Cisco CCNP

SWITCH: Implementing Cisco IP Switched Networks (SWITCH) 2.0

This course is a component of the Cisco CCNP Routing and Switching curriculum. This live class is available virtually with RemoteLive™ or locally at our Phoenix, AZ location.

$3,595.00

- 5 Days
- This course is a component of the Cisco CCNP Routing and Switching curriculum.

Upcoming Dates

Course Description

Implementing Cisco Switched Networks (SWITCH) v2.0 is a five-day instructor-led training course, designed to help students prepare to plan, configure, and verify the implementation of complex enterprise switching solutions for campus environments using the Cisco Enterprise Campus Architecture. These skills are validated in the Cisco CCNP©_ Routing and Switching certification, a professional-level certification specializing in the routing and switching field. This course is a component of the Cisco CCNP Routing and Switching curriculum. This course is designed to give students a firm understanding of how to manage switches in an enterprise campus environment. This training class reinforces the instruction by providing students with hands-on labs.

Course Outline

1. Analyzing Campus Network Designs

Enterprise Campus Architecture

- Describe Cisco SONA
- Evaluate the benefits of the enterprise campus architecture
- Determine the function of the core layer
- Evaluate the impact of traffic types on the network infrastructure

Cisco Lifecycle Services and Network Implementation

- Describe the PPDIOO life-cycle approach
- Describe PPDIOO implementation planning

2. Implementing VLANs in Campus Networks

Applying Best Practices for VLAN Topologies

- Describe the different VLAN segmentation models
- Given an enterprise VLAN network design, describe the information needed to create an implementation plan, identify the choices that need to be made, and analyze the consequences of those choices
- Given an enterprise VLAN network design that
  contains end-to-end VLANs and trunks, create an implementation and verification plan; then successfully execute that plan

- Given an enterprise VLAN network design that contains VTP, create an implementation and verification plan; then successfully execute that plan

Configuring Private VLANs

- Describe PVLANs
- Configure isolated PVLANs
- Configure community PVLANs
- Given an enterprise VLAN network design that contains PVLANs, create an implementation and verification plan; then successfully execute that plan
- Configure PVLANs across multiple switches

Configuring Link Aggregation with EtherChannel

- Understand the benefits of EtherChannel
- Compare the PAGP and the LACP
- Given an enterprise VLAN network design that contains Layer 2 EtherChannel links, create an implementation and verification plan; then successfully execute that plan
- Given an enterprise VLAN network design that contains load balancing among the ports included in an EtherChannel, create an implementation and verification plan; then successfully execute that plan

3. Implementing Spanning Tree

Spanning Tree Protocol Enhancements

- Describe the various STP standards
- Describe STP operations
- Implement and configure PVRST+
- Understand RSTP port roles
- Verify RSTP configurations
- Describe MSTP
- Implement and configure MSTP

Describing STP Stability Mechanisms

- Protect the operation of STP
- Configure BPDUGuard
- Configure BPDUFilter
- Configure RootGuard
- Configure LoopGuard
- Configure UDLD to detect and shut down unidirectional links
- Optimize STP operations by using the right combination of STP stability features

4. Implementing Inter-VLAN Routing

Describing Routing Between VLANs

- Configure both a switch and router to accommodate inter-VLAN packet transfer using an external router
- Describe a Layer 3 SVI
- Understand commands that are used to configure an SVI
- Describe a routed port on a multilayer switch
- Understand commands that are used to configure a routed port on a multilayer switch
- Configure Layer 3 Ether Channel links
- Configure inter-VLAN routing on a multilayer switch
- Configure DHCP services on a Layer 3 switch

Deploying Multilayer Switching with Cisco Express Forwarding

- Understand the process of multilayer switching, and how it differs when you are performing Layer 2 versus Layer 3 switching
- Understand the packet and frame header rewriting that is performed by a multilayer switch
- Explain Layer 3 switch processing
- Describe the various switching methods that are available on a Cisco switch
- Describe and configure Cisco Express Forwarding on a Cisco switch

5. Implementing a Highly Available Network

Understanding High Availability

- Evaluate the uses, requirements, benefits, and performance expectations of high availability in a given enterprise network design
- Describe resiliency for high availability
- Design the network for optimal redundancy

Implementing High Availability

- Implement high availability at the switch level
- Use Cisco StackWise technology on access switches
- Evaluate the impact of too little redundancy
- Assess the impact of uplink failure

Implementing Network Monitoring

- Implement network monitoring
- Configure IP SLA technology

6. Implementing Layer 3 High Availability

Configuring Layer 3 Redundancy with HSRP

- Describe routing issues
- Identify the router redundancy process
- Configure HSRP operations
- Describe and fine-tune HSRP Troubleshoot HSRP

Configuring Layer 3 Redundancy with VRRP and GLBP

- Describe VRRPIdentify the VRRP operations process
- Configure VRRP
- Describe GLBP
- Identify the GLBP operations process
- Configure GLBP

7. Minimizing Service Loss and Data Theft in a Campus Network

Understanding Switch Security Issues

- Describe switch and Layer 2 security as a subset of an overall network security plan
- Describe how a rogue device gains unauthorized access to a network
- Categorize switch attack types and list mitigation options
- Describe how a MAC flooding attack works to overflow a CAM Campus Backbone Layer table
- Describe how port security is used to block input from devices based on Layer 2 restrictions
- Describe the procedure for configuring port security on a switch
- Describe the methods that can be used for authentication using AAA

- Describe port-based authentication using 802.1X

Protecting Against VLAN Attacks

- Describe how VLAN hopping occurs and why it is a security vulnerability
- Explain the procedure for configuring a switch to mitigate VLAN hopping attacks
- Describe VACLs and their purpose as part of VLAN security
- Explain the procedure for configuring VACLs

Protecting Against Spoofing Attacks

- Identify DHCP spoofing attacks
- Prevent attacks using DHCP snooping
- Configure DHCP snooping
- Describe ARP poisoning
- Protect against ARP spoofing attacks with DAI

Securing Network Services

- Identify Cisco Discovery Protocol and LLDP vulnerabilities
- Identify Telnet protocol vulnerabilities
- Configure SSH
- Configure vty ACLs
- Configure Cisco IOS secure HTTP server
- Understand switch security considerations

8. Accommodating Voice and Video in Campus Networks

Planning for Support of Voice in a Campus Network

- Discuss the components of a VoIP network and the components of IP telephony
- Compare the uniform bandwidth consumption of voice traffic to the intermittent bandwidth consumption of data traffic
- Compare video bandwidth consumption to voice and data bandwidth consumption based on video application types
- Identify a solution for latency, jitter, bandwidth, packet loss, reliability, and security for voice and video traffic integration into a data network

Integrating and Verifying VoIP in a Campus Infrastructure

- Plan for VoIP requirements
- Describe Voice VLANs
- Configure and Verify Voice VLANs
- Plan PoE requirements and configure PoE
- Provide additional services required by VoIP devices
- Create a Test Plan for VoIP integration

Working with Specialists to Accommodate Voice and Video on Campus Switches

- Describe high availability applied to VoIP or video traffic
- Build an integrated voice/video/data campus network
- Explain the need for QoS for VoIP and video integration

9: Integrating Wireless LANs into a Campus Network

Comparing WLANs with Campus Networks

- Describe WLANs
- Compare wired and wireless LAN
- Describe main wireless LAN topologies
- Describe the settings specific to WLANs, such as SSIDs, and WLAN-to-VLAN mapping

Assessing the Impact of WLANs on Campus Networks

- Describe WLAN implementations
- Compare WLAN solutions
- Assess traffic flow in an autonomous AP configuration and its impact on the campus LAN
- Assess traffic flow in an controller-based configuration and its impact on the campus LAN

Preparing the Campus Infrastructure for WLANs

- Decide on the best placement for APs and controllers
- Configure switches for WLAN devices
- Gather WLAN requirements
- Plan WLAN integration
- Create a test plan

Audience

This course is intended for those engineers who are candidates for Cisco CCNP certifications as well as those who are candidates for Cisco CCIE Routing and Switching and CCIE certifications. Others who will benefit from this course are:

- Network professionals who will need to correctly implement switch-based solutions given a network design using Cisco IOS services and features. The typical job roles for this type of professional are network engineers; network operations center (NOC) technical support personnel, or help desk technicians.
- Any individual involved in network operations and support.

Prerequisites

Knowledge and experience equivalent to having attended the Interconnecting Cisco Networking Devices Part 1 (ICND1) and Interconnecting Cisco Networking Devices Part 2 (ICND2) courses. This includes knowledge and experience of the following issues:

- Network function, the functions of network components, the Open Systems Interconnection (OSI) reference model, and the ability to identify major network components
- Use of the host-to-host packet delivery process to describe issues related to increasing traffic on an Ethernet LAN and identifying switched LAN technology solutions to Ethernet networking issues
- The reasons for extending the reach of a LAN, and the methods that can be used to extend this reach, with a focus on RF wireless access
- The reasons for connecting networks with routers, and how routed networks transmit data through the use of TCP/IP
- The function of WANs and major WAN devices; configuration of PPP encapsulation, static and dynamic routing, and Port Address Translation (PAT) and Routing Information Protocol (RIP) routing
- Use of the command-line interface (CLI) to discover neighbors on the network and manage router startup and configuration
- How to configure and troubleshoot a small network
- How to expand a small-sized, switched LAN to a medium-sized LAN with multiple switches, supporting VLANs, trunking, and spanning tree
- Routing concepts as they apply to a medium-sized network and considerations when implementing routing on the network
- Configuring, verifying, and troubleshooting Open Shortest Path First (OSPF)
- Configuring, verifying, and troubleshooting Enhanced Interior Gateway Routing Protocol (EIGRP)
- How to apply access control lists (ACLs) based on network requirements, and configure, verify, and troubleshoot ACLs on a medium-sized network
- When to use Network Address Translation (NAT) or PAT on a medium-sized network and configure NAT or PAT on routers, and knowledge of IPv6 addressing and configuration IPv6 in a Cisco router

- How to identify and implement the appropriate WAN technology based on network requirement

What You Will Learn

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

- Analyze campus network designs
- Implement VLANs in a network campus
- Implement spanning tree
- Implement inter-VLAN routing in a campus network
- Implement a highly available network
- Implement high-availability technologies and techniques using multilayer switches in a campus environment
- Implement security features in a switched network
- Integrate WLANs into a campus network
- Accommodate voice and video in campus network