

# CISCO

## Cisco Associate-Level Training

### I. CCDA

#### 1. Applying a Methodology to Network Design

- Introducing SONA
- Identify Design Requirements
- Characterizing the Existing Network
- Using the Top-Down Approach
- Implementing the Design Methodology

#### 2. Structuring and Modularizing the Network

- Designing the Network Hierarchy
- Using a Modular Approach in Network Design
- Using Infrastructure Services
- Identifying Network Management Protocols and Features

#### 3. Basic Campus and Data Center Design Considerations

- Campus Design Methodology
- Designing the Campus Infrastructure Module
- Enterprise Data Center Considerations

#### 4. Designing Remote Connectivity

- Enterprise Edge WAN Design Methodology
- Selecting Wide Area Network Technology
- Designing the Enterprise Branch

#### 5. Designing IP Addressing in the Network and Selecting Routing Protocols

- Designing IP Addressing
- Introduction to IPv6
- Reviewing Enterprise Routing Protocols
- Designing a Routing Protocol Deployment

## **6. Evaluating Security Solutions for the Network**

- Defining Network Security
- The Cisco Self-Defending Network
- Selecting Network Security Solutions

## **7. Designing Voice Networking**

- Traditional Voice Architectures and Features
- Integrating Voice Architectures
- Identify the Requirements of Voice Technologies

## **8. Wireless Network Considerations**

- Cisco Unified Wireless Network
- Wireless Network Controller Technologies
- Designing Wireless Networks with Controllers

## **9. Additional Resources**

# **II. CCENT**

## **1. Building a Simple Network**

- Exploring the Functions of Networking
- Host-to-Host Communication Model
- TCP/IP Internet Layer
- TCP/IP Transport Layer
- Exploring the Packet Delivery Process
- Ethernet
- Connecting to an Ethernet LAN

## **2. Ethernet LANs**

- Understanding the Challenges of Shared LANs
- Solving Network Challenges with Switched LAN Technology
- Exploring the Packet Delivery Process

## **3. Wireless LANs**

- Exploring Wireless Networking

## **4. LAN Connections**

- Exploring the Functions of Routing
- Understanding Binary Basics
- Constructing a Network Addressing Scheme

## **5. Switches**

- Operating Cisco IOS Software
- Starting the Switch
- Implementing VLANs and Trunks
- Improving Performance with Spanning Tree
- Routing Between VLANs

## **6. Routers**

- Starting a Router
- Configuring a Router
- Exploring the Packet Delivery Process
- Accessing Remote Devices

## **7. WANs**

- Understanding WAN Technologies
- Enabling the Internet Connection
- Configuring Serial Encapsulation
- Point-to-Point WAN Connection with PPP
- WAN Connection with Frame Relay

## **8. Routing Concepts**

- Reviewing Routing Operations
- Distance Vector Routing
- Link State Routing
- Enabling Static Routing
- Routing Information Protocol (RIP)
- OSPF
- EIGRP
- Implementing VLSM

## **9. Network Environment Management**

- Discovering Neighbors on the Network
- Managing Router Startup and Configuration
- Managing Cisco Devices

## **10. ACLs**

- Introducing ACL Operation
- Configuring and Troubleshooting ACLs

## **11. Address Space Management**

- Scaling the Network with NAT and PAT

# III. CCNA

## 1. Building a Simple Network (ICND1)

- Exploring the Functions of Networking
- Securing the Network
- Host-to-Host Communication Model
- TCP/IP's Internet Layer
- TCP/IP's Transport Layer
- Packet Delivery Process
- Understanding Ethernet
- Connecting to an Ethernet LAN

## 2. Ethernet LANs (ICND1)

- Challenges of Shared LANs
- Solving Network Challenges with Switched LAN Technology
- Packet Delivery Process
- Operating Cisco IOS Software
- Starting the Switch
- Understanding Switch Security
- Maximizing the Benefits of Switching
- Troubleshooting Switch Issues

## 3. Wireless Local Area Networks (WLANS) (ICND1)

- Exploring Wireless Networking
- Understanding WLAN Security
- Implementing a WLAN

## 4. LAN Connections (ICND1)

- Functions of Routing
- Understanding Binary Basics
- Constructing a Network Addressing Scheme
- Starting a Router
- Configuring a Router
- Packet Delivery Process
- Understanding Router Security
- Using Cisco Router and Security Device Manager
- Using a Router as a DHCP Server
- Accessing Remote Devices

## 5. Network Environment Management (ICND1)

- Discovering Neighbors on the Network
- Managing Router Startup and Configuration
- Managing Cisco Devices

## **6. Small Network Implementation (ICND2)**

- Review Lab: Review of a Small Network Environment

## **7. Medium-Sized Switched Network Construction (ICND2)**

- Implementing VLANs and Trunks
- Improving Performance with Spanning Tree
- Routing Between VLANs
- Securing the Expanded Network
- Troubleshooting Switched Networks

## **8. Wide Area Networks (WANs) (ICND1)**

- WAN Technologies
- Enabling the Internet Connection
- Enabling Static Routing
- Configuring Serial Encapsulation
- Enabling Routing Information Protocol (RIP)

## **9. LAN Extension into a WAN (ICND2)**

- Establishing a Point-to-Point WAN Connection with PPP
- Establishing a WAN Connection with Frame Relay
- Troubleshooting Frame Relay WANs
- Introducing VPN Solutions

## **10. Medium-Sized Routed Network Construction (ICND2)**

- Reviewing Routing Operations
- Implementing VLSM

## **11. Single Area OSPF Implementation (ICND2)**

- Implementing OSPF
- Troubleshooting OSPF

## **12. EIGRP Implementation (ICND2)**

- Implementing EIGRP
- Troubleshooting EIGRP

## **13. Access Control Lists (ACLs) (ICND2)**

- Introducing ACL Operation
- Configuring and Troubleshooting ACLs

## 14. Address Space Management (ICND2)

- Scaling the Network with NAT and PAT
- Transitioning to IPv6

# Cisco Professional-Level Training

## I. CCDP

### BSCI - Building Scalable Cisco Internetworks v3.0

This course will help you develop an advanced set of skills to learn to optimize the configuration and deployment of a Cisco router-based internetwork. Learn the complex concepts and commands necessary to configure Cisco routers for scalable operation in large and/or growing internetworks. Whether your goal is to take your Cisco routing skills to the next level or to achieve CCNP or CCIP certification, this is the right course for you.

#### What You'll Learn

- Converged network requirements of various network and networked applications within the Cisco network architectures
- Advanced IP address configuration techniques to optimize your network
- Implement and verify EIGRP operations
- Build a scalable multi-area network with OSPF
- Configure integrated IS-IS in a single area
- Manipulate routing and packet flow
- Implement and verify BGP for enterprise ISP connectivity
- Implement and verify multicast forwarding using PIM and related protocols
- Network reconfiguration to adapt to new technologies, including IPv6
- How IPv6 functions in order to satisfy the increasingly complex requirements of hierarchical addressing
- IPv6 routing protocols

## **BSCI Course Outline**

- 1. Network Requirements**
- 2. Configuring EIGRP**
- 3. Configuring OSPF**
- 4. The IS-IS Protocol**
- 5. Manipulating Routing Updates**
- 6. Configuring Basic BGP**
- 7. Implementing IP Multicast**
- 8: Implementing IPv6**

## **BCMSN - Building Cisco Multilayer Switched Networks v3.0 Self-Paced e-Learning**

In this course, learn to implement campus networks using multilayer switching technologies over high-speed Ethernet and wireless topologies. This course addresses the integration of routing and switching technologies to create an efficient campus network. Design, build, and configure a campus network with device and link redundancy for high reliability, while maintaining the performance to meet today's demanding application requirements, such as voice, video, and secure wireless technologies. Learn to choose and configure the necessary Layer 2 and 3 protocols and features to guarantee constant access.

Technologies such as Spanning Tree, Rapid Spanning Tree (802.1W), Multiple Spanning Tree (802.1S), Uplinkfast, and Backbonefast will be covered in detail to determine how to optimize a network's convergence times in the event a physical path fails. Also learn how to get more bandwidth between network devices by configuring EtherChannel. Learn the advantages of and how to configure and troubleshoot HSRP, convergence of voice, video, and data in a real-time environment, and QoS. Configure basic security options such as 802.1x, Port security, BPDU guard, and DHCP spoof attack prevention.

This package includes in-depth lab demonstrations.

### **What You'll Learn**

- Create VLANs
- Propagate VLAN information with VTP
- Manage Redundant Links with Spanning Tree
- Enable InterVLAN Routing
- Improve IP Routing performance with Multilayer Switching
- Implement HSRP for Fault Tolerant Routing
- Implement secure wireless connectivity into the campus topology
- Use QoS to meet the service levels required by applications
- Secure the network and eliminate unwanted traffic

## **BCMSN Course Outline**

### **1. Introduction to Campus Networks**

- Campus Networks as part of an Enterprise Network
- Devices in a Nonhierarchical Network
- Layer 2 Network Issues
- Routed Network Issues
- What is a Multilayer Switch
- Issues with Multilayer Switches and VLANs in a Nonhierarchical Network
- The Enterprise Composite Model
- Benefits of the Enterprise Composite Model
- Campus Infrastructure Module

### **2. Defining Virtual Networks (VLANs)**

- Best Practices for VLAN Topologies
- Implementing VLANs
- Implementing Trunks
- Propagating VLAN Configurations with VTP
- Correcting Common VLAN Configuration Errors

### **3. Implementing Spanning Tree**

- Spanning Tree Protocol
- Preventing STP Forwarding Loops
- Implementing Rapid Spanning Tree Protocol (RSTP)
- Implementing the Multiple Spanning Tree Protocol (MSTP)
- Configuring Link Aggregation and EtherChannel

### **4. Implementing InterVLAN Routing**

- Routing Between VLANs
- Deploying CEF-Based Multilayer Switching
- Enabling Routing Between VLANs

### **5. Implementing High Availability in a Campus Environment**

- Configuring Layer 3 Redundancy with HSRP
- Configuring Layer 3 Redundancy with VRRP and GLBP

### **6. Wireless Client Access**

- Introducing Wireless LANs (WLANs)
- Wireless Theory and Standards
- Implementing WLANs
- Cisco WLAN
- Cisco Wireless Clients
- Configuring Basic WLAN

## **7. Configuring Campus Switches to Support Voice**

- Planning for Implementation of Voice in a Campus Network
- Accommodating Voice Traffic on Campus Switches

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

- Switch Security Issues
- Protecting Against VLAN Attacks
- Protecting Against Spoof Attacks
- Securing Network Switches
- STP Security Mechanisms

## **ARCH - Designing Cisco Network Service Architectures v1.0 Self-Paced e-Learning**

Gain the skills necessary to apply Cisco Network Solution Models and best practices to design stable, scalable, and optimal IP network solutions. Cisco AVVID network design principles are emphasized throughout this course.

### **What you'll learn**

- Apply design solutions to an enterprise network
- Present scalable, stable, and optimal enterprise network solutions geared to the customers' requirements
- Design for large-scale IP networks and complex Campus networks for the enterprises
- Fundamental aspects of the network solutions addressing QoS, Security, Network Management, fine-tuning Routing Protocols, Switching Structures, and IP Multicast
- Incorporate strategic technologies into your network, including Voice over IP, IP telephony, content and storage networking, wireless networking, and broadband access

### **ARCH Course Outline**

#### **1. Cisco Network Service Architectures**

- Why companies are seeking to implement enterprise-wide infrastructures to serve as a viable foundation to support emerging new technologies such as IP telephony, content networking, and storage networking
- Why enterprises commonly use WANs, on-demand connections, and the Internet to build an intranet
- Using the Cisco AVVID framework to support the operation of concurrent solutions
- The Enterprise Composite Network Model and how it is used in the design process

## **2. Designing Network Services**

- Implementation of the FCAPS network management process and the significant differences between reactive and proactive network management methods
- Design Cisco network management solutions for small, medium, and large enterprise networks, given specific network management requirements
- Necessary components of a high availability solution for the Enterprise Campus and the Enterprise Edge functional areas
- Appropriate actions that can be taken to prevent or mitigate the consequences of a network attack

## **3. Designing for Bandwidth and Delay Sensitive Traffic**

- How bandwidth-intensive applications may stretch network capabilities and resources and how to achieve the required QoS by managing delay, delay variation (jitter), bandwidth, and packet loss
- How multicasting provides bandwidth conservation to reduce traffic load by simultaneously delivering a single stream of information to multiple recipients and enabling multiple services
- NAT and IPSec issues associated with a remote-access VPN topology

## **4. Designing for Wireless and IP Telephony Networks**

- Benefits of wireless networks, including high-speed data rates and the freedom of mobility by being able to access broadband data anywhere within the LAN
- Compare the three different IEEE 802.11 standards that make up the group of protocol specifications for WLANs
- Components of a Cisco wireless solution
- Design a physical and logical IP telephony network, network features, and intelligent network services to support IP telephony, including Cisco CallManager clusters and CAC functionality

## **5. Designing for Content and Storage Networking Solutions**

- Components of Cisco's content networking solutions, including content edge delivery (caching), content switching, content routing, and content delivery and management
- How caching is used to dramatically improve end user response times in a content network
- Design for content networking to minimize the impact to an existing network and to scale to meet the end user's needs
- Design for IP-based storage networking in a Cisco environment
- Differences between NAS and SANs network storage models.
- Importance of Intelligent Network Services and their use in supporting storage networking.

# II. CCNP

- All four CCNP courses
  - BSCI - Building Scalable Cisco Internetworks v3.0
  - BCMSN - Building Cisco Multilayer Switched Networks v3.0
  - ISCW - Implementing Secure Converged Wide Area Networks
  - ONT - Optimizing Converged Cisco Networks
  
- a) BSCI - Building Scalable Cisco Internetworks v3.0

## 1. Network Requirements

## 2. Configuring EIGRP

- Introducing EIGRP
- Implementing and Verifying EIGRP
- Configuring Advanced EIGRP Options
- Configuring EIGRP Authentication
- Using EIGRP in an Enterprise Network

## 3. Configuring OSPF

- Introducing the OSPF Protocol
- OSPF Packet Types
- Configuring OSPF Routing
- OSPF Network Types
- Link State Advertisements
- Configuring OSPF Route Summarization
- Configuring OSPF Special Area Types
- Configuring OSPF Authentication

## 4. The IS-IS Protocol

- Introducing IS-IS and Integrated IS-IS Routing
- IS-IS Routing Operation
- Configuring Basic Integrated IS-IS

## 5. Manipulating Routing Updates

- Operating a Network Using Multiple IP Routing Protocols
- Configuring and Verifying Route Redistribution
- Controlling Routing Update Traffic
- Implementing Advanced IOS Features: Configuring DHCP

## **6. Configuring Basic BGP**

- Explaining BGP Concepts and Terminology
- Explaining EBGp and IBGP
- Configuring Basic BGP Operations
- Selecting a BGP Path
- Using Route Maps to Manipulate Basic BGP Paths

## **7. Implementing IP Multicast**

- Explaining Multicast
- IGMP and Layer 2 Issues
- Explaining Multicast Routing Protocols
- Multicast Configuration and Verification

## **8: Implementing IPv6**

- Introducing IPv6
- Defining IPv6 Addressing
- Implementing Dynamic IPv6 Addresses
- Using IPv6 with OSPF and Other Routing Protocols
- Using IPv6 with IPv4

b) BCMSN - Building Cisco Multilayer Switched Networks v3.0

## **1. Introduction to Campus Networks**

- Course Introduction
- Campus Networks as part of an Enterprise Network
- Devices in a Nonhierarchical Network
- Layer 2 Network Issues
- Routed Network Issues
- What is a Multilayer Switch
- Issues with Multilayer Switches and VLANs in a Nonhierarchical Network
- The Enterprise Composite Model
  - Building Access
  - Building Distribution
  - Server Farm Module
  - Campus Core
  - Network Management
- Benefits of the Enterprise Composite Model
- Campus Infrastructure Module

## **2. Defining Virtual Networks (VLANs)**

- Best Practices for VLAN Topologies
  - Issues in a Poorly Designed Network
  - Grouping Business Functions into VLANs
  - Interconnection Technologies
  - Determining Equipment and Cabling Needs
  - Mapping VLANs in a Hierarchical Network

- Considering Traffic Source to Destination
  - Reviewing Switch Configuration Interfaces
- Implementing VLANs
  - Benefits of VLANs in an Enterprise Network
  - Local VLANs
  - End-to-End VLANs
  - VLAN Configuration Modes
  - VLAN Access Ports
  - VLAN Implementation Commands
  - Implementing a VLAN
- Implementing Trunks
  - VLAN Trunks
  - ISL Trunking
  - 802.1Q Trunking
  - 802.1Q Native VLANs
  - Issues with 802.1Q Native VLANs
  - VLAN Ranges
  - Trunking Configuration Commands
  - Configuring Trunking
  - Setting Dynamic Trunking Protocol (DTP)
- Propagating VLAN Configurations with VTP
  - VTP Domains
  - VTP Protocol
  - VTP Modes
  - VTP Pruning
  - VTP Operation
  - VTP Configuration Commands
  - Configuring a VTP Management Domain
  - Adding New Switches to an Existing VTP
- Correcting Common VLAN Configuration Errors
  - Issues with 802.1Q Native VLANs
  - Resolving Trunk Link Problems

### **3. Implementing Spanning Tree**

- Spanning Tree Protocol
  - Transparent Bridges
  - Identifying Traffic Loops
  - Loop Free Network
  - 802.1D Spanning Tree Protocol
  - Root Bridge
  - Port Roles
  - Enhancements to STP
- Preventing STP Forwarding Loops
  - Unidirectional Link Detection
  - Loop Guard
  - Preventing STP Failures Due to Unidirectional Links
  - Configuring UDLD and Loop Guard

- Implementing Rapid Spanning Tree Protocol (RSTP)
  - RSTP
  - RSTP Port States
  - RSTP Port Roles
  - Edge Ports
  - RSTP Link Types
  - RSTP BPDU
  - RSTP Proposal and Agreement Process
  - RSTP Topology Change
  - RSTP Implementation Commands
  - Implementing RSTP Commands
- Implementing the Multiple Spanning Tree Protocol (MSTP)
  - MSTP
  - MSTP Regions
  - Extended System ID
  - Interacting between MSTP regions and 802.1Q
  - MSPT Implementation Commands
  - Configuring and Verifying MSTP
- Configuring Link Aggregation and EtherChannel
  - EtherChannel
  - PAgP and LACP Protocols
  - EtherChannel Configuration
  - Configuring Port Channels using EtherChannel
  - Configuring Load Balancing over EtherChannel

#### **4. Implementing InterVLAN Routing**

- Routing Between VLANs
  - Multilayer Switching
  - Layer 2 Switch Forwarding Process
  - Inter-VLAN Routing using an External Router
  - Inter-VLAN Routing using External Router Configuration Commands
  - Configuring Inter-VLAN Routing using an External Router
- Deploying CEF-Based Multilayer Switching
  - Layer 3 Switching
  - CEF-Based Multilayer Switches
  - Multilayer Switch Packet Forwarding Process
  - CEF Configuration Commands
  - Enabling CEF-Based Multilayer Switching
  - Common CEF problems and Solutions
  - CEF Troubleshooting Commands
  - Troubleshooting CEF-Based Multilayer Switching
- Enabling Routing Between VLANs
  - Layer 3 Switch Virtual Interfaces
  - Routed Interfaces on a Multilayer Switch
  - Configuration Commands for Inter-VLAN Communication on a Multilayer Switch
  - Configuring Inter-VLAN Routing on a Multilayer Switch

## 5. Implementing High Availability in a Campus Environment

- Configuring Layer 3 Redundancy with HSRP
  - Router Redundancy Process
  - Routing Issues
  - HSRP
  - HSRP Operations
  - HSRP States
  - HSRP Configuration Commands
  - Enabling HSRP
  - HSRP Optimization Options
  - Tuning HSRP Operations
  - HSRP Debug Commands
  - Debugging HSRP Operations
- Configuring Layer 3 Redundancy with VRRP and GLBP
  - Virtual Router Redundancy
  - VRRP Operations Process
  - Gateway Load Balancing Protocol
  - GLBP Operations Process
  - VRRP and GLBP Configuration
  - Enabling VRRP and GLBP

## 6. Wireless Client Access

- Introducing Wireless LANs (WLANs)
  - WLANs
  - Similarities Between A LAN and a WLAN
  - Differences Between a LAN and WLAN
  - WLAN Components
  - WLAN Technology Implementations
  - Building Blocks of AP WLAN Topologies
  - Building Blocks of Bridging WLAN Topologies
  - Topology Implementations
- Wireless Theory and Standards
  - Radio Frequency (RF) Basics
  - WLAN Math
  - Types of Antennas
  - Regulatory Agencies Governing WLANs
  - Operational Standards of IEEE 802.11
  - IEEE 802.11 Standards in the 2.4GHz Band
  - IEEE 802.11a
  - Comparing the 802.11 Standards
- Implementing WLANs
  - 802.11b/g Channel Reuse
  - 802.11a Channel Reuse
  - WLAN as a Shared Medium - Best Practices
  - Bridging Path Considerations
  - Power Implementation

- Cisco WLAN
  - Enterprise WLAN Issues
  - Overview of Cisco WLAN
  - Comparing Autonomous and Lightweight WLAN
  - Comparing Core and Advanced Feature Roaming
  - Split MAC Architecture
  - LWAPP AP Association
  - Mixing WLAPP with Autonomous APs
- Cisco Wireless Clients
  - Wireless Client Association
  - Open Authentication
  - Pre-Shared Key Authentication (WEP)
  - Introducing WLAN Security
  - Cisco Client Cards
  - Cisco Compatible Extensions Program
- Configuring Basic WLAN
  - Available Interfaces for WLAN Configuration
  - Connect to Controller
  - Configuring the Controller
  - Verify Controller Configuration

## **7. Configuring Campus Switches to Support Voice**

- Planning for Implementation of Voice in a Campus Network
  - Converged Network Benefits
  - VoIP Network Components
  - Traffic Characteristics of Voice and Data
  - VoIP Call Flow
  - Auxiliary VLANs
  - Quality of Service (QoS)
  - Importance of High Availability for VoIP
  - Power Requirements in Support of VoIP
- Accommodating Voice Traffic on Campus Switches
  - QoS Trust Boundaries
  - LAN-Based Classification and Marking
  - Basic Switch Commands to Support Attachment of a Cisco IP Phone
  - Configuring a Switch for the Attachment of a Cisco IP Phone
  - What is AutoQoS VoIP?
  - Configuring AutoQoS VoIP on a Catalyst Switch

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

- Switch Security Issues
  - Overview of Switch Security Concerns
  - Switch Attack Categories
  - MAC Flood Attack
  - Port Security
  - Port Security Configuration
  - Configuring Port Security on a Switch
  - Port Security with Sticky MAC Addresses
  - Unauthorized Access by Rogue Devices
  - 802.1x Port-Based Authentication

- Protecting Against VLAN Attacks
  - VLAN Hopping
  - Mitigating VLAN Hopping
  - VLAN Access Control Lists (VACLs)
  - Configuring VACLs
  - Private VLANs (PVLANS)
  - Configuring PVLANS
- Protecting Against Spoof Attacks
  - DHCP Spoof Attack
  - DHCP Snooping
  - DHCP Snooping Configuration Commands
  - Configuring DHCP Snooping
  - MAC Spoof Attack
  - Address Resolution Protocol
  - Commands to Configure Dynamic ARP Inspection
  - Protecting Against ARP Spoofing Attacks
- Securing Network Switches
  - Vulnerabilities in the Cisco Discovery Protocol
  - Vulnerabilities in the Secure Shell Protocol
  - Vulnerabilities in the Telnet Protocol
  - VTY ACLs
  - Commands to Apply ACLs to VTY
  
- STP Security Mechanisms
  - Protecting the Operation of STP
  - BPDU Guard Configuration
  - BPDU Filtering Configuration
  - Root Guard
  - Root Guard Configuration Commands
  - Configuring Root Guard

c) ISCW - Implementing Secure Converged Wide Area Networks

## 1. Network Requirements

- The IIN and the SONA framework
- Cisco conceptual network models, such as Cisco Enterprise Architecture and Cisco hierarchical network model
- Requirements for establishing secure remote connections in a converged network

## 2. Connect Teleworkers

- Topologies for Facilitating Remote Connections
  - Typical remote connections an enterprise network has to support
  - Challenges faced in connecting teleworkers to the enterprise network and the solutions that exist to address these challenges
- Cable Technology
  - Basic terminology and standards organizations that are relevant to cable technology
  - Components of a cable system that provide data services
  - Features of cable technology
  - How digital cable systems use the RF bands for signal transmission
  - How data services can be delivered over a cable network using an HFC architecture
  - Combination of technologies and components that make a cable system work
  - Provisioning a cable modem in a TCP/IP-based customer network
- DSL Technology
  - Features of DSL
  - Variants of DSL
  - Distance limitations of DSL
  - Basic facts of ADSL technology
  - How ADSL coexists with telephony service
  - CAP and DMT: the competing modulation standards for ADSL signaling
  - How data is transmitted over ADSL infrastructure with PPPoE
  - How data is transmitted over ADSL infrastructure with PPPoA
- Configuring the CPE as the PPPoE and PPPoA Client
  - Configure a Cisco router as a PPPoE client
  - Configure an ATM interface for PPPoE client operations
  - Configure the PPPoE DSL dialer interface
  - Configure PAT
  - Configure a DHCP server to allocate IP address to the users behind the client DSL router
  - Configure a static route
  - Review the output of various **debug** and **show** commands to verify the PPPoE operations
  - Step-by-step procedure to configure a PPPoA on the CPE router
  - Configure the DSL ATM interface
- Verifying Broadband ADSL Configurations
  - Bottom-up approach to troubleshoot a DSL connection problem
  - Isolate problems to Layer 1
  - Confirm an Administratively Down state
  - Confirm the correct DSL operating mode on the CPE router ATM interface
  - Isolate problems to Layer 2
  - Determine if data is being received from the ISP
  - Determine if PPP is negotiating successfully

### 3. Cisco Device Hardening

- Mitigating Network Attacks
  - Cisco Self-Defending Network strategy
  - Types of attacks that enterprise networks must defend against
  - Mitigate reconnaissance attacks including packet sniffers, port scans, ping sweeps, and Internet information queries
  - Mitigate access attacks including password attacks, trust exploitation, buffer overflow, port redirection, and man-in-the-middle attacks
  - Mitigate DoS attacks including IP spoofing and DDoS
  - Mitigate worm, virus, and Trojan horse attacks
  - Mitigate application layer attacks
  - Vulnerabilities in configuration management protocols and recommendations for mitigating these vulnerabilities
  - Use open source tools to discover network vulnerabilities and threats
- Securing Cisco Router Installations and Administrative Access
  - Configuring passwords
  - Setting a login failure rate and using IOS login enhancements
  - Setting timeouts
  - Setting multiple privilege levels
  - Configuring banner messages
  - Role-based CLI and the commands required to configure basic CLI views
  - Secure the Cisco IOS boot image and configuration files
- Configuring AAA on Cisco Routers
  - Three components of AAA
  - AAA access modes
  - AAA RADIUS and TACACS+ protocols
  - Configure AAA login authentication on Cisco routers using CLI
  - Configure AAA login authentication on Cisco routers using Security Device Manager (SDM)
  - Troubleshoot AAA on a Cisco perimeter router using the **debug aaa** command
  - AAA authorization and the commands that are required to configure it on Cisco routers
  - AAA accounting and the commands that are required to configure it on Cisco routers
- Disabling Unused Cisco Router Network Services and Interfaces
  - Router services and interfaces that are vulnerable to network attack
  - Using the **auto secure** command to automate the process of locking down a Cisco router
  - Configure AutoSecure on a Cisco router
  - Compare the process of locking down a Cisco router with the CLI **auto secure** command and the One-Step Lockdown mode of the Security Audit wizard available in SDM

- Securing Management and Reporting Features
  - Factors you must consider when planning the secure management and reporting configuration of network devices
  - Factors that affect the architecture of secure management and reporting in terms of in-band and OOB information paths
  - Steps used to configure an SSH server for secure management and reporting
  - How the syslog function plays a key role in network security
  - How to configure syslog on Cisco routers using **syslog** router commands
  - Security features of SNMPv3
  - Configure SNMPv3 on a Cisco IOS router or a switch
  - Configure an NTP client including authentication in client mode
  - Configure a Cisco router as an NTP server
- Mitigating Threats and Attacks with Access Lists
  - Types and formats of IP ACLs used by routers to restrict access and filter packets
  - Apply ACLs to router interfaces
  - Using traffic filtering with ACLs to mitigate threats in a network
  - Implement ACLs to mitigate threats
  - Configure router ACLs to help reduce the effects of DDoS attacks
  - Combine many ACL functions into two or three larger ACLs
  - Some of the caveats to be considered when building ACLs

#### 4. Cisco IOS Threat Defense Features

- Introducing the Cisco IOS Firewall
  - Basic structure of a layered defense
  - Operational strengths and weaknesses of the three firewall technologies
  - Basic operation of a stateful firewall
  - Features of the Cisco IOS Firewall
  - How the Cisco IOS Firewall combines the features of packet inspection and proxy firewalls to provide an optimal security solution
  - Cisco IOS Firewall process
- Implementing Cisco IOS Firewalls
  - Configure Cisco IOS Firewall from the Cisco IOS CLI
  - When and how to use the Basic and Advanced Firewall Configuration wizards in SDM
  - Configure a basic firewall using SDM
  - Configure the interfaces on an advanced firewall using SDM
  - Configure a DMZ on an advanced firewall
  - Configure inspection rules
  - Complete the Advanced Firewall wizard configuration by viewing the settings in the Summary window
  - Use the SDM logging function to monitor firewall activity
- Introducing Cisco IOS IPS
  - Functions and operations of IDS and IPS systems and the difference between IDS and IPS
  - Types of IDS and IPS systems
  - Four types of IDS and IPS signatures
  - What happens when a signature is matched

- Configuring Cisco IOS IPS
  - Configure and verify IOS IPS using the CLI interface
  - Cisco IOS IPS tasks you can complete with SDM
  - Select interfaces and configure SDF locations within the SDM IPS Policies wizard
  - View the IPS policy summary and deliver the IPS configuration to the router using the SDM IPS Policies wizard
  - Configure IPS policies and global settings using the SDM
  - View SDEE messages in the SDM
  - Tune signatures using the SDM

## 5. IPsec VPNs

- IPsec Components and IPsec VPN Features
  - IPsec protocol and basic functions; advantages of IPsec VPNs over other types of VPNs
  - IKE protocols
  - IKE functionality
  - Two protocols that are used for IPsec
  - Message authentication and integrity check
  - Differences and the functionality between symmetric and asymmetric encryption algorithms
  - PKI
- Site-to-Site IPsec VPN Operations
  - Five steps of IPsec operation
  - Configuration of IPsec
  - Configuration of the ISAKMP parameters
  - Configuration to define the IPsec transform set, the crypto ACL, and the crypto map
  - Configuration to apply the crypto map to the interface
  - Configuration of the interface ACL for IPsec
- Configuring IPsec Site-to-Site VPN Using SDM
  - Navigating the site-to-site VPN wizard interface
  - Components that will be configured by the SDM site-to-site VPN wizard
  - Launching the site-to-site VPN wizard
  - Set the parameters of the site-to-site VPN tunnel
  - How SDM sets IKE policies
  - Select a transform set and associate additional transform sets as required
  - Define the traffic that the VPN protects
  - Complete the configuration by viewing the settings in the Summary window
- Configuring GRE Tunnels over IPsec
  - GRE
  - Purpose of a secure GRE tunnel
  - Components that will be configured by the SDM site-to-site VPN secure GRE tunnel wizard
  - Configure a backup GRE-over-IPsec tunnel that the router can use when the primary tunnel fails
  - Select the authentication method to be used on the VPN
  - Configure IKE using the SDM wizard
  - Configure the IPsec transform set using the SDM wizard
  - Configure dynamic or static routing over the GRE and IPsec tunnel
  - Complete the configuration by viewing the settings in the Summary window

- High Availability Options
  - How high availability of IPsec VPNs is achieved
  - Failover option of backup IPsec peers
  - Use of HSRP for IOS IPsec VPN resiliency
  - IPsec stateful failover
  - How a WAN connection can be backed up by using an IPsec VPN
- Configuring Cisco Easy VPN and Easy VPN Server Using SDM
  - General operation of Cisco Easy VPN including its benefits and the role of each of its components
  - Functionality provided by Cisco Easy VPN Server, concept of dynamic crypto maps, and functionality provided by Easy VPN Remote
  - Steps required to configure Cisco Easy VPN Server using SDM
  - Configure IKE using the SDM wizard
  - Configure the IPsec transform set using the SDM wizard
  - Locations where Easy VPN group policies can be stored
  - Locations where user records for Xauth can be stored
  - Configure local group policies
  - Complete the configuration by viewing the settings in the Summary window
- Implementing the Cisco VPN Client
  - Steps required to configure the software VPN client on a PC
  - Steps required to configure Cisco VPN Client

## 6. Implement Frame-Mode MPLS

- Introducing MPLS Networks
  - Elements of the MPLS conceptual model
  - Router switching mechanisms
  - MPLS data and control planes
  - Structure of an MPLS label and its format
  - Function of different types of LSRs in MPLS networks
  - Interactions between the control plane and the data plane in an LSR that enable the basic functions of label switching and forwarding of labeled packets to occur
- Assigning MPLS Labels to Packets
  - Performing label allocation in a frame-mode MPLS network
  - Distributing labels in a frame-mode MPLS network
  - How the LFIB table is populated
  - Packet propagation across an MPLS network
  - How PHP improves MPLS performance by eliminating routing lookups on egress LSRs
- Implementing Frame-Mode MPLS
  - Configuring frame-mode MPLS on a Cisco IOS router
  - Enable IP CEF on a router as a step in implementing frame-mode MPLS
  - Enable MPLS on a frame-mode interface as a step in implementing frame-mode MPLS
  - Configure the MTU size in label switching as a step in implementing frame-mode MPLS

- MPLS VPN Technology
  - MPLS VPN architecture and how it improves on the traditional methods of overlay and peer-to-peer VPN
  - Components of an MPLS VPN and how they are interconnected to enable enterprise network connectivity between sites
  - How routing information is propagated across the P-network
  - End-to-end flow of routing updates in an MPLS VPN
  - MPLS VPN packet forwarding

d) ONT - Optimizing Converged Cisco Networks

### **1. Network Requirements**

### **2. Cisco VoIP Implementations**

- Introducing VoIP Networks
  - Benefits of VoIP when compared to traditional circuit-switched telephony
  - Components of a VoIP network
  - Analog connectivity options for legacy equipment to connect to a VoIP network
  - Digital interface options to connect VoIP equipment to PBXs or the PSTN
  - Three stages of a call
  - Compare the concept of distributed call control, where a voice gateway provides call control functions, to that of centralized call control, where the call control process is run by a call agent, such as Cisco Unified CallManager
- Digitizing and Packetizing Voice
  - Converting analog signals to digital signals
  - Converting digital signals to analog signals
  - Why voice is sampled at 8,000 bps for telephone calls
  - How a signal is quantized and combined with the Nyquist theorem to yield a standard voice channel bit rate of 64,000 bps
  - Common voice compression standards including bandwidth requirements and voice quality measurement
  - Purpose of a DSP in a voice gateway
- Encapsulating Voice Packets for Transport
  - Transporting digitized voice packets across a network in an RTP voice bearer stream
  - Role of RTP and UDP in encapsulating voice for transport across a network
  - How and when to reduce header overhead with cRTP
- Calculating Bandwidth Requirements
  - How the number of voice samples that are encapsulated impacts bandwidth requirements
  - Overhead for various Layer 2 protocols
  - How IPsec and GRE/LT2P tunneling affect bandwidth overhead
  - Calculating the total bandwidth required for a VoIP call
  - Operation of VAD and bandwidth savings associated with the use of VAD

- Implementing Voice Support in an Enterprise Network
  - Given an enterprise network topology diagram, identify the components that are necessary for VoIP support
  - Voice capabilities available on Cisco ISRs
  - **Exclusive:** Using ISRs as voice gateways in CallManager environments
  - Role of a call agent, such as Cisco Unified CallManager, in a VoIP implementation
  - **Exclusive:** Extended discussion of CallManager features
  - Main IP telephony deployment models that may be used in an enterprise
  - **Exclusive:** Scaling CallManager environments using intercluster trunks and gatekeepers
  - **Exclusive:** Overview of call control protocols: H.323, SIP, and MGCP
  - **Exclusive:** Dial Plan/Route Plan design in VoIP environments
  - Given a show running-config output from a Cisco router configured as a voice gateway, identify the sections of the configuration that are related to the voice implementation on the router
  - How CAC prevents calls from crossing overly busy links and how such calls can be rerouted by mechanisms, such as AAR, instead of simply being blocked

### 3. Introduction to IP QoS

- Introducing QoS
  - Four key quality issues with converged networks
  - How a lack of bandwidth can adversely impact a network and ways to effectively increase bandwidth on a link
  - How end-to-end delay can adversely impact a network and ways to effectively reduce delay
  - How packet loss can adversely impact a network and ways to manage packet loss
  - Defining QoS with respect to traffic in a network
  - Three key steps involved in implementing a QoS policy on a network
  - How traffic is recognized by type in a network and how those types resolve to QoS traffic classes
  - Defining QoS policies after traffic classes have been defined
- Identifying Models for Implementing QoS
  - Models for providing QoS on a network
  - Key features of the Best Effort model for QoS
  - Key features of the IntServ model for QoS
  - How RSVP enables the IntServ model to provide end-to-end QoS
  - Key features of the DiffServ model for QoS
  - Methods for Implementing QoS
  - Methods for configuring and monitoring QoS on a network
  - CLI (nonmodularized) method of configuring QoS
  - The Modular QoS CLI (MQC) method of configuring QoS
  - AutoQoS methods of configuring QoS
  - Cisco SDM QoS wizard, including how to access and use it to configure basic QoS functions
- Advantages

## 4. Implement the DiffServ QoS Model

- Introducing Classification and Marking
  - Purpose of packet classification
  - Purpose of packet marking
  - IP packet classification and marking at the data link layer
  - Purpose and function of the DiffServ model
  - Interoperability between DSCP-based and IP-precedence-based devices in a network
  - How DSCP values are determined and assigned to different per-hop behaviors (PHBs)
  - DSCP settings in the DiffServ Model
  - Data link to network layer interoperability between QoS markings
  - The term "QoS service class" and how service classes can be used to create a service policy throughout a network
  - How link layer and network layer markings are used to define QoS service classes and the different applications represented by each of these service classes
  - **Exclusive:** How switches preserve or modify Layer 2 and Layer 3 markings
  - Trust boundaries and how they are used with classification and marking
  - **Exclusive:** Queuing mechanisms on Cisco switches
- Using NBAR for Classification
  - Cisco IOS protocol discovery and classification mechanism known as NBAR
  - Types of applications supported by NBAR
  - Purpose of PDLMs in NBAR
  - NBAR protocol discovery
  - Cisco IOS commands required to configure and monitor NBAR protocol discovery
  - Cisco IOS commands required to configure NBAR to recognize static port protocols
  - Cisco IOS commands required to configure NBAR to recognize TCP and UDP stateful protocols
- Introducing Queuing Implementations
  - Need for congestion management mechanisms
  - Queuing algorithms
  - FIFO queuing algorithm
  - Priority queuing (PQ) algorithm
  - Round-robin queuing algorithm and its variants
  - Primary components of a queuing mechanism
- Configuring WFQ
  - Detailed explanation of WFQ
  - Architecture and benefits of WFQ
  - Cisco IOS commands required to configure and monitor WFQ on a Cisco router
- Configuring CBWFQ and LLQ
  - Advanced queuing mechanisms of CBWFQ and LLQ
  - Detailed explanation of CBWFQ
  - Architecture and benefits of CBWFQ
  - Cisco IOS commands required to configure and monitor CBWFQ on a Cisco router
  - Detailed explanation of LLQ
  - Architectures and benefits of LLQ
  - Cisco IOS commands required to configure and monitor LLQ on a Cisco router

- Introducing Congestion Avoidance
  - Default mechanism for managing interface congestion with tail drop
  - Limitations of using tail drop as a congestion management mechanism
  - RED and how it can be used to prevent congestion
  - WRED and how it can be used to prevent congestion
  - Traffic profiles that are used in WRED implementations
  - Cisco IOS software commands that are required to configure CB-WRED
  - Cisco IOS software commands that are used to monitor CB-WRED
- Introducing Traffic Policing and Shaping
  - Purpose of traffic conditioning using traffic policing and traffic shaping
  - Benefits of traffic conditioning using traffic policing and traffic shaping
  - Features of traffic policing and traffic shaping
  - How a token bucket can be used by network devices to measure traffic rates
  - How traffic can be policed using a single token bucket scheme
  - **Exclusive:** Dual token bucket mechanisms for single rate/bursting or dual rate policing
  - Key traffic policing and shaping mechanisms available in Cisco IOS software and how each compares to the others
  - Points in a network where rate-limiting can most effectively be employed
- WAN Link Efficiency Mechanisms
  - Various link efficiency mechanisms and their functions
  - Purpose of Layer 2 payload compression and how Layer 2 payload compression affects throughput and delay
  - Purpose of header compression and how header compression affects throughput and delay
  - How VoIP packets are susceptible to increased latency when large packets, such as FTP transfers, traverse slow WAN links
  - LFI operation and how LFI reduces the delay and jitter of VoIP packets
  - **Exclusive:** LFI features of PPP and Frame Relay encapsulations
  - Points in a network where link efficiency mechanisms can most effectively be employed
- Implementing QoS Pre-Classify
  - Purpose of VPNs
  - Purpose of pre-classification to support QoS in various VPN configurations
  - Situations where pre-classification is appropriate
  - VPN applications that support QoS pre-classification and situations where pre-classification is not appropriate
- Deploying End-to-End QoS
  - IP QoS SLA and SLA examples
  - Typical network requirements within each functional block which makes up an end-to-end network
  - Best practice QoS implementations and configurations within a campus LAN
  - Best practice QoS implementations and configurations on WAN CE and PE routers
  - Control Plane Policing (CoPP)

## 5. Implement AutoQoS

- Introducing AutoQoS
  - How AutoQoS is used to implement QoS policy
  - Prerequisites for using AutoQoS and how it is configured on a network using CLI
  - Verify that AutoQoS is functioning on a network
  - **Exclusive:** AutoQoS on switches
- Mitigating Common AutoQoS Problems
  - QoS technologies that are automatically implemented on the network using AutoQoS
  - Known problems with AutoQoS that users have had to contend with
  - Using the show commands, isolate areas in the running AutoQoS configuration where the known problems typically occur
  - Modify the QoS configuration created by AutoQoS

## 6. Implement Wireless Scalability

- WLAN QoS Implementation
  - Need for WLAN QoS
  - WLAN QoS
  - Current WLAN QoS Implementation
  - Configure QoS features on lightweight APs using WLC
- Introducing 802.1x
  - Need for WLAN security standards and why WLAN security is so important
  - Difference between authentication and encryption
  - How enhanced 802.11 security improves on basic 802.11 security
  - Basic concepts of 802.1x authentication
  - EAP Cisco Wireless
  - EAP-FAST
  - EAP-TLS
  - EAP-PEAP
  - WPA authentication process
  - **Exclusive:** Study guide for 802.1x authentication methods
- Configuring Encryption and Authentication on Lightweight Access Points
  - Configuring open authentication on the controller
  - Configuring pre-shared key authentication on the controller
  - Configuring web authentication on the controller
  - Configuring 802.1x on the controller

- WLAN Management
  - Compare wireless solutions using autonomous to wireless solutions using lightweight APs, identifying how the two solutions come together for a complete unified wireless network
  - How Cisco implements WLANs
  - Hierarchy of components that are required to build a WLAN
  - Basic features of WLSE for wireless feature set using autonomous APs and related products
  - Basic features of Cisco WCS for wireless feature set using lightweight APs and related products
  - Cisco WCS tracking options
  - Using monitor tab functions to manage the WLAN
  - Function of the 2700 Location Appliance
  - Basic Cisco WCS configuration
  - Add, change, and use maps in the Cisco WCS database
  - Cisco WCS rogue AP methodology

## III. CUCMBC

### CIPT1 Outline

#### 1. Cisco IP Telephony Introduction

- Objectives
- Prerequisites
- Information Sources

#### 2. Introduction to Cisco AVVID and Cisco Unified Communications Manager (CUCM)

- CUCM Servers
- CUCM Functions
- Layers of CUCM
- Operating System and Database
  - Supported Hardware
  - Device Weight Units
- Comparing Legacy and IP Telephony Technology

#### 3. Clustering CUCM

- Cluster Definition
- Intercluster Communication
- Cluster Options
- Deployment Methods

#### **4. Installing CUCM**

- Installation CDs
- Configuring Data
- Activating CCM Components
- Post-Installation Procedures
- Upgrading from Prior CUCM Versions

#### **5. Cisco IP Phones**

- Cisco IP Phone Overview
- Additional VoIP Devices
- Cisco IP Phone Codec Support

#### **6. Configuring CUCM to Support IP Phones**

- Server Configuration
- Phone Button Templates
- Configuring Auto-Registration
- Device Pools

#### **7. Cisco Catalyst® Switches**

- Catalyst Switch Models
- Powering the IP Phone
- Dual VLAN Configuration
- Configuring CoS and ToS

#### **8. Access Gateways**

- Analog vs. Digital
- Gateway Protocols
- Core Requirements
- Supplementary Services
- Call Survivability
- CUCMr Redundancy

#### **9. Route Plans**

- External Call Routing
- Route Pattern Wildcard
- Route Plan Configuration

## **10. Advanced Route Plans**

- Route Filters
- Discard Digits Instructions
- Transformation Masks
  - Translation Patterns
  - Route Groups
  - External Call Routing
  - Digit Analysis

## **11. Telephony Class of Service**

- Calling Search Spaces
- Partitions

## **12. Media Resources**

- Conference Bridge Resources
- Media Termination Point
- Music on Hold Server
- Media Resource Management

## **13. Call Admission Control and Survivable Remote Site Telephony**

- CAC
- SRST
- CUCM Gatekeeper Configuration

## **14. Features**

- Call Park
- IP Phone Services
- Call Pickup
- Music on Hold Resources
- Media Resource Management
- Transcoder Resources
- Softkey Templates
- Shared Line Appearance
- IP Phone Services

## **15. Users**

- Adding a User
- User Logon
- IP Phone Subscription

## **16. Bulk Administration Tool**

- Installation
- Templates
- Creating CSV Files

## CIPT2 Outline

### 1. Course Introduction

### 2. Applications

- CUCM Attendant Console
- Cisco IP SoftPhone
- Cisco Voice over IP Integrated Applications

### 3. Enabling Video Calling and Conferencing

- Cisco Video Telephony Solution Components
- Configuring CUCM for Video
- Configuring a Dial Plan for Video Telephony

### 4. Securing IP Communications

- Principles of IP Communications Security
- Authentication and Encryption Fundamentals
- Operating System and CUCM
- Secure Administration HTTPS
- MS Windows IPsec
- CUCM Hardening

### 5. Monitoring and Managing IP Communications

- Internal Server Tools
- Tools and Accounts
- Database Services
- Command-Line Tools
- Cisco CUCM Serviceability
- Real-Time Monitoring Tool
- Call Detail Records
- Directory Enhancements

## UCM50 Outline

### 1. Installing and Upgrading to CUCM 5.1

- CUCM 5.1 Cluster Architecture
- Installing CUCM Release 5.1
- Performing a Windows Upgrade to CUCM Release 5.1

### 2. Administering CUCM Release 5.1

- Administering the Cisco IPT Platform
- Performing General Administration
- Performing Serviceability Administration
- Backing Up and Restoring CUCM 5.1

### **3. Implementing New and Changed CUCM 5.1 Features**

- Configuring Presence
- Configuring SIP Endpoints and Identifying New SIP Trunk Features
- Implementing RSVP Call Admission Control in CUCM 5.1
- Implementing New and Changed Security Features

## **IV. CVOICE v5.0/QOS**

### **CVOICE v5.0 Outline**

#### **1. Introduction to Packet Voice Technologies**

- Traditional telephony networks
- Packet voice networks
- IP data networks

#### **2. Analog and Digital Voice Connections**

- Basics of analog and digital voice
- Processes and standards of voice digitization, compression, and digital signaling
  - Signaling methods
  - ISDN voice interfaces
  - Signaling between PBXs
  - Common Channel Signaling (CCS) systems
  - Internetworking of signaling systems
- Fax and modem usage over a VoIP network

#### **3. Configuring Voice Interfaces**

- Analog and digital voice interfaces
- Analog and digital voice ports for optimal voice quality

#### **4. Voice Dial Peers**

- Call flows
- Inbound and outbound dial peers
- Application of voice dial peers
- Special purpose connections

## 5. Introduction to Voice over IP

- Fundamentals of VoIP
- Differences and similarities between VoIP and Voice over other technologies, such as Frame Relay or ATM
- Roles of Gateways in integrating VoIP with the traditional voice technologies found in enterprise and service provider networks
  - VoIP protocol stack
  - Applied headers
  - Use of Real-Time Transport Protocol compressed (cRTP)
  - Bandwidth requirements for various codecs and data links
  - Methods to reduce bandwidth consumption
  - Implications of implementing security measures in VoIP networks

## 6. Voice over IP Signaling and Call Control

- Types of various signaling
- Call control models
- Call control services
- Functional components of H.323
- Functional components of SIP
- Functional components of MGCP
- H.323, SIP, and MGCP call control models

## 7. Improving and Maintaining Voice Quality

- Voice Quality Measurement including codec choice, which affects quality
- Transporting real-time voice in a non-real-time IP internetwork
- Quality of Service (QoS) functional areas and tools
  - Campus networks
  - WAN
- Effect of network design on QoS
- Overcoming jitter
- Overcoming delay
- Call Admission Control tools
- Resource Reservation Protocol (RSVP)
- Busy-hour bandwidth allocation for both voice and data traffic

## 8. Scalable Numbering and Applications

- Implementing a scalable numbering plan
- Cost-saving applications

## QoS Outline

### 1. Introduction to IP QoS

- The Need for QoS
- Understanding QoS
- Implementing QoS

## **2. The Building Blocks of IP QoS**

- Models for Implementing QoS
- The Differentiated Services Module
- IP QoS Mechanisms
- Case Study: QoS Mechanisms
- Case Study: The Life of a Packet

## **3. Introduction to Modular QoS CLI and AutoQoS**

- Introducing Modular QoS CLI
- Introducing AutoQoS

## **4. Classification and Marking**

- Classification and Marking Overview
- Case Study: Classification and Marking
- Using MQC for Classification
- Using MQC for Class-Based Marking
- Using NBAR for Classification
- Configuring QoS Pre-Classify
- Configuring QoS Policy Propagation Through BGP
- Configuring LAN Classification and Marking

## **5. Congestion Management**

- Introduction to Queuing
- Queuing Implementations
- FIFO and WFQ
- CBWFQ and LLQ
- LAN Congestion Management

## **6. Congestion Avoidance**

- Introduction to Congestion Avoidance
- Introduction to RED
- Configuring Class-Based Weighted RED
- Case Study: WRED Traffic Profiles
- Configuring Explicit Congestion Notification

## **7. Traffic Policing and Shaping**

- Traffic Policing and Shaping Overview
- Configuring Class-Based Policing
- Configuring Class-Based Shaping
- Configuring Class-Based Shaping on Frame Relay Interfaces

## **8. Link Efficiency Mechanisms**

- Link Efficiency Mechanisms Overview
- Class-Based Header Compression
- Link Fragmentation and Interleaving

## **9. QoS Best Practices**

- Traffic Classification Best Practices
- Case Study: Deploying End-to-End QoS

# Cisco Expert-Level Training

## I. CCIE Routing and Switching Mock Lab.

### 1. LAN Switching - 3550 and 3560

- Trunking, VLANs, channeling, security, QoS, and numerous scenarios on spanning tree, including MSTP

### 2. Frame Relay

- Multiple topologies to add complexity to routing & forwarding paths

### 3. Interior Gateway Routing Protocols

- RIP IPv4
- EIGRP IPv4
- OSPFv2 for IPv4 with complex peering requirements

### 4. Complex redistribution scenarios intended to cause issues that have to be resolved

### 5. BGP

- iBGP
- eBGP
- Route Reflectors
- Confederations
- Policy routing

### 6. IPv6 - Addressing, tunneling, OSPFv3, RIPv6, and BGP

- Including GRE, IPv6IP and 6to4 tunnels

### 7. IPv4 multicast routing

- PIM running in Sparse, Dense, Sparse-Dense, SSM, or Bi-directional mode
- IGMP v2 and v3
- MSDP

### 8. QoS

- Legacy QoS and queuing features
- Modular QoS Command Interface with shaping, policing, and CBWQ
- Switching QoS for 3550 and 3560

## 9. Security

- Switch port security
- Routing protocol security features
- Access lists
- DOS mitigation
- Access control

## 10. System Management

- SNMP
- RMON

# II. CCIE Routing and Switching Preparation.

## 1. Bridging and Switching

- Switching as Covered by CCIE Lab Blueprint
- Switching IOS Features
- Trunks, VLANs, VTP
- Cluster Commander, VACL, 802.1q
- Tunneling

## 2. WAN

- Frame Relay
- Point-to-Point Subinterfaces
- Multipoint Subinterfaces

## 3. RIP V2

- Distribute Lists, Route Filtering, Route Manipulation, Distance

## 4. EIGRP

- Timers
- Bandwidth Consumption
- Advanced Commands EIGRP

## 5. OSPF

- OSPF via Frame Relay
- Authentication
- Virtual Links
- Costs, Metrics of External Routes
- Tuning CPU Load

## 6. IGP Features

- Complex and Unusual Configurations
- Complex Redistribution Techniques
- Route Tagging
- Routing Loop Avoidance
- Route Filtering

## 7. BGP

- Large-Scale BGP Deployment
- Route Reflectors
- Confederations
- Route Maps
- AS-Path Lists
- Prefix Lists
- Route Manipulation with AS-Path Prepending, Local Preference, MED, etc.
- Route Flap Dampening
- Communities

## 8. IOS Features

- Advanced and Unusual IOS Commands
- Tunnels
- Policy-Based Routing

# III. CCIE Security.

### Day 1:

- Strategy
- Routing Protocols Overview
- NAT
- ACLs
- AAA
- MQC

### Day 2:

- IPSec/GRE tunnels
- CBAC
- Identity Management
- PIX/ASA
- MPF
- Contexts
- Transparent FW

**Day 3:**

- ACS Server
- IPS Sensor
- VPN 3000
- Network Attacks

**Day 4:**

- Mock lab exam

**Day 5:**

- Mock lab exam

## IV. CCIE Service Provider.

**Day 1:**

- Layer 2 Technologies
  - Serial
  - Frame
  - Ethernet
  - ATM
  - Switching
- Management Protocols

**Day 2:**

- Layer 3 Technologies
  - IGP Routing
  - BGP Routing
  - Policy

**Day 3:**

- Multicast
- MPLS
- Traffic Engineering
- QoS

**Day 4:**

- MPLS VPNs (Layer 2 and Layer 3)
- Multicast VPNs
- Multipoint GRE

**Day 5:**

- Separate 8-hour lab

## V. CCIE Voice.

### Day 1:

- Intro
- Infrastructure
- CallManager Basics
- CallManager Express Basics
- Gateway
- GateKeeper/Proxy
- SBC

### Day 2:

- Voice Security
- Dial Plan
- Media Resources
- AAR
- SRST
- COR
- Unity

### Day 3:

- Unity Express
- Applications and Features
- IPCC Express
- QoS

### Day 4:

- ATA
- VG248
- Fax
- Miscellaneous

### Day 5:

- Mock Lab Exam.