# CCNP1 : BSI : Building Scalable Internetworks v5.0

## Module 1: Scalable Network Design

1.1 IIN, SONA, and the ECNM
1.1.1 Technological Revolution Cycles
1.1.2 The Network as the Platform
1.1.3 The Intelligent Information Network (IIN)
1.1.4 The SONA Framework
1.1.5 Cisco Enterprise Architectures
1.1.6 The Hierarchical Network Model
1.1.7 The Enterprise Composite Network Model
1.2 Scalable Networks
1.2.1 Scalable Network Design
1.2.2 Five Characteristics of a Scalable Network
1.2.3 Making the Network Reliable and Available
1.2.4 Making the Network Responsive
1.2.5 Making the Network Efficient
1.2.6 Making the Network Adaptable
1.2.7 Making the Network Accessible But Secure
1.3 Converged Networks
1.3.1 Traffic Conditions in a Converged Network
1.3.2 Routing and Routing Protocols
1.4 ITA Topology
1.4.1 Overview of the International Travel Agency
1.4.2 The ITA Logical Topology
1.5 Overview of Course Labs
1.5.1 Lab 1-0 TCL Script Reference and Demonstration

## Module 2: EIGRP

2.1 EIGRP Fundamentals and Features
2.1.1 EIGRP Capabilities and Attributes
2.1.2 Underlying Process and Technologies
2.1.3 Protocol-dependent Modules
2.1.4 Reliable Transport Protocol
2.1.5 EIGRP Neighbor Discovery and Recovery
2.1.6 DUAL Finite-State Machine
2.1.7 DUAL Example
2.2 EIGRP Components and Operation
2.2.1 EIGRP Tables
2.2.2 EIGRP Neighbor Table
2.2.3 EIGRP Topology Table
2.2.4 EIGRP Routing Table
2.2.5 EIGRP Packet Formats
2.2.6 EIGRP Packet Exchange Example
2.2.7 EIGRP Metric
2.2.8 EIGRP Metric Calculation
2.2.9 EIGRP Metric Calculation Example
2.3 Implementing and Verifying EIGRP
2.3.1 Configuring Basic EIGRP
2.3.2 Configuring Basic EIGRP Example
2.3.3 Configure Basic Propagation of Default Route
2.3.4 Verifying EIGRP Example
2.3.5 The show ip eigrp neighbors Command
2.3.6 The show ip route eigrp Command
2.3.7 The show ip protocols Command
2.3.8 The show ip eigrp interfaces Command
2.3.9 The show ip eigrp topology Command
2.3.10 The show ip eigrp traffic Command
2.4 Implementing Advanced EIGRP Features
2.4.1 Route Summarization
2.4.2 Configuring Manual Route Summarization
2.4.3 Configuring Manual Route Summarization Example
2.4.4 Load Balancing Across Equal Cost Paths
2.4.5 Load Balancing Across Unequal Cost Paths

2.4.6 Load Balancing Across Unequal Cost Paths Example
2.4.7 EIGRP Bandwidth Use Across WAN Links
2.4.8 Bandwidth Utilization over WAN Interfaces
2.4.9 Configuring EIGRP in a Frame Relay Hub-and-Spoke Topology
2.4.10 Configuring EIGRP in a Hybrid Multipoint Topology
2.5 Configuring EIGRP Authentication
2.5.1 EIGRP Router Authentication
2.5.2 MD5 Authentication
2.5.3 Configuring MD5 Authentication
2.5.4 MD5 Authentication Example
2.5.5 Verifying MD5 Authentication
2.5.6 Troubleshooting MD5 Authentication
2.6 Using EIGRP in the Enterprise
2.6.1 EIGRP Scalability in a Large Network
2.6.2 EIGRP Queries
2.6.3 SIA Connections
2.6.4 EIGRP Stubs
2.6.5 EIGRP Stubs
2.6.6 Configuring EIGRP Stubs
2.6.7 Configuring EIGRP Stubs Example
2.6.8 Preventing SIA Connections
2.6.9 Graceful Shutdown
2.7 EIGRP Lab Exercises
2.7.1 Lab 2-1 EIGRP Configuration, Bandwidth, and Adjacencies
2.7.2 Lab 2-2 EIGRP Load Balancing
2.7.3 Lab 2-3 Summarization and Default Network Advertisement
2.7.4 Lab 2-4 EIGRP Frame Relay Hub and Spoke
2.7.5 Lab 2-5 EIGRP Authentication and Timers

## Module 3: OSPF

3.1 Review of OSPF Fundamentals and Features
3.1.1 Link-State Routing Protocols
3.1.2 Overview of OSPF Operations
3.1.3 OSPF Data Structures
3.1.4 OSPF Adjacency Database
3.1.5 OSPF Area Structure
3.1.6 OSPF Router Types
3.1.7 OSPF Terminology
3.1.8 Calculation the OSPF Metric
3.1.9 Link-State Data Structure
3.2 Review of OSPF Operation
3.2.1 OSPF Packet Types
3.2.2 OSPF Packet Header Format
3.2.3 Establishing OSPF Neighbor Adjacencies
3.2.4 Exchanging and Synchronizing LSDBs
3.2.5 Discovering the Network Routes
3.2.6 Maintaining Network Routes
3.2.7 Maintaining Link-State Sequence Numbers
3.2.8 Verifying Packet Flow
3.3 Implementing and Verifying OSPF
3.3.1 Configuring Basic Single-Area and Multiarea OSPF
3.3.2 Configuring Basic Single-Area OSPF Example
3.3.3 Configuring Basic Multiarea OSPF Example
3.3.4 Configuring a Router ID
3.3.5 Verifying the OSPF Router ID
3.3.6 Verifying the OSPF Operation
3.3.7 Example of the show ip route ospf Command
3.3.8 Example of the show ip ospf interface Command
3.3.9 Example of the show ip ospf neighbor Command
3.3.10 clear and debug Commands
3.4 OSPF Network Types
3.4.1 OSPF Network Types
3.4.2 Adjacency Behavior for a Point-to-Point Link
3.4.3 Adjacency Behavior for a Broadcast Link

3.4.4 Selecting the DR and BDR
3.4.5 Adjacency Behavior for a NBMA Network
3.4.6 DR Election in NBMA Topology
3.4.7 OSPF Over Frame Relay
3.4.8 OSPF over NBMA Topology Modes
3.5 Implementing OSPF in an NBMA Network
3.5.1 Configuring the OSPF Network Type
3.5.2 Configuring OSPF over Frame Relay
3.5.3 Using the neighbor Command
3.5.4 The show ip ospf neighbor Command
3.5.5 Point-to-Multipoint Configuration
3.5.6 Point-to-Multipoint Nonbroadcast Configuration
3.5.7 Using Subinterfaces in OSPF over a Frame Relay Configuration
3.5.8 Configuring a Point-to-Point Subinterface
3.5.9 Configuring a Multipoint Subinterface
3.5.10 OSPF over NBMA Topology Summary
3.5.11 Tracking OSPF Adjacencies
3.6 Multiarea OSPF Operation
3.6.1 Large OSPF Network Issues
3.6.2 OSPF LSA Types
3.6.3 OSPF LSA Types (cont.)
3.6.4 Interpreting the OSPF LSDB and Routing Table
3.6.5 Interpreting the Routing Table
3.6.6 Calculating Costs for E1 and E2 Routes
3.6.7 Configuring OSPF LSDB Overload Protection
3.6.8 Changing the Cost Metric
3.7 Stub, Totally Stubby, and Not-So-Stubby Areas
3.7.1 Configuring OSPF Area Types
3.7.2 Using Stub and Totally Stubby Areas
3.7.3 Configuring Stub Area
3.7.4 OSPF Stub Area Configuration Example
3.7.5 Configuring Totally Stub Areas
3.7.6 Totally Stubby Area Configuration Example
3.7.7 Interpreting Routing Tables
3.7.8 Configuring Not-So-Stubby Areas
3.7.9 Configuring Not-So-Stubby Area Example
3.7.10 Configuring an NSSA Totally Stubby Area Example
3.7.11 Verifying All Stub Area Types
3.8 Virtual Links
3.8.1 OSPF Virtual Links
3.8.2 Configuring Virtual Links
3.8.3 Virtual Link Configuration Example
3.8.4 Verifying a Virtual Link Configuration
3.9 Route Summarization
3.9.1 ABR and ASBR Implementation
3.9.2 OSPF Route Summarization Example
3.9.3 Configuring OSPF Route Summarization
3.9.4 Configuring Route Summarization at ABR
3.9.5 Configuring Route Summarization at ASBR
3.9.6 Benefits of a Default Route in OSPF
3.9.7 Configuring a Default Route in OSPF
3.9.8 Example of Configuring a Default Route in OSPF
3.10 OSPF Authentication
3.10.1 OSPF Authentication Methods
3.10.2 Configuring Simple Password Authentication
3.10.3 Example of Configuring Simple Password Authentication
3.10.4 Configuring MD5 Authentication
3.10.5 Example of Configuring MD5 Authentication
3.10.6 Troubleshooting Simple Password Authentication
3.10.7 Troubleshooting MD5 Authentication
3.11 OSPF Lab Exercises
3.11.1 Lab 3-1 Single-Area OSPF Link Costs and Interface Priorities
3.11.2 Lab 3-2 Multiple-Area OSPF with Stub Areas and Authentication

3.11.3 Lab 3-3 OSPF Virtual Links and Area Summarization
3.11.4 Lab 3-4 OSPF over Frame Relay

## Module 4: Integrated IS-IS

4.1 IS-IS Fundamentals
4.1.1 Uses for IS-IS Routing
4.1.2 IS-IS and OSPF
4.1.3 IS-IS Routing
4.1.4 IS-IS Features
4.1.5 IS-IS Link-State Operation
4.1.6 Integrated IS-IS
4.1.7 Principles and Issues of IS-IS Design
4.1.8 The ES-IS Protocol
4.1.9 OSI Routing Levels
4.1.10 IS-IS and OSPF Network Design
4.1.11 Differences Between Integrated IS-IS and OSPF
4.2 ISO Addressing
4.2.1 NSAP Addresses
4.2.2 NSAP Address Structure
4.2.3 NSAP Address Example
4.2.4 Identifying Systems in IS-IS
4.2.5 NET Addresses
4.2.6 Subnetwork Point of Attachment, Circuits, and Links
4.2.7 IS-IS Routing Levels
4.2.8 Intra-Area and Interarea Addressing and Routing Logic
4.2.9 OSI Addressing in Networks Example
4.2.10 Route Leaking
4.3 IS-IS Operation
4.3.1 IS-IS Protocol Data Units
4.3.2 Link-State Packets
4.3.3 LSP Headers
4.3.4 Implementing IS-IS in NBMA Networks
4.3.5 Implementing IS-IS in Broadcast Networks
4.3.6 LSP and IIH Levels
4.3.7 Comparing Broadcast and Point-to-Point Topologies
4.3.8 Link-State Database Synchronization
4.3.9 LSDB Synchronization
4.3.10 LAN LSDB Synchronization Example
4.3.11 Point-to-Point LSDB Synchronization Example
4.3.12 LAN Adjacencies
4.3.13 WAN Adjacencies
4.4 Configuring Basic Integrated IS-IS
4.4.1 Integrated IS-IS in an CLNS Environment
4.4.2 Building a Routing Table
4.4.3 Steps to Configuring Integrated IS-IS
4.4.4 Step 1: Define Area and Addressing
4.4.5 Step 2: Enable IS-IS on the Router
4.4.6 Step 3: Configure the NET
4.4.7 Step 4: Enable Integrated IS-IS on the Proper Interface
4.4.8 Simple Integrated IS-IS Example
4.5 Optimizing IS-IS
4.5.1 Changing the IS-IS Router Type
4.5.2 Changing the IS-IS Interface Level
4.5.3 Changing the IS-IS Metric
4.5.4 Tuning IS-IS Configuration Example
4.5.5 Configuring Route Summarization in IS-IS
4.6 Verifying and Troubleshooting IS-IS
4.6.1 IS-IS Lab
4.6.2 Verifying CLSN IS-IS Structures
4.6.3 Troubleshooting Integrated IS-IS Configurations
4.6.4 Troubleshooting Integrated IS-IS Configuration Example
4.7 IS-IS Lab Exercises
4.7.1 Lab 4-1 Configuring Basic Integrated IS-IS
4.7.2 Lab 4-2 Multi-Area Integrated IS-IS

4.7.3 Lab 4-3 Configuring IS-IS over Frame Relay

## Module 5: Route Optimization

5.1 Operating a Network Using Multiple Routing Protocols
5.1.1 Using Multiple Routing Protocols
5.1.2 Defining Route Redistribution
5.1.3 Redistributing Route Information
5.1.4 Using Seed Metrics
5.1.5 Seed Metrics Example
5.1.6 Defining Administrative Distance
5.1.7 Modifying Administrative Distances
5.2 Configuring and Verifying Router Redistribution
5.2.1 Configuring Redistribution
5.2.2 Redistributing Routes into a Classful Routing Protocol
5.2.3 Redistributing from Classless to Classful Protocols
5.2.4 Redistributing Routes into a Classless Routing Protocol
5.2.5 Redistributing Routes into OSPF Example
5.2.6 Redistributing Routes into EIGRP
5.2.7 Redistributing Routes into EIGRP Example
5.2.8 Redistributing Routes into IS-IS
5.2.9 Redistributing Routes into IS-IS Example
5.2.10 Redistributing Static and Connected Routes
5.2.11 Verifying Route Redistribution
5.2.12 Verifying Route Redistribution Example
5.2.13 Administrative Distance Problems with Redistribution
5.2.14 Administrative Distance Solution with Redistribution
5.3 Controlling Routing Update Traffic
5.3.1 Controlling Routing Updates
5.3.2 Passive Interfaces
5.3.3 Passive Interface Considerations
5.3.4 Configuring Route Filtering Using Distribute Lists
5.3.5 Implementing the Distribute List
5.3.6 Filtering Routing Updates with a Distribute List
5.3.7 Controlling Redistribution with Distribute Lists
5.4 Policy-based Routing
5.4.1 Defining Route Maps
5.4.2 Route Map Applications
5.4.3 Route Map Operation
5.4.4 Using Route Map Commands
5.4.5 The match Command
5.4.6 The set Command
5.4.7 Implementing Route Maps with Redistribution
5.5 DHCP
5.5.1 The Purpose of DHCP
5.5.2 Understanding the Function of DHCP
5.5.3 Configuring DHCP
5.5.4 DHCP Importing and Autoconfiguration
5.5.5 Configuring the DHCP Client
5.5.6 The IP Helper Address
5.5.7 Configuring the IP Helper Address
5.5.8 Customizing the Forwarded UDP Services
5.5.9 Configuring DHCP Relay Services
5.5.10 Verifying DHCP Relay Services
5.6 Route Optimization Lab Exercises
5.6.1 Lab 5-1 Redistribution Between RIP and OSPF
5.6.2 Lab 5-2 Redistribution Between EIGRP and OSPF
5.6.3 Lab 5-3 Redistribution Between EIGRP and IS-IS
5.6.4 Lab 5-4 Manipulating Administrative Distances
5.6.5 Lab 5-5 Configuring the Cisco IOS DHCP Server

## Module 6: BGP

6.1 BGP Concepts and Terminology
6.1.1 Using BGP in the Enterprise Network
6.1.2 BGP Multihoming Options

6.1.3 Option 1: Default Routes from All Providers
6.1.4 Option 2: Default Routes and Partial Updates
6.1.5 Option 3: Full Routes from All Providers
6.1.6 BGP Routing Between Autonomous Systems
6.1.7 Path-Vector Functionality
6.1.8 BGP Routing Policies
6.1.9 Features of BGP
6.1.10 BGP Databases
6.1.11 BGP Message Types
6.2 EBGP and IBGP
6.2.1 BGP Neighbor Relationships
6.2.2 Establishing a Connection Between External BGP Neighbors
6.2.3 Establishing a Connection Between Internal BGP Neighbors
6.2.4 Synchronization Within an Autonomous System
6.2.5 IBGP in a Nontransit Autonomous System
6.2.6 Routing Issues in a Transit Autonomous System
6.3 Configuring BGP
6.3.1 Basic BGP Configuration
6.3.2 Activate a BGP Session
6.3.3 Shutting Down a BGP Neighbor
6.3.4 BGP Configuration Considerations
6.3.5 IBGP Peering Issue
6.3.6 BGP neighbor update-source Command
6.3.7 EBGP Peering Issue
6.3.8 Next Hop Behavior
6.3.9 BGP neighbor next-hop-self Command
6.3.10 Injection Routing Information into BGP
6.3.11 BGP network Command Example
6.3.12 BGP Synchronization
6.3.13 BGP Synchronization Example
6.3.14 BGP Configuration Example
6.4 Advanced BGP Configuration and Verification
6.4.1 BGP Neighbor States
6.4.2 BGP Established and Idle States
6.4.3 BGP Active State Troubleshooting
6.4.4 Configuring a Peer Group
6.4.5 Configuring a Peer Group Example
6.4.6 BGP Peering
6.4.7 Configuring BGP Authentication
6.4.8 Troubleshooting BGP
6.4.9 Clearing the BGP Session
6.4.10 Hard Reset of BGP Sessions
6.4.11 Soft Reset of BGP Sessions
6.4.12 The debug ip bgp Command
6.5 Selecting a BGP Path
6.5.1 Characteristics of BGP Attributes
6.5.2 BGP Attributes
6.5.3 AS Path Attribute
6.5.4 Next-Hop Attribute
6.5.5 Origin Attribute
6.5.6 Local Preference Attribute
6.5.7 MED Attribute
6.5.8 Weight Attribute
6.5.9 Determining the BGP Path Selection
6.5.10 Selecting a BGP Path
6.5.11 Path Selection with Multihomed Connection
6.6 Manipulating BGP Path Selection with Route Maps
6.6.1 Setting Local Preference with Route Maps
6.6.2 Setting Local Preference with Route Maps Example
6.6.3 Changing the BGP Local Preference for All Routes
6.6.4 BGP Local Preference Example
6.6.5 BGP Local Preference Example (continued)
6.6.6 BGP Local Preference Example (continued)

6.6.7 Setting the MED with Route Maps
6.6.8 BGP Using Route Maps and the MED Example
6.6.9 BGP Using Route Maps and the MED Example (continued)
6.6.10 BGP Using Route Maps and the MED Example (continued)
6.6.11 Implementing BGP in the Enterprise
6.7 BGP Lab Exercises
6.7.1 Lab 6-1 Configuring BGP with Default Routing
6.7.2 Lab 6-2 Using the AS_PATH Attribute
6.7.3 Lab 6-3 Configuring IBGP and EBGP Sessions, Local Preference and MED
6.7.4 Lab 6-4 BGP Route Reflectors and Route Filters

## Module 7: IP Multicasting

7.1 Explaining Multicast
7.1.1 Explaining the Multicast Group Concept
7.1.2 Unicast versus Multicast
7.1.3 Multicast Advantages and Disadvantages
7.1.4 Multicast Applications
7.1.5 IP Multicast Addresses
7.1.6 Layer 2 Multicast Addressing
7.1.7 Multicast Sessions
7.2 IGMP and Layer 2 Issues
7.2.1 Introducing IGMPv2
7.2.2 IGMPv2 Join Group and Leave Group Messages
7.2.3 Introducing IGMPv3
7.2.4 IGMPv2 and IGMPv3 Interoperability
7.2.5 Multicast in the Layer 2 Switching Environment
7.2.6 Multicast in Layer 2 Solutions
7.2.7 Cisco Group Management Protocol (CGMP)
7.2.8 IGMP Snooping
7.3 Multicast Routing Protocols
7.3.1 Protocols Used in Multicast
7.3.2 Multicast Distribution Trees
7.3.3 Multicast Distribution Trees Identification
7.3.4 IP Multicast Routing
7.3.5 Protocol-Independent Multicast: Describing PIM-DM
7.3.6 Protocol-Independent Multicast: Describing PIM-SM
7.3.7 PIM Sparse-Dense-Mode
7.4 Multicast Configuration and Verification
7.4.1 Enabling PIM Sparse Mode and Sparse-Dense Mode
7.4.2 Inspecting the Multicast Routing Table
7.4.3 Finding PIM Neighbors
7.4.4 Checking RP Information
7.4.5 Checking the Group State
7.4.6 Configuring a Router to Be a Member of a Group
7.4.7 Configure a Router as a Statically Connected Member
7.4.8 Verifying IGMP Snooping
7.5 Multicast Lab Exercises
7.5.1 Lab 7-1 Implementing IGMP and IGMP Snooping
7.5.2 Lab 7-2 Routing IP Multicast with PIM Dense Mode
7.5.3 Lab 7-3 Routing IP Multicast with PIM Sparse Mode
7.5.4 Lab 7-4 Routing IP Multicast with PIM Sparse-Dense Mode

## Module 8: IPv6

8.1 Explaining IPv6
8.1.1 Introducing IPv6
8.1.2 IPv6 Features
8.1.3 Large Address Space
8.2 IPv6 Addressing
8.2.1 IPv6 Addressing Architecture
8.2.2 Comparing IPv4 and IPv6 Headers
8.2.3 IPv6 Extension Headers
8.2.4 Defining Address Representation
8.2.5 IPv6 Address Types
8.2.6 IPv6 Global Unicast and Anycast Addresses

8.3 Dynamic IPv6 Addresses
8.3.1 Defining Host Interface Addresses
8.3.2 Link Local Address
8.3.3 Stateless Autoconfiguration
8.3.4 EUI-64 to IPv6 Identifier
8.3.5 IPv6 over Data Link Layers
8.3.6 IPv6 Multicasting
8.3.7 Permanent Multicast Addresses
8.3.8 Addresses That Are Not Unique
8.3.9 Anycast
8.3.10 IPv6 Mobility
8.4 IPv6 Routing
8.4.1 Describing IPv6 Routing
8.4.2 OSPFv3 and IPv6
8.4.3 Similarities Between OSPFv2 and OSPFv3
8.4.4 Differences Between OSPFv2 and OSPFv3
8.4.5 LSA Types for IPv6
8.4.6 Address Prefix and LSAs
8.5 Implementing and Verifying OSPFv3
8.5.1 Configuring OSPFv3 in IPv6
8.5.2 Enabling OSPFv3 on an Interface
8.5.3 Configuring OSPFv3 Routing Specifics
8.5.4 OSPFv3 Route Summarization
8.5.5 OSPFv3 Configuration Example
8.5.6 Verifying OSPFv3
8.5.7 Verifying OSPFv3 Neighbors
8.5.8 Verifying OSPFv3 Database
8.6 Using IPv6 and IPv4
8.6.1 IPv6 to IPv4 Transition Mechanism
8.6.2 Cisco IOS Dual Stack
8.6.3 Overlay Tunnels
8.6.4 Isolated Dual-Stack Host
8.6.5 Configuring Tunneling
8.6.6 Example of a Configured Tunnel
8.6.7 IPv6 to IPv4 Tunneling and Addresses
8.6.8 Translation of NAT-PT
8.7 IPv6 Lab Exercises
8.7.1 Lab 8-1 Configuring OSPF for IPv6
8.7.2 Lab 8-2 Using Manual IPv6 Tunnels
8.7.3 Lab 8-3 Configuring 6to4 Tunnels

## CCNP2 : ISCWN : Implementing Secure Converged Wide-area Networks v5.0

### Module 1: Remote Network Connectivity Requirements

1.1 Enterprise Networking
1.1.1 Hierarchical Network Model
1.1.2 Cisco Enterprise Architecture
1.1.3 Remote Connection Requirements in a Converged Network
1.1.4 Remote Connection Considerations
1.1.5 Intelligent Information Network
1.1.6 Cisco SONA Framework

### Module 2: Teleworker Connectivity

2.1 Describing Remote Connection Topologies for Teleworkers
2.1.1 Remote Connection Topologies for the Teleworker
2.1.2 The Teleworker Solution
2.1.3 Options for Connecting the Teleworker
2.1.4 Components of the Teleworker Solution
2.1.5 Traditional Versus Business-Ready Teleworker Requirements
2.2 Describing Cable Technology
2.2.1 What is a Cable System?
2.2.2 Cable Technology Terms
2.2.3 Cable System Components

2.2.4 Cable System Benefits
2.2.5 Sending Digital Signals over Radio Waves
2.2.6 The Data-over-Cable Service Interface Specification: DOCSIS
2.3 Deploying Cable System Technology
2.3.1 Hybrid Fiber-Coaxial (HFC) Cable Networks
2.3.2 Sending Data over Cable
2.3.3 Cable Technology: Putting It All Together
2.3.4 Data Cable Network Technology Issues
2.3.5 Provisioning a Cable Modem
2.4 Describing DSL Technology
2.4.1 What is DSL
2.4.2 How Does DSL Work?
2.4.3 DSL Variants
2.4.4 Factors Affecting DSL Performance
2.4.5 DSL Distance Limitations
2.5 Deploying ADSL
2.5.1 ADSL
2.5.2 ADSL and POTS Coexistence
2.5.3 ADSL Channel Separation
2.5.4 Data over ADSL
2.5.5 PPPoE
2.5.6 DSL and PPPoE Deployment Options
2.5.7 PPPoE Session Establishment
2.5.8 Data over ADSL: PPPoA
2.6 Configuring the CPE as the PPPoE or PPPoA Client
2.6.1 Configuring the CPE as the PPPoE Client
2.6.2 Configuring the CPE as the PPPoE Client over the ATM Interface
2.6.3 Configuring a PPPoE Client
2.6.4 Configuring the PPPoE DSL Dialer Interface
2.6.5 Adjusting MSS and MTU Size
2.6.6 Configuring PAT
2.6.7 Configuring DHCP to Scale DSL
2.6.8 Configuring a Static Default Route
2.6.9 Verifying a PPPoE Configuration
2.6.10 Configuring a PPPoA DSL Connection
2.6.11 Configuring a DSL ATM Interface
2.7 Troubleshooting Broadband ADSL Configurations
2.7.1 Troubleshooting Layers 1, 2, and 3
2.7.2 Determine Whether the Router Is Properly Trained to the DSLAM
2.7.3 Troubleshooting Layer 1 Issues
2.7.4 Determining the Correct DSL Operating Mode
2.7.5 Troubleshooting Layer 2 Issues
2.7.6 Layer 2: Is Data Being Received from the ISP?
2.7.7 Proper PPP Negotiation
2.8 PPPoE Simulation Practice
2.8.1 PPPoE Simulation Practice

## Module 3: IPsec VPNs

3.1 Introducing VPN Technology
3.1.1 What Is Needed to Build a VPN?
3.1.2 Overlay and Peer-to-Peer VPN Architecture
3.1.3 VPN Topologies
3.1.4 Characteristics of a Secure VPNs
3.1.5 VPN Security: Encapsulation
3.1.6 VPN Security: IPsec and GRE
3.1.7 VPN Security: Symmetric and Asymmetric Encryption Algorithms
3.1.8 Symmetric Encryption Algorithms
3.1.9 Asymetric Encryption
3.1.10 Diffie-Hellman Key Exchange
3.1.11 Data Integrity
3.1.12 VPN Security: Authentication
3.2 Understanding IPsec Components and IPsec VPN Features
3.2.1 IPsec Security Features
3.2.2 IPsec Protocols and Headers

3.2.3 Internet Key Exchange
3.2.4 IKE Phases and Modes
3.2.5 Other IKE Functions
3.2.6 ESP and AH Protocols, Transport, and Tunnel Modes
3.2.7 AH Authentication and Integrity
3.2.8 ESP Protocol
3.2.9 Message Authentication and Integrity Check
3.2.10 PKI Environment
3.3 Implementing Site-to-Site IPsec VPN Operations
3.3.1 Site-to-Site IPsec VPN Operations
3.3.2 Step 2: IKE Phase 1
3.3.3 Step 3: IKE Phase 2
3.3.4 IPsec Tunnel Operation
3.3.5 Configuring a Site-to-Site IPsec VPN
3.4 Configuring IPsec Site-to-Site VPN Using SDM
3.4.1 Cisco SDM Features
3.4.2 Introducing the SDM VPN Wizard Interface
3.4.3 Site-to-Site VPN Components
3.4.4 Launching the Site-to-Site VPN Wizard
3.4.5 Using the Step-by-Step Wizard
3.4.6 Test, Monitor, and Troubleshoot Tunnel Configuration and Operation
3.5 Configuring GRE Tunnels over IPsec
3.5.1 Generic Routing Encapsulation
3.5.2 Secure GRE Tunnels?
3.5.3 Configuring GRE over IPsec Site-to-Site Tunnel Using SDM
3.5.4 Backup GRE Tunnel Information
3.5.5 Configuring VPN Authentication
3.5.6 Configuring IKE Proposals
3.5.7 Configuring the Transform Set
3.5.8 Routing Information
3.5.9 Completing the Configuration
3.5.10 Testing, Monitoring and Troubleshooting GRE Tunnel Configuration
3.6 Configuring High-Availability VPNs
3.6.1 High Availability for IOS IPsec VPNs
3.6.2 IPsec Backup Peer
3.6.3 Hot Standby Routing Protocol
3.6.4 HSRP for Default Gateway at Remote Site
3.6.5 HSRP for Head-end IPsec Routers
3.6.6 IPsec Stateful Failover
3.6.7 Backing Up a WAN Connection with an IPsec VPN
3.7 Introducing Cisco Easy VPN
3.7.1 Introducing Cisco Easy VPN
3.7.2 Cisco Easy VPN Components
3.7.3 Deployment Models
3.7.4 Requirements and Restrictions for Cisco Easy VPN Remote
3.7.5 Easy VPN Server and Easy VPN Remote Operation
3.8 Configuring Easy VPN Server using Cisco SDM
3.8.1 Required Preparation
3.8.2 Configuring the Prerequisites with VPN Wizards
3.8.3 Start the Easy VPN Server Wizard
3.8.4 Configure IKE Proposals
3.8.5 Configure the Transform Set
3.8.6 Storing Group Policy Configurations on the Local Router
3.8.7 Storing Group Policy Configurations on an External User Database via RADIUS
3.8.8 Local Group Policies
3.8.9 Completing the Configuration
3.9 Implementing the Cisco VPN Client
3.9.1 Cisco VPN Client Configuration Tasks
3.9.2 Task 1: Install Cisco VPN Client
3.9.3 Task 2: Create a New Client Connection Entry
3.9.4 Task 3: Configure Client Authentication Properties
3.9.5 Task 4: Configure Transparent Tunneling
3.9.6 Allowing Local LAN Access

3.9.7 Task 5: Enable and Add Backup Servers
3.9.8 Task 6: Configure Connection to the Internet Through Dialup Networking
3.10 IPsec VPN Lab Exercises
3.10.1 Lab 3.1 Configuring SDM on a Router
3.10.2 Lab 3.2 Configuring a Basic GRE Tunnel
3.10.3 Lab 3.3 Configuring Wireshark and SPAN
3.10.4 Lab 3.4 Configuring Site-to-Site IPsec VPNs with SDM
3.10.5 Lab 3.5 Configuring Site-to-Site IPsec VPNs with the IOS CLI
3.10.6 Lab 3.6 Configuring a Secure GRE Tunnel with SDM
3.10.7 Lab 3.7 Configuring a Secure GRE Tunnel with the IOS CLI
3.10.8 Lab 3.8 Configuring IPsec VTIs
3.10.9 Lab 3.9 Configuring Easy VPN with SDM
3.10.10 Lab 3.10 Configuring Easy VPN with the IOS CLI

## Module 4: Frame Mode MPLS Implementation

4.1 Introducing MPLS Networks
4.1.1 The MPLS Conceptual Model
4.1.2 Router Switching Mechanisms
4.1.3 MPLS Basics
4.1.4 MPLS Architecture
4.1.5 Label Switch Routers
4.1.6 LSR Component Architecture
4.2 Assigning MPLS Labels to Packets
4.2.1 Label Allocation in a Frame Mode MPLS Environment
4.2.2 Label Distribution and Advertisement
4.2.3 Populating the LFIB Table
4.2.4 Packet Propagation Across an MPLS Network
4.2.5 Penultimate Hop Popping
4.3 Implementing Frame Mode MPLS
4.3.1 The Procedure to Configure MPLS
4.3.2 Step 1: Configure CEF
4.3.3 Configuring MPLS on a Frame Mode Interface
4.3.4 Configuring the MTU Size in Label Switching
4.4 Describing MPLS VPN Technology
4.4.1 MPLS VPN Architecture
4.4.2 Benefits and Drawbacks of Each VPN Implementation Model
4.4.3 MPLS VPN Architecture
4.4.4 Propagation of Routing Information Across the P-Network
4.4.5 Using RDs in an MPLS VPN
4.4.6 Using Route Targets in an MPLS VPN
4.4.7 End-to-End Routing Information Flow
4.4.8 MPLS VPNs and Packet Forwarding
4.5 MPLS Lab Exercises
4.5.1 Lab 4.1 Configuring Frame Mode MPLS
4.5.2 Lab 4.2 Challenge Lab: Implementing MPLS VPNs (Optional)

## Module 5: Cisco Device Hardening

5.1 Thinking Like a Hacker
5.1.1 Seven Steps to Hacking a Network
5.1.2 Step 1: Footprint Analysis
5.1.3 Step 2: Enumerate Information
5.1.4 Step 3: Manipulate Users to Gain Access
5.1.5 Step 4: Escalate Privileges
5.1.6 Step 5: Gather Additional Passwords and Secrets
5.1.7 Step 6: Install Back Doors and Port Redirectors
5.1.8 Step 7: Leverage the Compromised System
5.1.9 Best Practices to Defeat Hackers
5.2 Mitigating Network Attacks
5.2.1 Types of Network Attacks
5.2.2 Reconnaissance Attacks
5.2.3 Packet Sniffers
5.2.4 Port Scans and Ping Sweeps
5.2.5 Access Attacks and Mitigation
5.2.6 Trust Exploitation

5.2.7 DoS and DDoS Attacks and Mitigation
5.2.8 IP Spoofing in DoS and DDoS
5.3 Network Attacks Using Intelligence
5.3.1 End Station Vulnerabilities: Worm, Virus, and Trojan Horses
5.3.2 Worm Attack, Mitigation and Response
5.3.3 Application Layer Attacks and Mitigation
5.3.4 Management Protocols and Vulnerabilities
5.3.5 Management Protocol Best Practices
5.3.6 Determining Vulnerabilities and Threats
5.4 Disabling Unused Cisco Router Network Services and Interfaces
5.4.1 Vulnerable Router Services and Interfaces
5.4.2 Locking Down Routers with AutoSecure
5.4.3 AutoSecure Process Overview
5.4.4 AutoSecure Processing
5.4.5 Display AutoSecure Configuration
5.4.6 Locking Down Routers with Cisco SDM
5.5 Securing Cisco Router Administrative Access
5.5.1 Cisco Router Passwords
5.5.2 Initial Password Configuration
5.5.3 Protecting Line Access
5.5.4 Additional Password Security
5.5.5 Protecting Your Router by Securing ROMMON
5.5.6 Setting Login Failure Rates and Conditions
5.5.7 Setting Timeouts
5.5.8 Setting Multiple Privilege Levels
5.5.9 Configuring Banner Messages
5.6 Configuring Role-Based CLI
5.6.1 Role-Based CLI Overview
5.6.2 Getting Started with Role-Based CLI
5.6.3 Configuring CLI Views
5.6.4 Configuring Superviews
5.6.5 Role-Based CLI Monitoring
5.6.6 Role-Based CLI Configuration Example
5.6.7 Secure Configuration Files
5.7 Mitigating Threats and Attacks with Access Lists
5.7.1 Overview of Cisco ACL
5.7.2 Applying ACLs to Router Interfaces
5.7.3 Using Traffic Filtering with ACLs
5.7.4 Filtering Network Traffic to Mitigate Threats
5.7.5 Mitigating DDoS with ACLs
5.7.6 Combining Access Functions
5.7.7 Caveats
5.8 Securing Management and Reporting Features
5.8.1 Secure Management and Reporting Planning Considerations
5.8.2 Secure Management and Reporting Architecture
5.8.3 Configuring an SSH Server for Secure Management and Reporting
5.8.4 Using Syslog Logging for Network Security
5.8.5 Configuring Syslog Logging
5.9 Configuring SNMP
5.9.1 SNMP Version 1 and 2
5.9.2 SNMPv3
5.9.3 Configuring an SNMP Managed Node
5.9.4 Task 1: Configuring the SNMP-Server Engine ID
5.9.5 Task 2: Configuring the SNMP-Server Group Names
5.9.6 Task 3: Configuring the SNMP-Server Users
5.9.7 Task 4: Configuring the SNMP-Server Hosts
5.10 Configuring the NTP Client
5.10.1 Understanding NTP
5.10.2 Configuring NTP Authentication
5.10.3 Configuring NTP Associations
5.10.4 Configuring Additional NTP Options
5.10.5 Implementing the NTP Server
5.10.6 Configuring NTP Server

5.11 Configuring AAA on Cisco Routers
5.11.1 Introduction to AAA
5.11.2 Router Access Modes
5.11.3 AAA Protocols: RADIUS and TACACS+
5.11.4 Configure AAA Login Authentication on Cisco Routers Using CLI
5.11.5 Configure AAA Login Authentication on Cisco Routers Using SDM
5.11.6 Troubleshoot AAA Login Authentication on Cisco Routers
5.11.7 AAA Authorization Commands
5.11.8 AAA Accounting Commands
5.11.9 Troubleshooting Accounting
5.12 Cisco Device Hardening Lab Exercises
5.12.1 Lab 5.1 Using SDM One-Step Lockdown
5.12.2 Lab 5.2 Securing a Router with Cisco AutoSecure
5.12.3 Lab 5.3 Disabling Unneeded Services
5.12.4 Lab 5.4 Enhancing Router Security
5.12.5 Lab 5.5 Configuring Logging
5.12.6 Lab 5.6 Configuring AAA Authentication
5.12.7 Lab 5.7 Configuring Role-Based CLI Views
5.12.8 Lab 5.8 Configuring NTP

## Module 6: Cisco IOS Threat Defense Features

6.1 Introducing the Cisco IOS Firewall
6.1.1 Layered Defense Strategy
6.1.2 Private VLAN
6.1.3 Firewall Technologies
6.1.4 Stateful Firewall Operation
6.1.5 Introducing the Cisco IOS Firewall Feature Set
6.1.6 Cisco IOS Firewall Functions
6.1.7 Cisco IOS Firewall Process
6.1.8 Stateful Inspection Enhancements
6.1.9 Alerts and Audit Trails
6.2 Configuring Cisco IOS Firewall from the CLI
6.2.1 Configuration Tasks
6.2.2 Pick an Interface: Internal or External
6.2.3 Configure IP ACLs at the Interface
6.2.4 Set Audit Trails and Alerts
6.2.5 Inspection Rules for Application Protocols
6.2.6 Apply an Inspection Rule to an Interface
6.2.7 Verifying Cisco IOS Firewall
6.2.8 Troubleshooting Cisco IOS Firewall
6.3 Basic and Advanced Firewall Wizards
6.3.1 Basic and Advanced Firewall Wizards
6.3.2 Configuring a Basic Firewall
6.3.3 Configuring Interfaces on an Advanced Firewall
6.3.4 Configuring a DMZ on an Advanced Firewall
6.3.5 Advanced Firewall Security Configuration
6.3.6 Complete the Configuration
6.3.7 Viewing Firewall Activity
6.4 Introducing Cisco IOS IPS
6.4.1 Introducing Cisco IOS IDS and IPS
6.4.2 Types of IDS and IPS Systems
6.4.3 Network-Based and Host-Based IPS
6.4.4 NIPS Features
6.4.5 Signature-Based IDS and IPS
6.4.6 Policy-Based IDS and IPS
6.4.7 Anomaly-Based IDS and IPS
6.4.8 Honeypot-Based IDS and IPS
6.4.9 IDS and IPS Signatures
6.5 Configuring Cisco IOS IPS
6.5.1 Cisco IOS IPS Signature Definition Files (SDF)
6.5.2 Cisco IOS IPS Alarms
6.5.3 Configuring Cisco IOS IPS
6.5.4 Cisco IOS IPS SDM Tasks
6.5.5 Selecting Interfaces and Configuring SDF Locations

6.5.6 Viewing the IPS Policy Summary and Delivering the Configuration to the Router
6.5.7 Configuring IPS Policies and Global Settings
6.5.8 Viewing SDEE Messages
6.5.9 Tuning Signatures
6.6 Threat Defense Lab Exercises
6.6.1 Lab 6.1 Configuring a Cisco IOS Firewall Using SDM
6.6.2 Lab 6.2 Configuring CBAC
6.6.3 Lab 6.3 Configuring IPS with SDM
6.6.4 Lab 6.4 Configuring IPS with CLI

# CCNP3 : BMSN : Building Multilayer Switched Networks v5.0

## Module 1: Network Requirements

1.1 Introducing Campus Networks
1.1.1 Intelligent Information Network and Service-Oriented Network Architecture
1.1.2 Cisco Network Models
1.1.3 Describing 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 The 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 2: Defining VLANs

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 Networ
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 Switches to an Existing VTP Domain
2.5 Correcting Common VLAN 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 Lab 2-0 Clearing a Switch
2.6.2 Lab 2-1 Catalyst 2960 and 3560 Series Static VLANS, VLAN Trunking, and VTP Domain and Modes

## Module 3: Implementing Spanning Tree

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 Spanning Tree Lab Exercises
3.5.1 Lab 3-1 Spanning Tree Protocol (STP) Default Behavior
3.5.2 Lab 3-2 Modifying Default Spanning Tree Behavior
3.5.3 Lab 3-3 Per-VLAN Spanning Tree Behavior
3.5.4 Lab 3-4 Multiple Spanning Tree
3.5.5 Lab 3-5 Configuring Etherchannel

## Module 4: Implementing Inter-VLAN Routing

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 SVI
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 Lab 4-1 Inter-VLAN Routing with an External Router
4.4.2 Lab 4-2 Inter-VLAN Routing with an Internal Route Processor and Monitoring CEF Functions

## Module 5: Implementing High Availability in a Campus Environment

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 High Availability Lab Exercise
5.4.1 Lab 5-1 Hot Standby Router Protocol

## Module 6: Wireless LANs

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 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 WLANs
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 WLAN Controller Configuration
6.6.5 Cisco Wireless LAN Controller Boot Menu
6.6.6 Web Wizard Initial Configuration
6.7 WLAN Lab Exercises
6.7.1 Lab 6-1 Configuring a WLAN Controller
6.7.2 Lab 6-2 Configuring a WLAN Controller via the Web Interface
6.7.3 Lab 6-3 Configuring a Wireless Client
**Module 7: Configuring Campus Switches to Support Voice**
7.1 Planning for Implementation of Voice in a Campus
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 Voice Support Lab Exercises
7.3.1 Lab 7-1 Configuring Switches for IP Telephony Support
**Module 8: Minimizing Service Loss and Data Theft in a Campus Network**
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 Methods
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 Switch Security Lab Exercises
8.7.1 Lab 8-1 Securing the Layer 2 Switching Devices
8.7.2 Lab 8-2 Securing Spanning Tree Protocol
8.7.3 Lab 8-3 Securing VLANs with Private VLANs, RACLs, and VACLs

# CCNP4 : OCN : Optimized Converged Networks v5.0

## Module 1: Converged Network Connectivity Requirements

1.1 The Evolution of Telephony in the Enterprise
1.1.1 A Basic Telephone System
1.1.2 Traditional Telephone Company Services
1.1.3 Digital Telephone Technologies
1.1.4 Digital Telephone Services
1.1.5 PBXs and Centrex Services
1.1.6 Long-Distance Services
1.1.7 The Concept of Convergence
1.2 Describing Converged Network Requirements
1.2.1 Hierarchical Network Model
1.2.2 Cisco Enterprise Architecture
1.2.3 Traffic Conditions in a Converged Network
1.2.4 Intelligent Information Network
1.2.5 Cisco SONA Framework

## Module 2: Cisco VoIP Implementations

2.1 Introducing VoIP Networks
2.1.1 Benefits of VoIP Networks
2.1.2 Components of a VoIP Network
2.1.3 Legacy Analog Interfaces in VoIP Networks
2.1.4 Digital Interfaces
2.1.5 Stages for Completing a VoIP Telephone Call
2.1.6 Distributed Call Control
2.1.7 Centralized Call Control
2.2 Digitizing and Packetizing Voice
2.2.1 Basic Voice Encoding: Converting Analog Signals to Digital Signals
2.2.2 Basic Voice Encoding: Converting Digital Signals to Analog Signals
2.2.3 Sampling
2.2.4 Quantization
2.2.5 Digital Voice Encoding
2.2.6 Companding
2.2.7 Common Voice Codec Characteristics
2.2.8 Selecting a Codec Using the Mean Opinion Score

2.2.9 A Closer Look at a DSP
2.3 Encapsulating Voice Packets for Transport
2.3.1 Voice Transport in Circuit-Switched Networks
2.3.2 Voice Transport in IP Networks
2.3.3 Protocols Used in Voice Encapsulation
2.3.4 Voice Encapsulation Codecs
2.3.5 Reducing Header Overhead with cRTP
2.3.6 When to Use RTP Header Compression
2.4 Calculating Bandwidth Requirements for VoIP
2.4.1 Impact of Voice Samples and Packet Size on Bandwidth
2.4.2 Impact of Codecs on Bandwidth
2.4.3 How the Packetization Period Affects VoIP Packet Size and Rate
2.4.4 Data-Link Overhead
2.4.5 Security and Tunneling Overhead
2.4.6 Extra Headers in Security and Tunneling Protocols
2.4.7 Calculating the Total Bandwidth for a VoIP Call
2.4.8 Quick Bandwidth Calculation
2.4.9 Effects of VAD on Bandwidth
2.5 Implementing VoIP in an Enterprise Network
2.5.1 Enterprise Voice Implementations
2.5.2 Deploying CAC
2.5.3 Voice Gateway Functions on a Cisco Router
2.5.4 Cisco Unified CallManager Functions
2.5.5 Enterprise IP Telephony Deployment Models
2.5.6 Cisco IOS Configurations for VoIP
2.6 VoIP Lab Exercises
2.6.1 Lab 2.1 Configure CME using the CLI and Cisco IP Communicator

## Module 3: Introduction to IP QoS

3.1 Introducing QoS
3.1.1 Converged Network Quality Issues
3.1.2 Quality Issues in Converged Networks
3.1.3 Measuring Available Bandwidth
3.1.4 Increasing Available Bandwidth
3.1.5 Effects of End-to-end Delay and Jitter
3.1.6 Reducing the Impact of Delay on Quality
3.1.7 Packet Loss
3.1.8 Congestion Management: Ways to Prevent Packet Loss
3.2 Implementing Cisco IOS QoS
3.2.1 What is QoS?
3.2.2 Congestion-Management Tools
3.2.3 Queue Management (Congestion-Avoidance Tools)
3.2.4 Preparing to Implement QoS
3.2.5 Step 1: Identify Types of Traffic and Their Requirements
3.2.6 Step 2: Define Traffic Classes
3.2.7 Step 3: Define QoS Policy
3.3 Selecting an Appropriate QoS Policy Model
3.3.1 Three QoS Models
3.3.2 Best-Effort Model
3.3.3 IntServ Model
3.3.4 RSVP and the IntServ QoS Model
3.3.5 RSVP Operation
3.3.6 The DiffServ Model
3.4 Using MQC for Implementing QoS
3.4.1 Methods for Implementing QoS Policy
3.4.2 Configuring QoS at the CLI
3.4.3 Modular QoS CLI
3.4.4 Modular QoS CLI Step 1: Configuring Class Maps
3.4.5 Step 2: Configuring Policy Maps
3.4.6 Step 3: Attaching a Service Policy to Interfaces
3.4.7 Nested Class Maps
3.4.8 MQC Example
3.4.9 Basic MQC Verification Commands
3.5 Implementing QoS with Cisco SDM QoS Wizard

3.5.1 Configuring QoS with Cisco SDM QoS Wizard
3.5.2 Creating a QoS Policy
3.5.3 Reviewing the QoS Configuration
3.5.4 Monitoring QoS Status
3.6 Introduction QoS Lab Exercises
3.6.1 Lab 3.1 Preparing for QoS
3.6.2 Lab 3.2 Installing SDM
3.6.3 Lab 3.3 Configuring QoS with SDM

## Module 4: Implement the DiffServ QoS Model

4.1 Introducing Classification and Marking
4.1.1 Classification
4.1.2 Marking
4.1.3 Classification and Marking at the Link Layer
4.1.4 DiffServ Model
4.1.5 IP Precedence and DSCP Compatibility
4.1.6 Per-Hop Behaviors
4.1.7 Standard PHB Groups
4.1.8 Mapping CoS to Network Layer QoS
4.1.9 QoS Service Class Defined
4.1.10 Implementing QoS Policy Using a QoS Service Class
4.1.11 Trust Boundaries
4.2 Using NBAR for Classification
4.2.1 Network-Based Application Recognition
4.2.2 NBAR Application Support
4.2.3 Packet Description Language Module
4.2.4 Protocol Discovery
4.2.5 Configuring and Monitoring NBAR Protocol Discovery
4.2.6 Configuring NBAR for Static Protocols
4.2.7 Configuring Stateful NBAR for Dynamic Protocols
4.3 Introducing Queuing Implementations
4.3.1 Congestion and Queuing
4.3.2 Congestion Management - Queuing Algorithms
4.3.3 FIFO
4.3.4 Priority Queuing
4.3.5 Round Robin
4.3.6 Router Queuing Components
4.4 Configuring WFQ
4.4.1 Weighted Fair Queuing
4.4.2 WFQ Architecture and Benefits
4.4.3 WFQ Classification
4.4.4 WFQ Insertion and Drop Policy
4.4.5 Benefits and Drawbacks of WFQ
4.4.6 Configuring WFQ
4.4.7 Monitoring WFQ
4.5 Configuring CBWFQ and LLQ
4.5.1 Combining Queuing Methods
4.5.2 Class-Based Weighted Fair Queuing
4.5.3 CBWFQ Architecture, Classification and Scheduling
4.5.4 Configuring and Monitoring CBWFQ
4.5.5 Low Latency Queuing
4.5.6 LLQ Architecture and Benefits
4.5.7 Configuring and Monitoring LLQ
4.6 Congestion Avoidance
4.6.1 Managing Interface Congestion with Tail Drop
4.6.2 Tail Drop Limitations
4.6.3 Using Random Early Detection
4.6.4 Weighted Random Early Detection
4.6.5 WRED Drop Profiles
4.6.6 Configuring CBWRED
4.6.7 WRED Profiles: DSCP-Based WRED (AF)
4.6.8 Monitoring CBWRED
4.7 Introducing Traffic Policing and Shaping
4.7.1 Traffic Policing and Shaping Overview

4.7.2 Why Use Traffic Conditioners?
4.7.3 Policing vs. Shaping
4.7.4 Measuring Traffic Rates with Tokens
4.7.5 Single Token Bucket Class-Based Policing
4.7.6 Cisco IOS Traffic Policing and Shaping Mechanisms
4.7.7 Applying Traffic Policing
4.8 Understanding WAN Link Efficiency Mechanisms
4.8.1 Link Efficiency Mechanisms
4.8.2 Compression Overview
4.8.3 Layer 2 Payload Compression
4.8.4 Header Compression
4.8.5 Large Packets "Freeze Out" Voice on Slow WAN Links
4.8.6 Link Fragmentation and Interleaving
4.8.7 Applying Link Efficiency Mechanisms
4.9 Implementing QoS Preclassify
4.9.1 Virtual Private Networks
4.9.2 Implementing QoS with Preclassification
4.9.3 QoS Preclassify Applications
4.9.4 QoS Preclassification Deployment Options
4.10 Deploying End-to-End QoS
4.10.1 QoS SLAs
4.10.2 Typical SLA Requirements for Voice
4.10.3 Deploying End-to-End QoS
4.10.4 Enterprise Campus QoS Implementations
4.10.5 WAN Edge QoS Implementations
4.10.6 WAN Edge Design
4.10.7 Control Plane Policing?
4.11 DiffServ QoS Lab Exercises
4.11.1 Lab 4.1 Default Queuing Tools
4.11.2 Lab 4.2 Intermediate Queuing Tools
4.11.3 Lab 4.3 TCP Header Compression
4.11.4 Lab 4.4 Comparing Queuing Strategies
4.11.5 Lab 4.5 Class-based Queuing and NBAR
4.11.6 Lab 4.6 Class-based Marking, Shaping, and Policing
4.11.7 Lab 4.7 WAN QoS Tools
4.11.8 Lab 4.8 Shaping and Policing
4.11.9 Lab 4.9 QoS Pre-classify

## Module 5: Implement Cisco AutoQoS

5.1 Introducing Cisco AutoQoS
5.1.1 Cisco AutoQoS
5.1.2 Cisco AutoQoS Evolution
5.1.3 Deploying Cisco AutoQoS on Switches
5.1.4 Cisco AutoQoS for the Enterprise: Router Deployment Restrictions
5.1.5 Router Design Considerations
5.1.6 Router Prerequisites
5.1.7 Deploying Cisco AutoQoS for the Enterprise on Routers: A Two-Step Approach
5.1.8 Verifying Cisco AutoQoS
5.2 Mitigating Common Cisco AutoQoS Issues
5.2.1 Automation with Cisco AutoQoS
5.2.2 DiffServ QoS Mechanisms Enabled by Cisco AutoQoS
5.2.3 Automated Cisco AutoQoS DiffServ Class Provisioning
5.2.4 Common Issues with Cisco AutoQoS
5.2.5 Interpreting Cisco AutoQoS Configurations
5.2.6 Modifying the Active Cisco AutoQoS Configuration with MQC
5.2.7 Modifying AutoQoS Generated Policy with MQC
5.3 AutoQoS Lab Exercises
5.3.1 Lab 5.1 AutoQoS

## Module 6: Implement Wireless Scalability

6.1 Implementing WLAN QoS
6.1.1 A Standard for WLAN QoS
6.1.2 WLAN QoS Description
6.1.3 WLAN QoS RF Backoff Timing

6.1.4 Lightweight Access Point—Split MAC Architecture
6.1.5 WLAN QoS Challenges
6.1.6 WLAN QoS Implementation
6.1.7 Packet Tagging
6.1.8 WLAN QoS Configuration
6.2 Introducing Wireless Security
6.2.1 The Need for WLAN Security
6.2.2 802.11 WEP
6.2.3 WLAN Authentication
6.2.4 Cisco Enhanced 802.11 WEP Security
6.2.5 802.1x Overview
6.2.6 LEAP
6.2.7 EAP-FAST
6.2.8 EAP-TLS
6.2.9 PEAP
6.2.10 Wi-Fi Protected Access
6.2.11 WPA Issues
6.3 Managing WLANs
6.3.1 Cisco Unified Wireless Network
6.3.2 Cisco WLAN Implementation and Components
6.3.3 CiscoWorks WLSE for the Autonomous WLAN Solution
6.3.4 Simplified CiscoWorks WLSE Express Setup
6.3.5 CiscoWorks WLSE Benefits
6.3.6 Cisco WCS for the LWLAN Solution
6.3.7 Cisco WCS Software Features
6.3.8 Cisco WCS User Interface
6.3.9 Cisco Wireless Location Appliance
6.4 Deploying Cisco WCS
6.4.1 Cisco WCS Configuration Example
6.4.2 Adding a Cisco Wireless LAN Controller to Cisco WCS
6.4.3 Configuring a Cisco Access Point
6.4.4 Adding a Campus Map to the Cisco WCS Database
6.4.5 Adding New Building to the Cisco WCS Database
6.4.6 Rogue Access Point Detection
6.4.7 Rogue Access Point Location
6.5 Configuring Encryption and Authentication on Lightweight Access Points
6.5.1 Configuring Open Authentication
6.5.2 Configuring Static WEP Key Authentication
6.5.3 Configuring WPA Preshared Key
6.5.4 Configuring Web Authentication
6.5.5 Customizing the Web Login Page
6.5.6 Configuring 802.1x Authentication
6.5.7 Configuring WPA with 802.1x
6.5.8 WPA2
6.6 WLAN Lab Exercises
6.6.1 Lab 6.1 Configuring a WLAN Controller
6.6.2 Lab 6.2 Configuring a WLAN Controller via the Web Interface
6.6.3 Lab 6.3 Configuring a Wireless Client
6.6.4 Lab 6.4 Configuring WPA Security with Preshared Keys
6.6.5 Lab 6.5 Configuring LEAP