Hands-On

SWITCH Implementing Cisco IP Switched Networks

CCNP Course 2

Course Description

Revised CCNP Curriculum and Exams

Cisco has redesigned the CCNP courses and exams to reflect the evolving job tasks of global network professionals.

Course 1 ROUTE v1.0 Implementing Cisco IP Routing is a five-day instructor-led course in which network professionals learn to plan, configure, and verify the implementation of complex enterprise LAN and WAN routing solutions, using a range of routing protocols. ROUTE v1.0 also covers configuration of secure routing solutions to support branch offices and mobile workers. The course includes more than seven hours of e-learning lessons and demos that students can absorb at their own pace.

Course 2 SWITCH v1.0 Implementing Cisco IP Switched Networks is a five-day instructor-led course in which network professionals will learn to plan, configure, and verify the implementation of complex enterprise switching solutions, using Cisco Enterprise Campus Architecture. SWITCH v1.0 also covers secure integration of VLANs, WLANs, voice, and video into campus networks.

Course 3 TSHOOT v1.0 Troubleshooting and Maintaining Cisco IP Networks is a five-day instructor-led course in which network professionals learn to (1) plan and perform regular maintenance on complex enterprise routed and switched networks, and (2) use technology-based practices and a systematic ITIL-compliant approach to perform network troubleshooting. Extensive labs provide hands-on learning and reinforce troubleshooting skills. The course includes more than nine hours of e-learning lessons and demos that students can absorb at their own pace.Learn the advanced routing skills you need to provide scalability for Cisco routers that are connected to LANs and WANs as part of a medium-to-large network site. You will learn how to dramatically increase the number of routers and sites using EIGRP and OSPF techniques, instead of redesigning the network when additional sites or configurations are added.

This Course 2 SWITCH v1.0 Implementing Cisco IP Switched Networks includes extensive hands-on labs to help you learn to plan, configure, and verify the implementation of complex enterprise switching solutions for campus environments using the Cisco Enterprise Campus Architecture. In order to gain a firm understanding of how to manage switches in an enterprise campus environment, you'll cover VLANs and WLANs, Spanning tree, Inter-VLAN routing Security features and many study aides and materials to pass your exam.

Students Will Learn

- **Analyze campus network designs**
- **Implement VLANs in a network campus**
- **Implement spanning tree**
- **Implement inter-VLAN routing in a campus 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 networks**

Target Audience

Network engineers with at least one year of professional work experience who are ready to advance their skills and work independently on complex network solutions

Network engineers, technical support personnel, or help desk technicians who will need to correctly implement and/or support switch-based solutions

Prerequisites

CCNA certification

OR

Familiarity with internetworking technologies the ability to perform basic router configuration experience installing, operating, and maintaining routers and switches in an enterprise environment

Knowledge of IP, including the ability to perform IP subnetting on non-octal boundaries, configure IP standard and extended access lists, operate and configure distance vector routing protocol, configure serial interface, and interpret a routing table

Course Outline

1. Analyzing Campus Network Designs

- Enterprise Campus Architecture
  - Cisco SONA
  - Benefits of the enterprise campus architecture
  - Function of the core layer
  - Impact of traffic types on the network infrastructure
- Cisco Lifecycle Services and Network Implementation
  - PPDIOO lifecycle approach
  - PPDIOO implementation planning

2. Implementing VLANs in Campus Networks

- Best Practices for VLAN Topologies
  - VLAN segmentation models
  - Creating an implementation plan
  - Implementation choices and their consequences
  - Implementation and verification plans for a VLAN network with end-to-end VLANs and trunks and VLAN Trunk Protocol (VTP)
- Configuring Private VLANs (PVLANs)
  - Configure isolated and community PVLANs
  - Implementation and verification plans for a VLAN network design that contains PVLANs
  - Configure PVLANs across multiple switches
- Configuring Link Aggregation with EtherChannel
  - Benefits of EtherChannel
  - Compare the PAgP and the LACP
  - Create and execute an implementation and verification plan in a VLAN network with Layer 2 EtherChannel links and load balancing among the ports included in an EtherChannel

3. Implementing Spanning Tree

- Spanning Tree Protocol (STP) Enhancements
  - STP standards and operations
  - Implement and configure PVRST+ and MSTP
  - RSTP port roles
  - Verify RSTP configurations
- STP Stability Mechanisms
  - Protect and optimize the operation of STP
  - Configure BPDUGuard, BPDUFilter, RootGuard, and LoopGuard
  - Configure UDLD to detect and shut down unidirectional links

4. Implementing Inter-VLAN Routing

- Routing Between VLANs
  - Configure and verify inter-VLAN routing in a Layer 2 topology using an external router, a switch SVI, or a switch-routed interface
  - Configure both a switch and router to accommodate inter-VLAN packet transfer using an external router
  - Layer 3 SVI
  - Commands used to configure an SVI
  - A routed port on a multilayer switch
  - Commands used to configure a routed port on a multilayer switch
  - Configure Layer 3 EtherChannel links
  - Configure inter-VLAN routing on a multilayer switch
  - Configure DHCP services on a Layer 3 switch
- Deploying Multilayer Switching with Cisco Express Forwarding
  - Configure and verify inter-VLAN routing in a Layer 2 topology using multilayer switching with Cisco Express Forwarding
  - Multilayer switching and how it differs when you are performing Layer 2 vs. Layer 3 switching
  - Packet and frame header rewriting performed by a multilayer switch
  - Layer 3 switch processing
  - Switching methods available on a Cisco switch
  - Configure Cisco Express Forwarding on a Cisco switch

5. Implementing a Highly Available Network

- High Availability
    - Uses, requirements, benefits, and performance expectations
    - Resiliency for high availability
    - Design the network for optimal redundancy
- Implementing High Availability
    - Use Cisco StackWise technology on access switches
    - Evaluate the impact of too little redundancy
    - Assess the impact of uplink failure
- Implementing Network Monitoring
    - Configure IP SLA technology

6. Implementing Layer 3 High Availability

- Configuring Layer 3 Redundancy with HSRP
    - Routing issues
    - Router redundancy process
    - Configure HSRP operations
    - Fine-tune and troubleshoot HSRP
- Configuring Layer 3 Redundancy with VRRP and GLBP
    - VRRP operations process
    - Configure VRRP
    - GLBP operations process
    - Configure GLBP

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

- Switch Security Issues
    - Switch and Layer 2 security as a subset of an overall network security plan
    - How a rogue device gains unauthorized access to a network
    - Categorize switch attack types and list mitigation options
    - How a MAC flooding attack overflows a CAM Campus Backbone Layer table
    - How port security is used to block input from devices based on Layer 2 restrictions
    - Configure port security on a switch
    - Authentication methods using AAA
    - Port-based authentication using 802.1X
- Protecting Against VLAN Attacks
    - VLAN hopping
    - Configure a switch to mitigate VLAN hopping attacks
    - VACLs and their purpose as part of VLAN security
    - Configure VACLs
- Protecting Against Spoofing Attacks
    - DHCP spoofing attacks
    - Configure DHCP snooping
    - ARP poisoning
    - Protect against ARP spoofing attacks with DAI
- Securing Network Services
    - Cisco Discovery Protocol and LLDP vulnerabilities
    - Telnet protocol vulnerabilities
    - Configure SSH

    - Configure vty ACLs
    - Configure Cisco IOS secure HTTP server
    - Switch security considerations

8. Accommodating Voice and Video in Campus Networks
    - Planning for Support of Voice in a Campus Network
        - Components of a VoIP network and IP telephony
        - Bandwidth consumption of voice traffic vs. data traffic
        - Video bandwidth consumption vs. voice and data bandwidth consumption
        - Solve for latency, jitter, bandwidth, packet loss, and reliability
        - Security for voice and video traffic integration into a data network
    - Integrating and Verifying VoIP in a Campus Infrastructure
        - Plan for VoIP requirements
        - 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
    - Accommodate Voice and Video on Campus Switches
        - High availability applied to VoIP or video traffic
        - Build an integrated voice/video/data campus network
        - The need for QoS for VoIP and video integration
        - Configure basic QoS for voice and video VLANs

9. Integrating Wireless LANs into a Campus Network
    - Comparing WLANs with Campus Networks
        - Compare wired and wireless LAN
        - Main wireless LAN topologies
        - Settings specific to WLANs, such as SSIDs, and WLAN-to-VLAN mapping
    - Assessing the Impact of WLANs on Campus Networks
        - WLAN implementations
        - Compare WLAN solutions
        - Assess traffic flow and impact on the campus LAN of an autonomous AP configuration and a controller-based configuration
    - Preparing the Campus Infrastructure for WLANs
        - Best placement for APs and controllers
        - Configure switches for WLAN devices
        - Gather WLAN requirements
        - Plan WLAN integration
        - Create a test plan

Delivery Method

Instructor-Led with numerous Hands-On labs and exercises.

Equipment Requirements

(This apply's to our hands-on courses only)

BTS always provides equipment to have a very successful Hands-On course. BTS also encourages all attendees to bring their own equipment to the course. This will provide attendees the opportunity to incorporate their own gear into the labs and gain valuable training using their specific equipment.

Course Length

5 Days