



Cisco | Networking Academy®
Mind Wide Open™

**Scope and
Sequence**

CCNP: Building Multilayer Switched Networks

Cisco Networking Academy: CCNP Version 5.0



This document is exclusive property of Cisco Systems, Inc. Permission is granted to print and copy this document for non-commercial distribution and exclusive use by instructors in the CCNP: Building Multilayer Switched Networks v5.0 course as part of an official Cisco Networking Academy Program.

Cisco Networking Academy Program Version 5.0 TABLE OF CONTENTS

CCNP: BUILDING MULTILAYER SWITCHED NETWORKS.....	1
TARGET AUDIENCE.....	3
PREREQUISITES.....	3
COURSE DESCRIPTION	3
COURSE OBJECTIVES	3
LAB REQUIREMENTS.....	4
CERTIFICATION ALIGNMENT	4
COURSE OVERVIEW.....	4
COURSE OUTLINE	5
<i>Module 1. Network Requirements.....</i>	<i>5</i>
<i>Module 2. Defining VLANs.....</i>	<i>5</i>
<i>Module 3. Implementing Spanning Tree.....</i>	<i>7</i>
<i>Module 4. Implementing Inter-VLAN Routing.....</i>	<i>8</i>
<i>Module 5. Implementing High Availability in a Campus Environment.....</i>	<i>9</i>
<i>Module 6. Wireless LANs.....</i>	<i>10</i>
<i>Module 7. Configuring Campus Switches to Support Voice.....</i>	<i>11</i>
<i>Module 8. Minimizing Service Loss and Data Theft in a Campus Network</i>	<i>12</i>

Target Audience

The target audience is individuals desiring to continue their post-CCNA preparation for a career as a network administrator, Level 2 support engineer, Level 2 systems engineer, network technician, or deployment engineer. This also includes CCNA certified individuals pursuing CCNP, CCIP, CCSP, CCVP, CCDP, or CCIE certifications.



Prerequisites

Prior to taking this course, students should have completed CCNA 1 through 4 or the equivalent. The following prerequisites are beneficial, but not required:

- CCNA certification
- Work experience

Course Description

CCNP: Building Multilayer Switched Networks is one of four courses leading to the Cisco Certified Network Professional (CCNP) designation. Multilayer Switching teaches students about the deployment of state-of-the-art campus LANs. The course focuses on the selection and implementation of the appropriate Cisco IOS services to build reliable, scalable multilayer-switched LANs. Students will develop skills in the following areas:

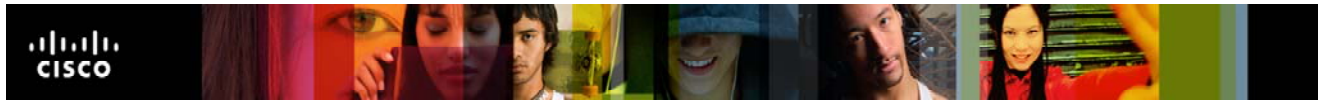
- Introduction to Campus Networks
- Virtual Local Area Networks (VLANs)
- Spanning Tree Protocol
- Inter-VLAN Routing
- High Availability in a Campus Environment
- Wireless Client Access
- Minimizing Service Loss and Data Theft in a Campus Network
- Configuring Campus Switches to Support Voice

This hands-on, lab-oriented course stresses the design, implementation, operation, and troubleshooting of multilayer switched networks.

Course Objectives

Upon completing this course, the learner will be able to meet these overall objectives:

- Describe the Campus Infrastructure module of the ECNM
- Define VLANs to segment network traffic and manage network utilization
- Explain the procedure for configuring both 802.1Q and ISL trunking between two switches so that VLANs that span the switches can connect



- Describe how VLAN configuration of switches in a single management domain can be automated with the Cisco proprietary VTP
- Implement high availability technologies and techniques using multilayer switches in a campus environment
- Understand Wireless LANs
- Describe and configure switch infrastructure to support voice
- Describe and implement security features in a switched network

Lab Requirements

Please refer to the CCNP Equipment Bundle Spreadsheets on Cisco Academy Connection (CAC).

Certification Alignment

The curriculum is aligned with the 642-812 Building Cisco Multilayer Switched Networks (BCMSN) exam. This exam is one of four exams required to achieve the Cisco Certified Network Professional (CCNP) designation.

Course Overview

The course is designed to be delivered in a 70 contact hour time frame. Approximately 45 hours will be devoted to lab activities and 25 hours will be spent on curriculum content. Case studies on multilayer switching are required, but format and timing are to be determined by the Local Academy.

Course Outline

Module 1. Network Requirements

Overview

1.1 Introducing Campus Networks

1.1.1 Intelligent Information Network and Service-Oriented Network Architecture Layer 2 Network Issues

1.1.2 Cisco Network Models

- 1.1.3 Discussing Non-Hierarchical Campus Network Issues
- 1.1.4 Describing Layer 2 Network Issues
- 1.1.5 Describing Routed Network Issues
- 1.1.6 Multilayer Switching
- 1.1.7 Issues with Multilayer Switches and VLANs in a Non-Hierarchical Network
- 1.1.8 Enterprise Composite Network Model
- 1.1.9 Benefits of the Enterprise Composite Network Model
- 1.1.10 Describing the Campus Infrastructure Module
- 1.1.11 Reviewing Switch Configuration Interfaces Module Summary Module Quiz

Module 2. Defining VLANs

Overview

2.1 Implementing Best Practices for VLAN Topologies

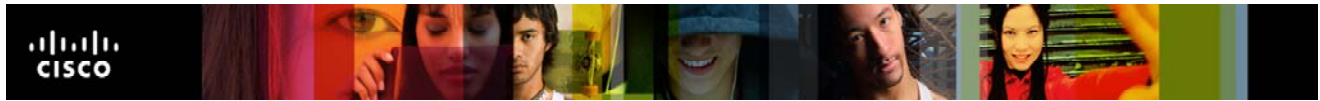
- 2.1.1 Describing Issues in a Poorly Designed Network
- 2.1.2 Grouping Business Functions into VLANs
- 2.1.3 Describing Interconnection Technologies
- 2.1.4 Determining Equipment and Cabling Needs
- 2.1.5 Considering Traffic Source to Destination Paths
- 2.1.6 Describing End-to-End VLANs
- 2.1.7 Describing Local VLANs
- 2.1.8 Benefits of Local VLANs in Enterprise Campus Network
- 2.1.9 Mapping VLANs in a Hierarchical Network

2.2 Implementing VLANs

- 2.2.1 VLAN Configuration Modes
- 2.2.2 Explaining VLAN Access Ports
- 2.2.3 Describing VLAN Implementation Commands
- 2.2.4 Implementing a VLAN

2.3 Implementing Trunks

- 2.3.1 Explaining VLAN Trunks



- 2.3.2 Describing ISL Trunking
- 2.3.3 Describing 802.1Q Trunking
- 2.3.4 Explaining 802.1Q Native VLANs
- 2.3.5 Explaining VLAN Ranges
- 2.3.6 Describing Trunking Configuration Commands
- 2.3.7 Configuring Trunking

2.4 Propagating VLAN Configurations with VLAN Trunking

- 2.4.1 Explaining VTP Domains
- 2.4.2 Describing VTP
- 2.4.3 VTP Modes
- 2.4.4 Describing VTP Pruning
- 2.4.5 Describing VTP Operation
- 2.4.6 Describing VTP Configuration Command
- 2.4.7 Configuring a VTP Management Domain
- 2.4.8 Adding New Switching to an Existing VTP Domain

2.5 Correcting Common VMAL Configuration Errors

- 2.5.1 Describing Issues with 802.1Q Native VLANs
- 2.5.2 Resolving Issues with 802.1Q Native VLANs
- 2.5.3 Describing Trunk Link Problems
- 2.5.4 Resolving Trunk Link Problems
- 2.5.5 Common Problems with VTP Configuration
- 2.5.6 Best Practice for VTP Configuration

2.6 VLAN Lab Exercises

- 2.6.1 Clearing a Switch
- 2.6.2 Catalyst 2960 and 3560 Series Static VLANs, VLAN Trunking, and VTP Domain and Modes

Module Summary Module Quiz

Module 3. Implementing Spanning Tree



Overview

3.1 Describing STP

3.1.1 Describing Transparent Bridges

3.1.2 Identifying Traffic Loops

3.1.3 Explaining a Loop Free Network

3.1.4 Describing the 802.1D Spanning Tree Protocol

3.1.5 Describing the Root Bridge

3.1.6 Describing Port Roles

3.1.7 Explaining Enhancements to STP

3.2 Implementing RSTP

3.2.1 Describing the Rapid Spanning Tree Protocol

3.2.2 Describing RSTP Port States

3.2.3 Describing RSTP Port Roles

3.2.4 Explaining Edge Ports

3.2.5 Describing RSTP Link Types

3.2.6 Examining the RSTP BPDU

3.2.7 Identifying the RSTP Proposal and Agreement Process

3.2.8 Identifying the RSTP Topology Change

3.2.9 Describing Rapid PVST Implementation

3.2.10 Implementing Rapid PVST Commands

3.3 Implementing MSTP

3.3.1 Explaining MSTP

3.3.2 Describing MST Regions

3.3.3 Describing the Extended System ID

3.3.4 Interacting Between MST Regions and 802.1D Networks

3.3.5 Describing MSTP Implementation Commands

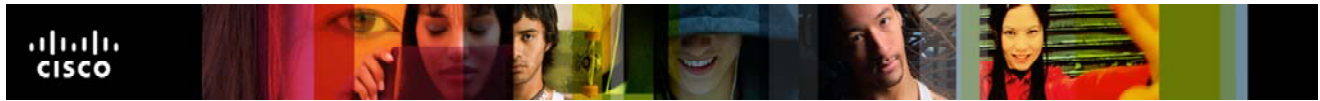
3.3.6 Configuring and Verifying MSTP

3.4 Configuring Link Aggregation with EtherChannel

3.4.1 Describing EtherChannel

3.4.2 Describing PAgP and LACP

3.4.3 Describing EtherChannel Configuration Commands



- 3.4.4 Configuring Port Channels Using EtherChannel
- 3.4.5 Configuring Load Balancing over EtherChannel
- 3.5 Implementing Spanning Tree Labs
 - 3.5.1 Spanning Tree Protocol (STP) Default Behavior
 - 3.5.2 Modifying Default Spanning Tree Behavior
 - 3.5.3 Per-VLAN Spanning Tree Behavior
 - 3.5.4 Multiple Spanning Tree
- 3.5.5 Configuring Etherchannel
- Module Summary
- Module Quiz

Module 4. Implementing Inter-VLAN Routing

Overview

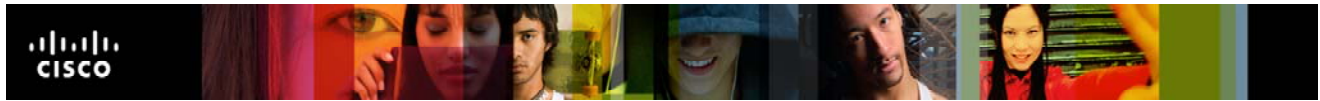
4.1 Describing Routing Between VLANs

- 4.1.1 Inter-VLAN Routing Using an External Router
- 4.1.2 Describing Inter-VLAN Routing Using External Router Configuration Commands
- 4.1.3 Configuring Inter-VLAN Routing Using an External Router
- 4.1.4 Explaining Multilayer Switching
- 4.1.5 Frame Rewrite

4.2 Enabling Routing Between VLANs

- 4.2.1 Describing Layer 3 SVIs
- 4.2.2 Describing Configuration Commands for Inter-VLAN Communication on a Multilayer Switch
- 4.2.3 Configuring Inter-VLAN Routing on a Multilayer Switch
- 4.2.4 Describing Routed Ports on a Multilayer Switch
- 4.2.5 Configuration of Routed Ports on a Multilayer Switch
- 4.2.6 Configuring Routed Ports on a Multilayer Switch

4.3 Deploying CEF-Based Multilayer Switching



- 4.3.1 Explaining Layer 3 Switch Processing
- 4.3.2 Explaining CEF-Based Multilayer Switches
- 4.3.3 Identifying the Multilayer Switch Packet Forwarding Process
- 4.3.4 Describing CEF Configuration Commands
- 4.3.5 Enabling CEF-Based MLS
- 4.3.6 Describing Common CEF Problems and Solutions
- 4.3.7 Describing CEF Troubleshooting Commands
- 4.3.8 Troubleshooting Layer 3 CEF-Based MLS

4.4 Inter-VLAN Routing Lab Exercises

- 4.4.1 Inter-VLAN Routing with an External Router
 - 4.4.2 Inter-VLAN Routing with an Internal Route Processor and Monitoring CEF Functions
- Module Summary

Module Quiz

Module 5. Implementing High Availability in a Campus Environment

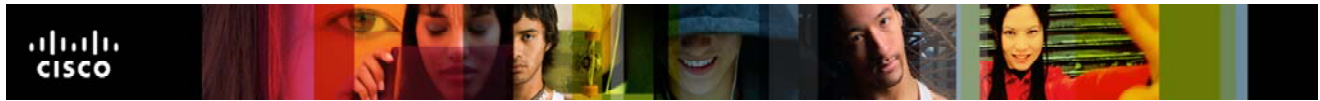
Overview

5.1 Configuring Layer 3 Redundancy with HSRP

- 5.1.1 Describing Routing Issues
- 5.1.2 Identifying the Router Redundancy Process
- 5.1.3 Describing HSRP
- 5.1.4 Identifying HSRP Operations
- 5.1.5 Describing HSRP States
- 5.1.6 Describing HSRP Configuration Commands
- 5.1.7 Enabling HSRP

5.2 Optimizing HSRP

- 5.2.1 Describing HSRP Optimization Options
- 5.2.2 Tuning HSRP Operations
- 5.2.3 Describing Load Sharing
- 5.2.4 HSRP Debug Commands



5.2.5 Debugging HSRP Operations

5.3 Configuring Layer 3 Redundancy with VRRP and GLBP

5.3.1 Describing Virtual Router Redundancy

5.3.2 Identifying the VRRP Operations Process

5.3.3 Configuring VRRP

5.3.4 Describing GLBP

5.3.5 Identifying the GLBP Operations Process

5.4 Implementing High Availability Lab

5.4.1 Hot Standby Routing Protocol

Module Summary

Module Quiz

Module 6. Wireless LANs

Overview

6.1 Introducing Wireless LANs

6.1.1 Wireless Data Technologies

6.1.2 Wireless LANs

6.1.3 WLANs and Other Wireless Technologies

6.1.4 WLANs and LANs

6.2 Describing Wireless LAN Topologies

6.2.1 WLAN Topologies

6.2.2 Typical WLAN Topologies

6.2.3 Roaming through Wireless Cells

6.2.4 Wireless VLAN Support

6.2.5 Wireless Mesh Networking

6.3 Explaining Wireless LAN Technology Standards

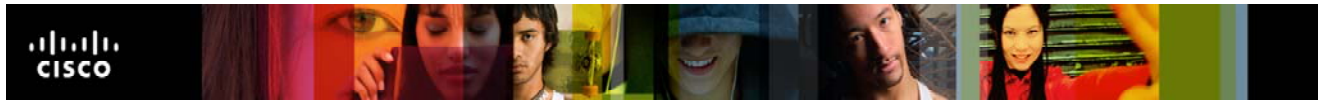
6.3.1 Unlicensed Frequency Bands

6.3.2 WLAN Regulation and Standardization

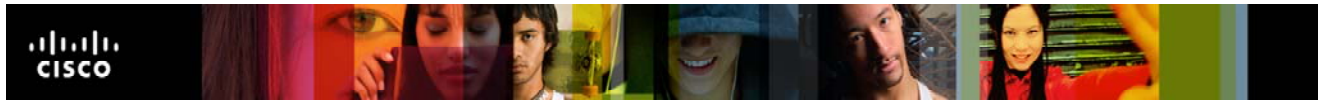
6.3.3 IEEE 802.11b Standard

6.3.4 IEEE 802.11a Standard

6.3.5 IEEE 802.11g Standard



- 6.3.6 802.11 Comparison
- 6.3.7 General Office Wireless LAN Design
- 6.3.8 WLAN Security
- 6.4 Configuring Cisco WLAN Clients
 - 6.4.1 Cisco 802.11a/b/g WLAN Client Adapters
 - 6.4.2 Cisco Aironet Desktop Utility Installation
 - 6.4.3 ADU Diagnostics: Advanced Statistics
 - 6.4.4 Cisco Aironet Site Survey Utility: Associated AP Status
 - 6.4.5 Windows XP WLAN Configuration
 - 6.4.6 Cisco Aironet Client Administration Utility
 - 6.4.7 Cisco WLAN IP Phone
 - 6.4.8 Compatible Extensions Program for WLAN Client Devices
- 6.5 Implementing Wireless LANs
 - 6.5.1 Wireless Client Association
 - 6.5.2 Lightweight Access Point Protocol
 - 6.5.3 Describing WLAN Components
 - 6.5.4 Cisco Unified Wireless Network
 - 6.5.5 Cisco Aironet Access Points and Bridges
 - 6.5.6 Power over Ethernet
 - 6.5.7 Explaining WLAN Antennas
 - 6.5.8 Multipath Distortion
 - 6.5.9 Definition of a Decibel
 - 6.5.10 Effective Isotropic Radiated Power
- 6.6 Configuring Wireless LANs
 - 6.6.1 Autonomous Access Point Configuration
 - 6.6.2 Role of Autonomous Access Points in a Radio Network
 - 6.6.3 Autonomous Access Point Configuration via the Web Browser
 - 6.6.4 Lightweight Wireless LAN Controller Configuration
 - 6.6.5 Cisco Wireless LAN Controller Boot Menu
 - 6.6.6 Web Wizard Initial Configuration
- 6.7 Challenge Labs



- 6.7.1 Configuring a WLAN Controller
- 6.7.2 Configuring a WLAN Controller via the Web Interface

6.7.3 Configuring a Wireless Client

Module Summary

Module Quiz

Module 7. Configuring Campus Switches to Support Voice

7.1 Planning for Implementation of Voice in a Campus Network

- 7.1.1 Converged Network Benefits
- 7.1.2 VoIP Network Components
- 7.1.3 Traffic Characteristics of Voice and Data
- 7.1.4 VoIP Call Flow
- 7.1.5 Auxiliary VLANs
- 7.1.6 QoS
- 7.1.7 Importance of High Availability for VoIP
- 7.1.8 Power Requirements in Support of VoIP

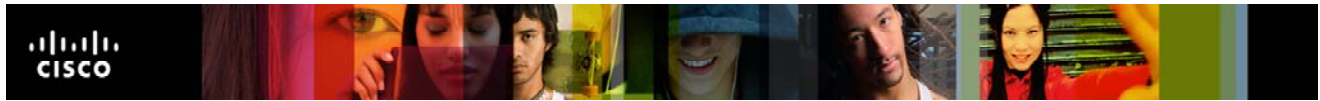
7.2 Accommodating Voice Traffic on Campus Switches

- 7.2.1 QoS and Voice Traffic in the Campus Module
- 7.2.2 LAN-Based Classification and Marking
- 7.2.3 Describing QoS Trust Boundaries
- 7.2.4 Configuring a Switch for the Attachment of a Cisco Phone
- 7.2.5 Basic Switch Commands to Support Attachment of a Cisco IP Phone
- 7.2.6 What is AutoQoS VoIP?
- 7.2.7 Configuring AutoQoS VoIP on a Cisco Catalyst Switch

7.3 Challenge Labs

7.3.1 Configuring Switches for IP Telephone Support Module Summary Module Quiz

Module 8. Minimizing Service Loss and Data Theft in a Campus Network



Overview

8.1 Understanding Switch Security Issues

- 8.1.1 Overview of Switch Security Concerns
- 8.1.2 Describing Unauthorized Access by Rogue Devices
- 8.1.3 Switch Attack Categories
- 8.1.4 Describing a MAC Flooding Attack
- 8.1.5 Describing Port Security
- 8.1.6 Configuring Port Security on a Switch
- 8.1.7 Port Security with Sticky MAC Addresses
- 8.1.8 Authentication, Authorization, and Accounting
- 8.1.9 Authentication xCMethods
- 8.1.10 802.1x Port-Based Authentication

8.2 Protecting against VLAN Attacks

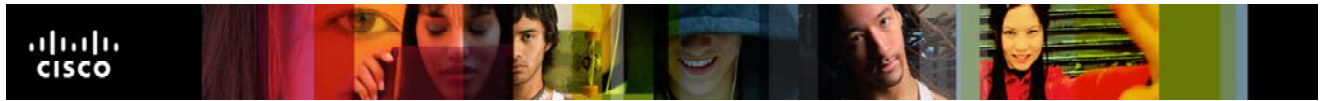
- 8.2.1 Explaining VLAN Hopping
- 8.2.2 Mitigating VLAN Hopping
- 8.2.3 VLAN Access Control Lists
- 8.2.4 Configuring VACLs
- 8.2.5 Private VLANs and Protected Ports
- 8.2.6 Configuring PVLANS

8.3 Protecting against Spoof Attacks

- 8.3.1 Describing a DHCP Spoof Attack
- 8.3.2 Describing DHCP Snooping
- 8.3.3 Configuring DHCP Snooping
- 8.3.4 Describing ARP Spoofing
- 8.3.5 Dynamic ARP Inspection
- 8.3.6 Configuring Dynamic ARP Inspection
- 8.3.7 Protecting against ARP Spoofing Attacks

8.4 STP Security Mechanisms

- 8.4.1 Protecting the Operation of STP
- 8.4.2 Configuring BPDU Guard
- 8.4.3 Configuring BPDU Filtering



8.4.4	Root Guard	
8.4.5	Configuring Root Guard	
8.5	Preventing STP Forwarding Loops	
8.5.1	Unidirectional Link Detection	
8.5.2	Loop Guard	
8.5.3	Configuring UDLD and Loop Guard	
8.5.4	Preventing STP Failures Due to Unidirectional Links	
8.6	Securing Network Switches	
8.6.1	Describing Vulnerabilities in CDP	
8.6.2	Telnet Protocol Vulnerabilities	
8.6.3	Configuring the Secure Shell Protocol	
8.6.4	VTY ACLs	
8.6.5	Applying ACLs to VTY Lines	
8.6.6	Best Practices for Switch Security	
8.7	Challenge Labs	
8.7.1	Securing Layer 2 Switching Devices	
8.7.2	Securing the Spanning Tree Protocol	
8.7.3	Securing the VLANs with Private VLANs, RAACLs and VACLs	
Module		Summary
Module		Quiz

Case Studies

- 1 VLANs, VTP and Inter-VLAN Routing
- 2 Voice and Security in a Switched Network