2.1: Spanning Tree Protocol (STP).....	12
Section 2.2: Spanning Tree Protocols.....	14
Section 2.3: Optional STP Features and UDLD	15
Section 2.4: Verifying STP Configurations	17
Section 2.5: EtherChannel	18
Section 3.1: Inter-VLAN Routing.....	19
Section 3.2: Inter-VLAN Routing Configuration	20
Section 3.3: Troubleshooting Inter-VLAN Routing	21
Section 4.1: Gateway Redundancy	22
Section 4.2: HSRP Configuration.....	23
Section 4.3: VRRP Configuration.....	24
Section 4.4: GLBP Configuration.....	25
Section 4.5: Troubleshooting Gateway Redundancy	26
Section 5.1: VoIP Overview	27
Section 5.2: Voice VLANs	28
Section 5.3: Quality of Service (QoS) and Trust Boundary	29
Section 5.4: VoIP Configuration.....	30
Section 5.5: Power over Ethernet (PoE)	32
Section 6.1: Layer 2 Security Threats.....	33
Section 6.2: Port Security	34
Section 6.3: Additional Switch Security Features	36
Section 6.4: Switch Hardening	38
Section 7.1: Wireless Overview.....	39
Section 7.2: Cisco Unified Wireless Network	40
Practice Exams.....	41

Course Overview

This course prepares students for the Cisco Exam 642-812 BCMSN. It focuses on information and skills necessary to implement multilayer switched networks.

Module 0 – Introduction

This module introduces the prerequisites to this course and discusses the two paths students can take to obtain BCMSN certification. Students will become familiar with how to use the Cisco Simulator as a learning tool to complete the simulations throughout the course. Students will learn the basics of multilayer switching and hierarchical network design. They will also explore initial switch configuration modes, prompts and commands.

Module 1 – Virtual LANs (VLANs)

This module discusses the functions of VLANs and how to create and configure a VLAN. Students will learn how to configure VLAN trunking and VTP. They will also learn the show commands used to troubleshoot VLAN configurations.

Module 2 – Spanning Tree

In this module students will learn the functions of Spanning Tree Protocols. They will learn how to configure Rapid PVST+, MSTP optional STP features, and UDLD. Show commands to troubleshoot STP are discussed as well as commands to configure an EtherChannel with PAgP or LACP.

Module 3 – Inter-VLAN Routing

This module covers the basics of using Inter-VLAN routing. Students will also learn the commands to configure and troubleshoot Inter-VLAN routing.

Module 4 – Gateway Redundancy

In Module 4 students will learn the basics of gateway redundancy protocols. They will learn the commands to configure and verify HSRP, VRRP, and GLBP and the show commands used to troubleshoot gateway redundancy.

Module 5 – Voice over IP (VoIP)

Module 5 provides an overview of working with VoIP, Voice VLANs, QoS, and trust boundaries. Students will learn how to configure VoIP. They will also learn how to use PoE for IP phones.

Module 6 – Switch Security

Module 6 discusses security threats for Layer 2 devices. It also discusses methods to enhance the security of the network; configuring port security, configuring switch security, and switch hardening.

Module 7 – Wireless

This module provides an overview of wireless networking. Students will learn the functions of the components of a wireless network. They will become familiar with Cisco Unified Wireless Network used to manage a wireless network and Cisco Aironet Desktop Utility (ADU), the wireless client.

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 test.

Section 0.1: Introduction

Summary

In this section the students will learn the topics that will be presented in this course, how to use the Cisco Simulator, and the icons used to represent network devices and connections.

The prerequisites for this course are that the students should have completed the following course 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: Multilayer Switching Overview

Summary

This section provides an overview of Multilayer Switching. Students will compare the marketing terms of switches which perform functions at different layers:

- Layer 2 Switching
- Layer 3 Switching
- Layer 4 Switching
- Layer 7 Switching

They will learn that the hierarchical network design is typically referred to as submodules or layers which represent the physical implementation of the network devices used in multilayer networks:

- Building Access submodule – also known as Access Layer
- Building Distribution submodule – also known as Distribution Layer
- Campus Backbone – also known as Core Layer

Students will compare the characteristics of various Ethernet implementations:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- 10-Gigabit Ethernet

Lecture Focus Questions:

- What is the difference between Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet?
- What are the three common submodules in a Cisco hierarchical network design?
- Which submodule is designed to provide fast failure recovery?
- What is a hierarchical network?
- Where can you find distribution-layer and access-layer switches in a hierarchical network?

Time

About 10 minutes

Section 0.3: Initial Switch Configuration

Summary

This section explores details of initial switch configuration modes, prompts and commands. Modes include:

- User EXEC
- Privileged EXEC
- Global Configuration
- Line
- Interface
- Config-vlan
- VLAN Configuration

Students will also learn common port configuration commands.

Lecture Focus Questions:

- What is the difference between the **config-vlan** mode and the **VLAN configuration** mode?
- What is the difference between using **exit** or **Ctrl + Z** when changing configuration modes?
- What three different duplex modes can be set on the interface?
- What will be the result of disabling the Auto-MDIX?

Time

About 15 minutes

Section 1.1: VLANs

Summary

This section discusses why to use VLANs, how to create a VLAN, and how to configure management settings.

Students will learn how to:

- Display the current VLAN configuration.
- Execute common VLAN configuration commands.
- Given a scenario, create a VLAN and assign port membership as assigned.
- Given a scenario, configure management VLAN settings.

Building Converged Cisco Multilayer Switched Networks Objectives

- 101. Explain the functions of VLANs in a hierarchical network.
- 102. Configure VLANs (e.g., Native, Default, Static and Access).

Lecture Focus Questions:

- What are the administrative advantages of creating VLANs?
- Why are end-to-end VLANs more difficult to troubleshoot than local VLANs?
- What is the difference between a static VLAN and a dynamic VLAN?
- What two configuration steps must you take to manage a Layer 2 switch from a remote network?

Time

About 30 minutes

Lab/Activity

- Create VLANs
- Configure Management VLAN Settings

Section 1.2: VLAN Trunking

Summary

In this section students will learn to connect multiple switches on a VLAN by trunking. They will learn commands for configuring and monitoring trunking on a switch. Two trunking protocols are discussed:

- Inter-Switch Link (ISL)
- 802.1Q

Students will learn how to:

- Manually configure trunking on interfaces where switches will be attached.
- Configure switches to use 802.1Q trunking protocol and dynamic desirable mode.
- Configure the native VLAN for a trunk link.
- Configure which VLANs are permitted to communicate over a trunk link.

Building Converged Cisco Multilayer Switched Networks Objectives

- 103. Explain and configure VLAN trunking (i.e., IEEE 802.1Q and ISL)
- 105. Verify or troubleshoot VLAN configurations.

Lecture Focus Questions:

- When does the trunking protocol not tag the frame over a trunk link, and how does it handle the frame?
- When does dynamic trunking configure a trunk link?
- What happens if two switches on a VLAN trunk are both configured for auto dynamic trunking?

Time

About 40 minutes

Lab/Activity

- Configure Trunk Ports
- Configure Trunking Protocol and Mode
- Configure the Native VLAN
- Configure Allowed VLANs

Section 1.3: VLAN Trunking Protocol (VTP)

Summary

This section examines how the VLAN Trunking Protocol (VTP) simplifies VLAN configuration on a multi-switch network by propagating configuration changes to other switches. Students will learn VTP commands to configure and monitor switches.

Switches are configured in one of the following VTP Modes:

- Server
- Client
- Transparent

VTP message types include:

- Summary advertisements
- Subset advertisements
- Advertisement request

VTP pruning reduces broadcast traffic by forwarding messages to switches with specific VLANs.

Students will learn how to:

- Configure the VTP mode, domain, and password.
- Confirm the VTP status of a switch.

Building Converged Cisco Multilayer Switched Networks Objectives

- 104. Explain and configure VTP.

Lecture Focus Questions:

- What two conditions on switches will *not* allow you to modify the VLAN configuration?
- What is the easiest way to recover from losing the *only* VTP server?
- Which type of VTP message is the most frequently sent by switches?
- What happens when you add a switch to the network with a higher revision number to your VTP configuration?
- How do you remove a VTP domain name?

Time

About 30 minutes

Lab/Activity

- Configure VTP Settings

Section 1.4: Verifying and Troubleshooting VLANs

Summary

In this section students will learn show commands used to display VLAN configurations for verification and troubleshooting:

- Show vlan brief
- Show vlan <VLAN id>
- Show interfaces trunk
- Show interfaces fa 0/1 switchport

Students will learn how to:

- Given a scenario, verify VLAN information.
- Given a scenario, troubleshoot a VLAN trunking link.

Building Converged Cisco Multilayer Switched Networks Objectives

- 105. Verify or troubleshoot VLAN configurations.

Lecture Focus Questions:

- When examining the output from the **show interfaces fa 0/1 trunk** command, what does the **n-** in front of the protocol designate?
- How can you determine which VLANs are allowed to communicate over a trunk link?
- How can you determine when an interface is operating as an access port or a trunk port?
- Which command displays an overview of VLAN and trunking information of an interface?

Time

About 25 minutes

Lab/Activity

- Find VLAN Information
- Troubleshooting VLANs 1
- Troubleshooting VLANs 2

Section 2.1: Spanning Tree Protocol (STP)

Summary

This section examines using Spanning Tree protocol (STP) to prevent bridging loops (packets passed endlessly between redundant paths). With the STP protocol the bridge or switch for each route is assigned one of the following roles:

- Root bridge
- Designated bridge
- Backup bridge

Students will learn about the following elements of STP

- Bridge Protocol Data Units (BPDUs)
- Port states
- Timers
- Port types
- Cost
- Spanning Tree configuration tasks

Students will learn how to:

- Given the MAC Address of a switch, configure it to be the root bridge.
- Configure a switch to be a primary root bridge.
- Configure a switch to be a secondary root bridge

Building Converged Cisco Multilayer Switched Networks Objectives

- 201. Explain the functions and operations of the Spanning Tree protocols (i.e., RSTP, PVRST, MISTP).

Lecture Focus Questions:

- How does STP eliminate bridging loops?
- Which port state builds the bridge database with MAC addresses?
- Which timers can be configured to speed up STP performance?
- Which devices generate configuration Bridge Protocol Data Units (BPDUs)?
- What is the difference between a root port and a designated port?

Time

About 50 minutes

Lab/Activity

- Configure the Root Bridge
- Configure the Primary and Secondary Root Bridge

Section 2.2: Spanning Tree Protocols

Summary

In this section students will learn the details of different types of Spanning Tree protocols:

- Common Spanning Tree (CST)
- Per-VLAN Spanning Tree (PVST)
- Per-VLAN Spanning Tree Plus (PVST+)
- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree (MST)

They will learn the commands to configure RSTP (RPVST+) and MSTP.

Students will learn how to:

- Given a scenario, configure Rapid PVST+ on assigned switches.
- Given a scenario, configure MST on multiple switches with the minimum amount of MST instances.

Building Converged Cisco Multilayer Switched Networks Objectives

- 201. Explain the functions and operations of the Spanning Tree protocols (i.e., RSTP, PVRST, MISTP).
- 202. Configure RSTP (PVRST) and MISTP.

Lecture Focus Questions:

- What are the differences between PVST and PVST+?
- What are the three STP modes available on Cisco Catalyst switches?
- Which Rapid PVST+ port states are different than PVST+ port states and why?
- What is the difference between a Rapid PVST+ alternate port and a backup port?
- What is MSTP region?

Time

About 30 minutes

Lab/Activity

- Configure Rapid PVST+
- Configure MSTP

Section 2.3: Optional STP Features and UDLD

Summary

This section discusses optional STP features which Cisco introduced to improve convergence and fine tune STP:

- Port Fast
- BPDU guard
- BPDU filtering
- UplinkFast
- BackboneFast
- Root Guard
- Loop Guard

Unidirectional Link Detection (UDLD) disables ports which are determined to be one-way. UDLD supports two modes of operation:

- Normal
- Aggressive

Students will become familiar with the commands to configure UDLD and advanced STP features.

Students will learn how to:

- Given a scenario, configure Port Fast on access ports.
- Given a scenario, configure a switch to use Port Fast BPDU filtering.
- Secure the STP topology by configuring FastEthernet ports with Root Guard.
- Protect a spanning tree topology with Loop Guard.
- Within a hierarchical network, configure UplinkFast.
- Within a hierarchical network, configure BackboneFast.

Building Converged Cisco Multilayer Switched Networks Objectives

- 203. Describe and configure STP security mechanisms (i.e., BPDU Guard, BPDU Filtering, Root Guard).
- 204. Configure and Verify UDLD and Loop Guard.

Lecture Focus Questions:

- Which optional STP feature helps to prevent loops on a port where Port Fast is enabled?
- What will be the response if a switch receives a BPDU after being globally enabled with BPDU guard?

- What is the difference between globally-enabled BPDU filtering and per-port-enabled BPDU filtering?
- Which optional STP feature provides an alternate path back to the root bridge if the root port or link goes down?
- How does BackboneFast detect failures on indirect links or connections?
- What happens when a switch sends a superior BPDU to a root guard enabled interface?
- Which UDLD mode will make up to eight attempts before changing the port state to the err-disabled state?

Time

About 60 minutes

Lab/Activity

- Configure Port Fast
- Configure BPDU Filtering
- Configure Root Guard
- Configure Loop Guard
- Configure UplinkFast
- Configure BackboneFast

Section 2.4: Verifying STP Configurations

Summary

This section examines show commands used to display and verify STP configurations.

Students will learn how to:

- Given a scenario, verify STP information.
- Given a scenario, troubleshoot a STP topology.

Building Converged Cisco Multilayer Switched Networks Objectives

- 205. Verify or troubleshoot Spanning Tree protocol operations.

Lecture Focus Questions:

- Which command displays whether Loopguard, UplinkFast, BPDU Filter, and BPDU Guard are enabled?
- How can you verify that spanning tree is working?
- How can you determine the root bridge within a STP topology?
- Where can you discover the root bridge's priority and MAC address?

Time

About 20 minutes

Lab/Activity

- Find STP Information 1
- Find STP Information 2

Section 2.5: EtherChannel

Summary

In this section students will learn that EtherChannel combines multiple switch ports into a single, logical link between two switches. Some of the advantages are that EtherChannel provides communication between the switches, increases the bandwidth between switches, and establishes automatic redundant paths between switches. Cisco Catalyst switches use one of the following protocols for EtherChannel configuration:

- Port Aggregation Protocol (PAgP)
- Link Aggregation Control Protocol (LACP)

Students will become familiar with the commands used to configure EtherChannel.

Students will learn to:

- Given a scenario, configure switches to negotiate the PAgP EtherChannel.
- Given a scenario, configure interfaces to negotiate an EtherChannel with LACP.

Building Converged Cisco Multilayer Switched Networks Objectives

- 206. Configure and verify link aggregation using PAgP or LACP.

Lecture Focus Questions:

- What will happen to redundant links between switches when EtherChannel is configured?
- What are the differences between LACP and PAgP?
- When would you choose LACP over PAgP when configuring EtherChannel?

Time

About 25 minutes

Lab/Activity

- Configure an EtherChannel with PAgP
- Configure an EtherChannel with LACP

Section 3.1: Inter-VLAN Routing

Summary

This section covers using inter-VLAN routing to enable communication between workstations in one VLAN with workstations in other VLANs. The following layer 3 devices are capable of providing inter-VLAN routing:

- Router
- Multilayer switch

Students will learn the basic process of how Multi-Layer Switching (MLS) can move traffic at wire speed and still provide Layer 3 routing.

Cisco Express Forwarding (CEF), an advanced Layer 3 switching technology, is used to increase overall performance. CEF consists of two key components:

- Forwarding Information Base (FIB)
- Adjacency Table

Building Converged Cisco Multilayer Switched Networks Objectives

- 301. Explain and configure Inter-VLAN routing (i.e., SVI and routed ports).
- 302. Explain and enable CEF operation.

Lecture Focus Questions:

- To provide inter-VLAN routing, a device must have which layer of functionality?
- What are two implementations of inter-VLAN routing?
- Is a SVI a logical or physical interface?
- What function includes the concept of route once, switch many?

Time

About 20 minutes

Section 3.2: Inter-VLAN Routing Configuration

Summary

In this section student will learn the commands used to configure and verify inter-VLAN routing.

Students will learn how to:

- Implement inter-VLAN routing with an external router.
- Configure SVIs on a switch for inter-VLAN routing.

Building Converged Cisco Multilayer Switched Networks Objectives

- 301. Explain and configure Inter-VLAN routing (i.e., SVI and routed ports).
- 302. Explain and enable CEF operation.
- 303. Verify or troubleshoot Inter-VLAN routing configurations.

Lecture Focus Questions:

- Why shouldn't you set up an IP address on a router's subinterface for an inter-VLAN routing configuration?
- How does a router know which subinterface to use within inter-VLAN routing?
- How do you display the networks connected to a Layer 3 switch?
- When does a Layer 2 switch need a default gateway IP address?

Time

About 30 minutes

Lab/Activity

- Configure Inter-VLAN Routing 1
- Configure Inter-VLAN Routing 2
- Configure Inter-VLAN Routing 3

Section 3.3: Troubleshooting Inter-VLAN Routing

Summary

In this section students will learn show commands used to display inter-VLAN routing configuration for verification and troubleshooting:

- Show vlan brief
- Show ip route
- Show run

Students will learn how to:

- Given a scenario, verify inter-VLAN routing information.
- Given a scenario, troubleshoot an inter-VLAN routing implementation.

Building Converged Cisco Multilayer Switched Networks Objectives

- 303. Verify or troubleshoot Inter-VLAN routing configurations.

Lecture Focus Questions:

- How can you tell when a SVI is configured on a Layer 3 switch?
- What commands should you use to verify a router-on-a-stick configuration?

Time

About 15 minutes

Lab/Activity

- Troubleshoot Inter-VLAN Routing 1
- Troubleshoot Inter-VLAN Routing 2

Section 4.1: Gateway Redundancy

Summary

This section discusses how gateway redundancy ensures that if a router fails, a backup router takes responsibility as the default gateway. Students will learn the details of the following gateway redundancy protocols:

- Hot Standby Router Protocol (HSRP)
- Virtual Router Redundancy Protocol (VRRP)
- Gateway Load Balancing Protocol (GLBP)

Building Converged Cisco Multilayer Switched Networks Objectives

- 401. Explain the functions and operations of gateway redundancy protocols (i.e., HSRP, VRRP, and GLBP).

Lecture Focus Questions:

- How does a virtual router help to protect against single point of failure?
- If there are three routers in a HSRP group, how many virtual IP addresses would be assigned to that group of routers?
- What are the main differences between HSRP and VRRP, and are they compatible?
- What is the maximum number of routers that can act as active IP default gateways in a GLBP group?
- If there are two routers in a GLBP group, how many virtual MAC addresses are assigned to routers in that group?

Time

About 35 minutes

Section 4.2: HSRP Configuration

Summary

This section examines commands used to configure and verify HSRP.

Students will learn how to:

- Configure multiple routers to form a HSRP virtual default gateway.
- Configure preemption for a HSRP group.
- Configure interface tracking within a HSRP group

Building Converged Cisco Multilayer Switched Networks Objectives

- 402. Configure HSRP, VRRP, and GLBP.
- 403. Verify High Availability configurations.

Lecture Focus Questions:

- Which router in a HSRP group will be the active router if all the routers in a HSRP group are assigned the same priority?
- What is the function of preemption?
- What is interface tracking and how does it affect the HSRP priority value?
- How many routers in a HSRP group need to be configured with the virtual IP address?
- When does a router in a HSRP group send a coup message?
- How is the HSRP group number identified in the virtual MAC address?

Time

About 30 minutes

Lab/Activity

- Configure HSRP
- Configure HSRP Preemption
- Configure HSRP Interface Tracking

Section 4.3: VRRP Configuration

Summary

This section explores commands used to configure and verify VRRP.

Students will learn how to:

- Configure two routers to form a VRRP group.

Building Converged Cisco Multilayer Switched Networks Objectives

- 402. Configure HSRP, VRRP, and GLBP.
- 403. Verify High Availability configurations.

Lecture Focus Questions:

- What is the difference between setting up a VRRP group or a HSRP group?
- How many routers in a VRRP group need to be configured with the virtual IP address?
- What happens to the VRRP master router when another router in the VRRP group is configured with preemption?

Time

About 10 minutes

Lab/Activity

- Configure VRRP

Section 4.4: GLBP Configuration

Summary

This section discusses commands used to configure and verify GLBP.

Students will learn how to:

- Configure two routers in a GLBP group to form a virtual default gateway, and implement a load balancing method.

Building Converged Cisco Multilayer Switched Networks Objectives

- 402. Configure HSRP, VRRP, and GLBP.
- 403. Verify High Availability configurations.

Lecture Focus Questions:

- What is difference when configuring a GLBP group and a HSRP group?
- What are the different choices available for GLBP load-balancing?

Time

About 10 minutes

Lab/Activity

- Configure GLBP

Section 4.5: Troubleshooting Gateway Redundancy

Summary

This section provides the details of the output generated from the following show commands which are used to troubleshoot gateway redundancy:

- Show stand by
- Show glbp

Students will learn how to:

- Configure a scenario, verify and troubleshoot gateway redundancy configurations.

Building Converged Cisco Multilayer Switched Networks Objectives

- 403. Verify High Availability configurations.

Lecture Focus Questions:

- How can you tell when an interface is participating in a gateway redundancy configuration?
- How does the tracking feature affect a gateway redundancy configuration?
- Which commands allow you to verify a HSRP gateway redundancy configuration?

Time

About 20 minutes

Lab/Activity

- Troubleshoot Gateway Redundancy 1
- Troubleshoot Gateway Redundancy 2

Section 5.1: VoIP Overview

Summary

This section provides an overview of what Voice over IP (VoIP) is and how it functions. Students will become familiar with:

- VoIP call data flows
- Guidelines for implementing VoIP
- Fine-tuning the network

Building Converged Cisco Multilayer Switched Networks Objectives

- 701. Describe the characteristics of voice in the campus network.

Lecture Focus Questions:

- What are the disadvantages of sending voice signals over an IP network?
- Under what circumstances should you enable Quality of Service (QoS) features?
- At what point (in milliseconds) will callers be aware of roundtrip delays?
- What are the characteristics of VoIP traffic?
- What two data flows make up a VoIP call?

Time

About 10 minutes

Section 5.2: Voice VLANs

Summary

In this section students will learn the basics of using a voice VLAN on a switch to separate both data and voice traffic to their respective VLANs. Students will learn the steps to configuring a voice VLAN that operates in a typical Cisco IP Phone daisy chain configuration.

Building Converged Cisco Multilayer Switched Networks Objectives

- 701. Describe the characteristics of voice in the campus network.
- 702. Describe the functions of Voice VLANs and trust boundaries.

Lecture Focus Questions:

- What is the function of a voice VLAN on a switch?
- What is another name for a voice VLAN?
- Which protocol separates voice traffic from data traffic?
- How should you configure an IP phone daisy chain configuration which includes IP phones that do not understand CDP?
- When you disable a voice VLAN on an interface that had the Port Fast feature enabled, what happens to the status of Port Fast?

Time

About 10 minutes

Section 5.3: Quality of Service (QoS) and Trust Boundary

Summary

This section discusses using Quality of Service (QoS) to guarantee a certain level of performance to data flow by managing traffic behavior. Two QoS service models are used in an IP network:

- Integrated services (IntServ)
- Differentiated services (DiffServ)

Cisco switches provide the following QoS components:

- Classification
- Marking
- Traffic conditioning
- Congestion Management and Avoidance

Students will learn details of configuring the trust boundary on devices as close to the traffic source as possible so the proper boundary can be set but not extended too far.

Building Converged Cisco Multilayer Switched Networks Objectives

- 701. Describe the characteristics of voice in the campus network.
- 702. Describe the functions of Voice VLANs and trust boundaries.

Lecture Focus Questions:

- What QoS technologies are available to prevent delay and/or jitter in a VoIP network?
- What is the difference between Auto-QoS and standard QoS methods?
- Where is the best location to set the trust boundary?
- What is the problem with extending the trust boundary too far?

Time

About 15 minutes

Section 5.4: VoIP Configuration

Summary

This section examines configuring VoIP. Students will learn the commands to configure and verify:

- Voice VLANs
- QoS settings on a switch
- Auto-QoS on a switch

Students will learn how to:

- Configure a switch to instruct the IP phone to separate voice traffic to another VLAN.
- Configure a switch to instruct the IP phone to give voice traffic priority and keep all traffic on the access VLAN.
- Configure QoS settings for VoIP with 802.1p and trust CoS values for traffic.
- Configure a trust boundary on the network edge and set trust configurations within the network.
- Configure Auto-QoS on switches for a VoIP configuration.

Building Converged Cisco Multilayer Switched Networks Objectives

- 702. Describe the functions of Voice VLANs and trust boundaries.
- 703. Configure and verify basic IP Phone support (i.e. Voice VLAN, Trust and CoS options, AutoQoS for voice).

Lecture Focus Questions:

- How far should you extend the trust boundary and how is it done?
- How do you configure a switch to instruct an IP phone to separate voice traffic from data traffic?
- How do you configure the switch to trust incoming QoS markings on voice traffic?
- Which command will instruct the IP phone to elevate the priority of voice traffic, but still send all traffic on the access VLAN?
- Which commands will instruct the IP phone to trust or overwrite incoming QoS markings from the workstation?

Time

About 60 minutes

Lab/Activity

- Configure Voice VLANs 1

- Configure Voice VLANs 2
- Configure CoS Trusting
- Configure a Secure Trusted Boundary
- Configure Point-to-Point Trusting
- Configure IP Phone Data Ports
- Configure Auto-QoS 1
- Configure Auto-QoS 2

Section 5.5: Power over Ethernet (PoE)

Summary

This section provides an overview of using Power over Ethernet (PoE) to eliminate the need to have a separate power cable for the phone. Students will become familiar with the commands used to configure PoE on a switch.

Students will learn how to:

- Configure a switch to use PoE for IP phones and for devices which do not need PoE.

Building Converged Cisco Multilayer Switched Networks Objectives

- 701. Describe the characteristics of voice in the campus network.
- 703. Configure and verify basic IP Phone support (i.e. Voice VLAN, Trust and CoS options, AutoQoS for voice).

Lecture Focus Questions:

- What is the advantage of using a switch with PoE capability?
- How does a PoE-capable device notify the switch of its power needs?

Time

About 15 minutes

Lab/Activity

- Configure PoE

Section 6.1: Layer 2 Security Threats

Summary

This section discusses how Layer 2 devices usually have a default operational mode which forwards all traffic unless configured otherwise. Students will learn about typical types of rogue devices and the following types of Layer 2 security threats:

- MAC Flooding
- VLAN Hopping
- DHCP Address Exhaustion and DHCP Server Spoofing
- ARP Spoofing
- MAC Address Spoofing

Building Converged Cisco Multilayer Switched Networks Objectives

- 601. Describe common Layer 2 network attacks (e.g., MAC Flooding, Rogue Devices, VLAN Hopping, DHCP Spoofing, etc.)

Lecture Focus Questions:

- What type of attack causes a switch to act like a hub and send all incoming packets out each port?
- What is the difference between MAC Flooding and MAC Address Spoofing?
- How does ARP Spoofing confuse the network devices?
- How does VLAN hopping allow attackers to gain access to unauthorized VLANs?

Time

About 5 minutes

Section 6.2: Port Security

Summary

This section provides details of configuring switch port security by restricting the devices that can be connected to a switch through the port using the MAC address of the devices. Port security uses the following three MAC address types:

- SecureConfigured
- SecureDynamic
- SecureSticky

Students will become familiar with the commands used to manage switch port security and verify post security operations.

Students will learn how to:

- Configure Port Security by enabling port-security and configuring security parameters.
- Configure Port Security to only allow access of a specific MAC address and drop frames of unauthorized MAC addresses.
- Configure Port Security settings on an interface that has previously been configured to support Voice VLANs.

Building Converged Cisco Multilayer Switched Networks Objectives

- 602. Explain and configure Port Security, 802.1x, VACLs, Private VLANs, DHCP Snooping, and DAI.
- 603. Verify Catalyst switch (IOS-based) security configurations (i.e., Port Security, 802.1x, VACLs, Private VLANs, DHCP Snooping, and DAI).

Lecture Focus Questions:

- What is the main difference between a SecureDynamic address and a SecureSticky address?
- When configuring a Port Security maximum on a port with a voice VLAN, how many MAC addresses should you account for?
- What is the difference between port security and MAC filtering?

Time

About 40 minutes

Lab/Activity

- Configure Port Security 1
- Configure Port Security 2

- Configure Port Security 3

Section 6.3: Additional Switch Security Features

Summary

This section explores additional Switch Security features and the commands to configure each:

- DHCP snooping
- IP Source Guard (IPSG)
- 802.1X port-based authentication
- Dynamic ARP Inspection (DAI)

Also discussed are the four types of ACLs used by Layer 3 catalyst switches to control switched traffic:

- VLAN Access Control List (VACL)
- Router Access Control List (RACL)
- QoS Access Control List (QoS ACL or QACL)
- Port Access Control List (PACL)

Private VLANs (PVLANS) are used to turn a single VLAN broadcast domain into multiple small broadcast domains. Students will become familiar with three types of PVLAN members and considerations when implementing private VLANs:

- Promiscuous port
- Isolated port
- Community port

Students will learn how to:

- Configure DAI to prevent ARP cache poisoning and *man-in-the-middle* attacks.
- Configure DAI to trust inter-network ARP requests.

Building Converged Cisco Multilayer Switched Networks Objectives

- 602. Explain and configure Port Security, 802.1x, VACLs, Private VLANs, DHCP Snooping, and DAI.
- 603. Verify Catalyst switch (IOS-based) security configurations (i.e., Port Security, 802.1x, VACLs, Private VLANs, DHCP Snooping, and DAI).

Lecture Focus Questions:

- How does DHCP snooping provide security for the network?
- Which 802.1X option forces the switch to allow all communication on an interface?

- How does DAI help to prevent *man-in-the-middle* attacks?
- What are the default DAI configuration settings?
- Which type of private VLAN would you typically configure on a default gateway?

Time

About 35 minutes

Lab/Activity

- Configure DAI 1
- Configure DAI 2

Section 6.4: Switch Hardening

Summary

This section discusses switch hardening. Students will learn the actions that can enhance the security of the network:

- Physical security
- Secure password
- Banner
- Unused services
- Console password
- Control remote access
- Secure SNMP
- Unused ports
- Secure STP
- CDP
- AAA Authentication
- Access lists
- HTTP Server

Building Converged Cisco Multilayer Switched Networks Objectives

- 602. Explain and configure Port Security, 802.1x, VACLs, Private VLANs, DHCP Snooping, and DAI.

Lecture Focus Questions:

- Why should you disable CDP on all interfaces with a connection outside the network?
- How does a banner with a warning that displays when a user logs into the router protect the network?
- What different ways can you use to secure passwords?
- What processes can you use to control remote access?

Time

About 10 minutes

Section 7.1: Wireless Overview

Summary

This section provides an overview of wireless networks. Students will become familiar with the following elements of wireless networking:

- Characteristics of radio waves
- Carrier Sense, Multiple Access/Collision Avoidance (CSMA/CA)
- Natural causes that impact broadcasted radio waves
- Methods of wireless networking
- Components of a Wireless network
- Identifiers for wireless networks
- Access points
- Antenna types
- Organizations involved with wireless communication standards
- Wireless standards
- Implementation considerations
- Security methods for wireless networks
- Authentication methods for wireless networks

Building Converged Cisco Multilayer Switched Networks Objectives

- 501. Describe the components and operations of WLAN topologies (i.e., AP and Bridge).

Lecture Focus Questions:

- What is a best practice to eliminate interference caused by wireless devices operating on overlapping channels?
- Which wireless component acts as a hub on the wireless side and a bridge on the wired side?
- What is the difference between an IBSS and ESS?
- What is the difference between refraction and multipath radio wave interference?
- What protocol does an access point use within a wireless mesh network to find the wired network?
- How can you overcome multipath interference in a wireless network?

Time

About 35 minutes

Section 7.2: Cisco Unified Wireless Network

Summary

In this section students will learn how Cisco Unified Wireless Network centralizes WLAN security, deployment and management of a wireless network. They will become familiar with features of the network devices which are part of the Unified Wireless Network infrastructure:

- Wireless LAN Controller (WLAN controller)
- Lightweight Access Point
- Autonomous Access Point
- Client adaptors
- Wireless Bridge

Students will become familiar with the functions of Cisco Aironet Desktop Utility (ADU), the client portion of the Cisco Unified Wireless Network, and considerations when configuring security settings on the ADU. They will learn to recognize the status of the wireless signal depending upon the color of the tray icon.

Building Converged Cisco Multilayer Switched Networks Objectives

- 502. Describe the features of Client Devices, Network Unification, and Mobility Platforms (i.e., CCX, LWAPP).
- 503. Configure a wireless client (i.e., ADU).

Lecture Focus Questions:

- What is the difference between an autonomous access point and a lightweight access point?
- How does a WLAN controller communicate with a lightweight access point?
- What type of traffic is encrypted and encapsulated between a lightweight access point and a WLAN controller?
- What WLAN management devices are found within a Unified Wireless Network infrastructure?
- What is the process used by the lightweight access point to associate with a WLAN controller?
- What are the benefits of using ADU profiles?
- When does a client begin to roam to another access point?
- What does it mean when the ADU tray icon is red?
- How can you enable AES with the ADU?
- In what order should multiple WEP keys be configured on wireless devices?

Time

About 20 minutes

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

- 100. VLANs, All Questions (45 questions)
- 200. Spanning Tree, All Questions (49 questions)
- 300. Inter-VLAN Routing, All Questions (19 questions)
- 400. Gateway Redundancy, All Questions (41 questions)
- 500. Wireless, All Questions (32 questions)
- 600. Security, All Questions (35 questions)
- 700. VoIP, All Questions (35 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 test.