Implementing Cisco IP Switched Networks (SWITCH) 2.0

Course Overview:

Implementing Cisco IP Switched Networks (SWITCH) v2.0 is a 5-day training program designed to give you the knowledge and skills needed to create an efficient and expandable enterprise network. You will focus on Layer 2 and multilayer switch functions including VLANs, trunks, inter-VLAN routing, port aggregation, spanning tree, first hop redundancy, as well as network security and high availability features. The Cisco CCNP switch course will provide you with in-demand skills such as configuring Layer 2 and Layer 3 port aggregation, implements inter-VLAN routing, and working with network security features to keep data safe. Sign up for this CCNA study course and get the skills you need for your position or to advance your career.

Who Should Attend:

- Network engineers and technicians
- Support engineers
- Systems engineers
- Network analysts
- Senior network administrators
- Anyone involved in planning, implementing, verifying, and troubleshooting switch-based solutions in enterprise networks

Prerequisites:

The knowledge and skills you must have before taking this course consist of the following:

- Taking ICND1 v2.0 and ICND2 v2.0 (or CCNAX v2.0) is highly recommended
- Know how to:
  - Configure network fundamentals, including the ability to establish Internet, LAN, and WAN connectivity using both IPv4 and IPv6
  - Operate and support a medium-sized LAN that has multiple switches, including VLANs, trunking, and spanning tree functionality
  - Troubleshoot IPv4 and IPv6 connectivity issues
  - Configure and troubleshoot EIGRP and OSPF, for both IPv4 and IPv6
  - Configure devices for SNMP, Syslog, and NetFlow

- Manage network device security, Cisco device configurations, Cisco IOS images, and licenses
- ICND1 v2.0 - Interconnecting Cisco Networking Devices, Part 1
- ICND2 v2.0 - Interconnecting Cisco Networking Devices, Part 2
- CCNAX v2.0 - CCNA Routing and Switching Boot Camp

Course Objectives:

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

- Components of the Cisco Enterprise Campus Architecture including the operation of Layer 2 and multilayer switches
- Switching Database Manager (SDM) templates and how they are used
- Implementing device features including LLDP and PoE
- VLANs and trunks and how VTP works
- Configuring a device to be a DHCP server and relay agent, for both IPv4 and IPv6
- Configuring Layer 2 and Layer 3 port aggregation
- Different types of spanning tree protocols and mechanisms, including STP, RSTP, and MST
- Implementing inter-VLAN routing on both a router and a multilayer switch
- Network high availability including NTP, SNMPv3, IP SLA, port mirroring, and switch virtualization
- First hop redundancy protocols for IPv4 and IPv6 including HSRP, VRRP, and GLBP
- Implementing network security features including port security, storm control, DHCP snooping, IP source guard, dynamic ARP inspection, VLAN ACLs, and private VLANs
- Using an external authentication server in your network, including implementing IEEE 802.1x

Course Outline:

Module 1: Basic Concepts and Network Design

- Analyzing Campus Network Structure
- Comparing Layer 2 and Multilayer Switches
- Using Cisco SDM Templates
- Implementing LLDP
- Implementing PoE

Module 2: Campus Network Architecture

- Implementing VLANs and Trunks
- Introducing VTP
- Implementing DHCP
- Implementing DHCP for IPv6
- Configuring Layer 2 Port Aggregation

Module 3: Spanning Tree Implementation

- Implementing RSTP
- Implementing STP Stability Mechanisms
- Implementing Multiple Spanning Tree Protocol

Module 4: Configuring Inter-VLAN Routing

- Implementing Inter-VLAN Routing Using a Router
- Configuring a Switch to Route

Module 5: Implementing High Availability Networks

- Configuring Network Time Protocol
- Implementing SNMP Version 3
- Implementing IP SLA
- Implementing Port Mirroring for Monitoring Support
- Verifying Switch Virtualization

Module 6: First Hop Redundancy Implementation

- Configuring Layer 3 Redundancy with HSRP
- Configuring Layer 3 Redundancy with VRRP
- Configure VRRP With Load Balancing
- Configuring Layer 3 Redundancy with GLBP
- Configuring First Hop Redundancy for IPv6

Module 7: Campus Network Security

- Implementing Port Security
- Implementing Storm Control
- Implementing Access to External Authentication
- Mitigating Spoofing Attacks
- Securing VLAN Trunks
- Configuring Private VLANs

Lab Outline:

- Discovery 1: Investigating the CAM
- Discovery 2: Configuring VLANs and Trunks
- Discovery 3: VTP Operation
- Discovery 4: Exploring DHCP
- Discovery 5: Obtaining IPv6 Address Dynamically
- Discovery 6: EtherChannel Configuration and Load Balancing
- Discovery 7: Discovering and Modifying STP Behavior
- Discovery 8: RootGuard
- Discovery 9: Configuring MST
- Discovery 10: Routing with an External Router
- Discovery 11: Routing on a Multilayer Switch
- Discovery 12: NTP Configuration
- Discovery 13: IP SLA Echo Configuration
- Discovery 14: Configuring and Tuning HSRP
- Discovery 15: Configure VRRP and Spot the Differences from HSRP
- Discovery 16: Configure GLBP
- Discovery 17: Port Security
- Challenge 1: Network Discovery
- Challenge 2: Configure DHCP
- Challenge 3: Configure DHCPv6
- Challenge 4: Configure EtherChannel
- Challenge 5: Implementing Rapid Spanning-Tree
- Challenge 6: Improving STP Configuration
- Challenge 7: Configure MST
- Challenge 8: Configure Routing Between VLANs Using a Router
- Challenge 9: Configure Routing on a Multilayer Switch
- Challenge 10: Configure NTP
- Challenge 11: Configure Network Monitoring Using IP SLA
- Challenge 12: Configure HSRP With Load Balancing
- Challenge 13: Configure VRRP With Load Balancing
- Challenge 14: Implement GLBP
- Challenge 15: Configure HSRP for IPv6

- Challenge 16: Controlling Network Access Using Port Security