

CCNP 2: Remote Access

**Cisco Networking Academy Program
Version 3.0**

Table of Contents

CCNP 2: REMOTE ACCESS.....	1
TARGET AUDIENCE	3
PREREQUISITES	3
COURSE DESCRIPTION.....	3
COURSE OBJECTIVES.....	3
LAB REQUIREMENTS	4
CERTIFICATION ALIGNMENT.....	4
COURSE OVERVIEW	4
COURSE OUTLINE.....	5
<i>Module 1. WANs.....</i>	<i>5</i>
<i>Module 2. Modems and Async Connections</i>	<i>6</i>
<i>Module 3. PPP</i>	<i>7</i>
<i>Module 4. ISDN and DDR.....</i>	<i>8</i>
<i>Module 5. Dialer Profiles</i>	<i>10</i>
<i>Module 6. Frame Relay.....</i>	<i>11</i>
<i>Module 7. Managing Frame Relay Traffic</i>	<i>11</i>
<i>Module 8. WAN Backup</i>	<i>12</i>
<i>Module 9. Managing and Optimizing Traffic</i>	<i>13</i>
<i>Module 10. Scaling IP Addressing with NAT.....</i>	<i>14</i>
<i>Module 11. Using AAA Scale Access Control.....</i>	<i>15</i>
<i>Module 12. Broadband Connections.....</i>	<i>16</i>
<i>Module 13. Virtual Private Networks</i>	<i>17</i>
<i>Case Study: Remote Access</i>	<i>19</i>

Target Audience

Those desiring to continue their post-CCNA preparation for a career as a network administrator, Level 2 support engineer, Level 2 systems engineer, network technician, or deployment engineer. CCNA certified individuals pursuing CCNP, CCIP, CCSP, CCDP, or CCIE certifications.

Prerequisites

- Students should have completed CCNA 1 – 4 or equivalent.
- CCNA Certification desired but not required.
- CCNP 1 desired but not required.
- Work experience beneficial.

Course Description

CCNP 2: Remote Access is the second of four courses leading to the Cisco Certified Network Professional (CCNP) designation. CCNP 2 introduces student to the implementation of Cisco routers in WAN applications. The course focuses on the selection and implementation of the appropriate Cisco IOS services required to build intranet remote access links. Students will develop skills with the specific WAN technologies of analog dialup, ISDN BRI and PRI, Frame Relay, broadband, and VPN. This hands-on, lab-oriented course stresses the design, implementation, operation, and level 1 troubleshooting of common WAN connectivity options.

Course Objectives

The CCNP certification indicates knowledge of networking for the small-office, home-office (SOHO) market and enterprise markets and the ability to work in businesses or organizations whose networks have between 100 and 500 nodes. A CCNP certified individual should be able to:

- Implement appropriate technologies to build a scalable routed network
- Build campus networks using multilayer switching technologies
- Improve traffic flow, reliability, redundancy, and performance for campus LANs, routed and switched WANs, and remote access networks
- Create and deploy a global intranet
- Troubleshoot an environment that uses Cisco routers and switches for multiprotocol client hosts and services
- Perform entry-level tasks in the planning, design, installation, operation and troubleshooting of Ethernet, TCP/IP networks.

CCNP 2 is an integral step towards achieving CCNP Certification.

Upon completion of this course, students will have performed tasks related to:

- WANs
- Modems and asynchronous connections
- PPP and serial connections
- ISDN BRI and PRI and DDR
- Frame Relay configuration and traffic shaping
- WAN backup, managing and optimizing traffic
- NAT and AAA
- Broadband connections
- VPNs

Lab Requirements

Please refer to CCNP Equipment Bundle Spreadsheets on Cisco Academy Connection (CAC)

Certification Alignment

The curriculum is aligned with ILSGs BCMSN course and the 642-821 exam.

Course Overview

The course is designed to be delivered in a 70 contact hour time frame. Approximately 45 hours will be designated to lab activities and 25 hours on curriculum content. A case study on remote access is required, but format and timing are determined by the Local Academy.

What has changed from CCNP versions 2.x?

- Removal of X.25
- Revision of queuing
- Addition of Broadband module
- Addition of VPN module
- More than 40 eLabs are included in the curriculum
- Focus is maintained on hands-on labs

Course Outline

Module 1. WANs

Overview

1.1 Introduction to WANs

- 1.1.1 WAN connection types
- 1.1.2 Dedicated connections
- 1.1.3 Dedicated connections
- 1.1.4 Circuit-Switched connections
- 1.1.5 Asynchronous dialup connections
- 1.1.6 ISDN connections
- 1.1.7 Packet-switched networks
- 1.1.8 WAN encapsulation protocols

1.2 Choosing WAN Technologies

- 1.2.1 Choosing a WAN connection
- 1.2.2 Identifying site requirements and solutions
- 1.2.3 Central site considerations
- 1.2.4 Branch office considerations
- 1.2.5 Telecommuter-site considerations

1.3 Selecting Cisco Remote Access Solutions

- 1.3.1 Routers
- 1.3.2 Determining the appropriate interfaces -- fixed interfaces
- 1.3.3 Determining the appropriate interfaces -- modular interfaces

1.4 Assembling and Cabling WAN Components

- 1.4.1 Network overview
- 1.4.2 Central site equipment
- 1.4.3 Branch-office router equipment
- 1.4.4 Telecommuter-site router equipment
- 1.4.5 International Travel Agency

1.5 Lab Exercises

- 1.5.1 Lab: Getting started
- 1.5.2 Lab: Capturing HyperTerminal and Telnet sessions
- 1.5.3 Lab: ACL Basics and Extended Ping

Summary

Module 2. Modems and Async Connections

Overview

2.1 Modem Functions

- 2.1.1 Digital to Analog Conversion
- 2.1.2 The role of the modem
- 2.1.3 Modem signaling and cabling
- 2.1.4 The EIA/TIA-232 standard
- 2.1.5 DTE communication termination
- 2.1.6 Modem cabling components
- 2.1.7 Connecting a modem to a router
- 2.1.8 Connecting a modem to an access server, async lines
- 2.1.9 Connecting a modem to a PC
- 2.1.10 Directly connecting a DTE to another DTE -- null modem
- 2.1.11 Modem modulation standards
- 2.1.12 Error control and data compressions

2.2 Configuring Asynchronous Interfaces and Terminal Lines

- 2.2.1 Connecting to the modem - reverse telnet
- 2.2.2 Line types and numbering
- 2.2.3 Configuring reverse telnet
- 2.2.4 Asynchronous interfaces and line configuration
- 2.2.5 Basic terminal line configuration
- 2.2.6 Basic auxiliary port configuration
- 2.2.7 Configuring the console port to use a modem
- 2.2.8 Configuring a serial interface to use a modem
- 2.2.9 Configuring asynchronous interfaces
- 2.2.10 Asynchronous interface configuration example
- 2.2.11 Introduction to DDR - Dialer List

2.3 Modem Configuration

- 2.3.1 Modem configuration methods
- 2.3.2 Manual configuration of modems with standard commands
- 2.3.3 Manual configuration of modems with nonstandard modem commands
- 2.3.4 Modem initialization strings
- 2.3.5 Automatic configuration of modems
- 2.3.6 Modem capability database

- 2.3.7 Modem autodiscovery
- 2.3.8 Modem autoconfiguration
- 2.3.9 Fine tuning modem autoconfiguration
- 2.3.10 Chat scripts for async lines
- 2.3.11 Configuring asynchronous connections between remote routers
- 2.4 Verifying Modem Autoconfiguration
 - 2.4.1 Verifying and debugging modem autoconfiguration
 - 2.4.2 Troubleshooting modem autoconfiguration
- 2.5 Lab Exercises
 - 2.5.1 Lab: Configuring an asynchronous dialup connection
 - 2.5.2 Lab: Configuring an asynchronous dialup connection on the AUX port
 - 2.5.3 Lab: Configuring an asynchronous dialup PPP
- Summary

Module 3. PPP

Overview

3.1 PPP Overview

- 3.1.1 Point-to-point links
- 3.1.2 PPP architecture
- 3.1.3 Configuring PPP
- 3.1.4 Dialup PPP vs. dialup EXEC sessions
- 3.1.5 Configuring dedicated PPP sessions
- 3.1.6 Configuring interactive PPP sessions
- 3.1.7 Configuring the interface addressing method for local devices
- 3.1.8 Configuring the interface addressing method for remote devices
- 3.1.9 PPP LCP Options

3.2 PPP Authentication

- 3.2.1 PAP and CHAP authentication
- 3.2.2 Configuring PAP authentication
- 3.2.3 Configuring CHAP authentication
- 3.2.4 Configuring CHAP and PAP authentication

3.3 PPP Callback

- 3.3.1 Dialup PPP callback overview

- 3.3.2 PPP callback operation
- 3.3.3 Configuring the callback server
- 3.3.4 Configuring the callback client
- 3.4 PPP Compression
 - 3.4.1 Data compression
 - 3.4.2 Configuring compression
 - 3.4.3 Verifying compression
- 3.5 PPP Multilink
 - 3.5.1 PPP multilink overview
 - 3.5.2 Multilink PPP operation and configuration
 - 3.5.3 Multilink PPP example
- 3.6 Verifying PPP configuration
 - 3.6.1 Verifying and troubleshooting PPP
 - 3.6.2 PPP configuration example
- 3.7 Lab Exercises
 - 3.7.1 Lab: Configuring PPP interactive mode
 - 3.7.2 Lab: Configuring PPP options: Authentication and Compression
 - 3.7.3 Lab: Configuring PPP callback
- Summary

Module 4. ISDN and DDR

- 4.1 ISDN Architecture
 - 4.1.1 ISDN versus asynchronous dialup
 - 4.1.2 ISDN services and channelized E1 and T1
 - 4.1.3 BRI call processing
 - 4.1.4 BRI functional groups and reference points
 - 4.1.5 Physical representation of BRI reference points
 - 4.1.6 PRI reference points
- 4.2 ISDN Protocol Layers
 - 4.2.1 ISDN Layer 1
 - 4.2.2 ISDN Layer 2 -- Q.921
 - 4.2.3 ISDN Layer 3 -- Q.931

- 4.2.4 ISDN call setup
- 4.2.5 ISDN call teardown
- 4.3 Configuring ISDN BRI
 - 4.3.1 ISDN BRI configuration overview
 - 4.3.2 Configuring the ISDN switch type
 - 4.3.3 Configuring the SPIDs
 - 4.3.4 Configuring the encapsulation protocol
- 4.4 Configuring Dial-on-Demand Routing (DDR)
 - 4.4.1 DDR configuration overview
 - 4.4.2 Defining interesting traffic
 - 4.4.3 Assigning the dialer-list to an interface
 - 4.4.4 Defining destination parameters
 - 4.4.5 Defining optional call parameters
- 4.5 Static and Default Routing
 - 4.5.1 Use of static and default routes
 - 4.5.2 Configuring static routes
 - 4.5.3 Configuring default routes
 - 4.5.4 Configuring route redistribution
 - 4.5.5 Deactivating routing updates
 - 4.5.6 Snapshot routing
 - 4.5.7 Snapshot routing model
 - 4.5.8 Enabling snapshot routing
 - 4.5.9 Snapshot routing configuration example
- 4.6 Optional Configurations
 - 4.6.1 B-channel aggregation
 - 4.6.2 Cisco proprietary BOD
 - 4.6.3 Multilink PPP
 - 4.6.4 ISDN caller identification
 - 4.6.5 Called-party number answering
 - 4.6.6 ISDN rate adaptation
 - 4.6.7 ISDN BRI configuration example
- 4.7 Verifying ISDN BRI Operation
 - 4.7.1 The show interface bri command
 - 4.7.2 ISDN show commands
 - 4.7.3 Verifying and troubleshooting PPP multilink
 - 4.7.4 ISDN debug command

4.8 Configuring ISDN PRI

- 4.8.1 PRI configuration tasks
- 4.8.2 Selecting the PRI switch
- 4.8.3 Configuring the T1/E1 controller for PRI
- 4.8.4 Additional ISDN PRI configuration parameters
- 4.8.5 PRI configuration example
- 4.8.6 ISDN BRI to PRI connection example using DDR

4.9 Lab Exercises

- 4.9.1 Lab: Configuring ISDN BRI
- 4.9.2 Lab: Configuring snapshot routing
- 4.9.3 Lab: Using PPP multilink for ISDN B-Channel aggregation
- 4.9.4 Lab: Configuring ISDN PRI

Summary

Module 5. Dialer Profiles

5.1 Legacy DDR

- 5.1.1 Legacy DDR with a single destination
- 5.1.2 Legacy DDR with multiple destinations
- 5.1.3 Rotary group overview
- 5.1.4 Using rotary groups
- 5.1.5 Configuring rotary groups
- 5.1.6 Configuring ISDN for dialer rotary groups
- 5.1.7 Asynchronous interface groups
- 5.1.8 Legacy DDR limitations

5.2 Dialer Profiles

- 5.2.1 Overview of dialer profiles
- 5.2.2 Configuring dialer profiles
- 5.2.3 Dialer pools
- 5.2.4 Placing calls with dialer profiles
- 5.2.5 Receiving calls with dialer profiles
- 5.2.6 Using dialer profiles with ISDN B channels
- 5.2.7 Using dialer profiles with ISDN PRI
- 5.2.8 Dialer map class

5.3 Lab Exercises

- 5.3.1 Lab: Configuring ISDN using dialer profiles
- 5.3.2 Lab: Using a dialer map-class with dialer profiles

Summary

Module 6. Frame Relay

Overview

6.1 Frame Relay overview

- 6.1.1 Frame Relay overview
- 6.1.2 Frame Relay devices
- 6.1.3 Frame Relay operation
- 6.1.4 Frame Relay DLCIs
- 6.1.5 Frame Relay LMI
- 6.1.6 Inverse ARP

6.2 Configuring Frame Relay

- 6.2.1 Configuring Frame Relay encapsulation
- 6.2.2 Configuring Frame Relay maps
- 6.2.3 Configuring encapsulation per PVC
- 6.2.4 Verifying Frame Relay interface configuration
- 6.2.5 Verifying Frame Relay operation

6.3 Frame Relay topologies

- 6.3.1 Frame Relay topologies
- 6.3.2 Solution for split horizon issue, subinterfaces
- 6.3.3 Configuring Frame Relay subinterfaces

6.4 Lab Exercises

- 6.4.1 Lab: Basic Frame Relay router and switch configuration
- 6.4.2 Lab: Configuring full mesh Frame Relay
- 6.4.3 Lab: Configuring full mesh Frame Relay with subinterfaces
- 6.4.4 Lab: Configuring hub and spoke Frame Relay

Summary

Module 7. Managing Frame Relay Traffic

Overview

7.1 Frame Relay Traffic Shaping

- 7.1.1 Frame Relay traffic flow

- 7.1.2 Overview of Frame Relay traffic shaping
 - 7.1.3 Types of Frame Relay traffic management
 - 7.1.4 Configuring traffic shaping over Frame Relay
 - 7.1.5 Traffic shaping configuration steps
 - 7.1.6 Traffic shaping through rate enforcement
 - 7.1.7 Traffic shaping through dynamic rate enforcement
 - 7.1.8 Traffic shaping with queuing
 - 7.1.9 Verifying Frame Relay traffic shaping
 - 7.2 Lab Exercises
 - 7.2.1 Lab: Configuring Frame Relay subinterfaces and traffic shaping
 - 7.2.2 Lab: Configuring Frame Relay traffic shaping with CBWFQ
- Summary

Module 8. WAN Backup

Overview

8.1 Dial Backup

- 8.1.1 Dial backup
- 8.1.2 Example of dial backup for link failure
- 8.1.3 Activating a dial backup to support primary line traffic
- 8.1.4 Example of dial backup for excessive traffic load

8.2 Backup interface Operations

- 8.2.1 Standby mode
- 8.2.2 Dialer Profiles as backup interfaces
- 8.2.3 Configuring dial backups with dialer profiles

8.3 Load backup IGRP and EIGRP

- 8.3.1 Load backup with OSPF
- 8.3.2 Load backup with IGRP and EIGRP

8.4 Verifying dial backup configuration

- 8.4.1 Show interface type number command

8.5 Floating Static Routes

- 8.5.1 Configuring floating static routes as backup

8.6 Dialer Watch

- 8.6.1 Dialer watch overview
- 8.6.2 Configuring dialer watch

8.7 Lab Exercises

- 8.7.1 Lab: Configuring ISDN Dial backup
- 8.7.2 Lab: Using secondary links for on-demand bandwidth
- 8.7.3 Lab: Configuring dialer backup with dialer profiles
- 8.7.4 Lab: Configuring DDR backup with BRI and dialer-watch

Summary

Module 9. Managing and Optimizing Traffic

Overview

9.1 Queuing Options

- 9.1.1 Queuing overview
- 9.1.2 Effective use of traffic prioritization
- 9.1.3 Establishing a queuing policy
- 9.1.4 Choosing a Cisco IOS queuing option

9.2 Configuring Weighted Fair Queuing

- 9.2.1 Weighted fair queuing overview
- 9.2.2 Weighted fair queuing operation
- 9.2.3 Configuring weighted fair queuing
- 9.2.4 Weighted Fair Queuing example

9.3 Class-Based Weighted Fair Queuing Overview

- 9.3.1 CBWFQ
- 9.3.2 CBWFQ versus flow-based WFQ
- 9.3.3 CBWFQ and tail drops
- 9.3.4 Weighted random early detect (WRED)
- 9.3.5 Configuring CBWFQ - Step 1
- 9.3.6 Configuring CBWFQ - Step 2
- 9.3.7 Configuring CBWFQ with WRED - Step 2
- 9.3.8 Configuring CBWFQ default class - Step 3
- 9.3.9 Configuring CBWF - Step 3
- 9.3.10 CBWFQ Queuing Example 1

9.4 Configuring Low Latency Queuing

- 9.4.1 Low Latency Queuing (LLQ)
- 9.4.2 Configuring Low Latency queuing

9.5 Verifying Queuing Operation

- 9.5.1 Verifying queuing operation

- 9.5.2 Queuing comparison summary
- 9.6 Optimizing traffic flow with data compression
 - 9.6.1 Implementing compression overview
 - 9.6.2 Link compression over a point-to-point connection
 - 9.6.3 Payload compression
 - 9.6.4 TCP/IP header compression
 - 9.6.5 Implementing MPPC
 - 9.6.6 Other compression considerations
- 9.7 Configuring Data Compression
 - 9.7.1 Configuring compression
- 9.8 Lab Exercises
 - 9.8.1 Lab: Weighted Fair Queuing
 - 9.8.2 Lab: Priority Queuing
 - 9.8.3 Lab: Custom Queuing
- Summary

Module 10. Scaling IP Addressing with NAT

Overview

10.1 NAT Overview

- 10.1.1 NAT terminology
- 10.1.2 Private addressing
- 10.1.3 NAT terminology
- 10.1.4 NAT functions

10.2 Configuring NAT

- 10.2.1 Dynamic NAT
- 10.2.2 Configuring dynamic NAT
- 10.2.3 Dynamic NAT configuration example
- 10.2.4 Static NAT
- 10.2.5 Configuring static NAT
- 10.2.6 NAT overload
- 10.2.7 Configuring NAT overload
- 10.2.8 TCP load distribution
- 10.2.9 Configuring TCP load distribution
- 10.2.10 TCP load distribution example
- 10.2.11 Overlapping networks

10.3 Verifying NAT Configuration

- 10.3.1 Verifying NAT translations
- 10.3.2 Troubleshooting NAT translations
- 10.3.3 Clearing NAT translations
- 10.4 NAT Considerations
 - 10.4.1 NAT advantages
 - 10.4.2 NAT disadvantages
 - 10.4.3 Traffic types supported by Cisco
- 10.5 Lab Exercises
 - 10.5.1 Lab: Configuring static NAT
 - 10.5.2 Lab: Configuring dynamic NAT
 - 10.5.3 Lab: Configuring NAT overload
 - 10.5.4 Lab: Configuring TCP load distribution
- Summary

Module 11. Using AAA Scale Access Control

Overview

11.1 Introduction to AAA

- 11.1.1 Introduction to AAA
- 11.1.2 Security protocols
- 11.1.3 TACACS+
- 11.1.4 Radius
- 11.1.5 Cisco Secure Access Control Server

11.2 Configuring AAA

- 11.2.1 The aaa new-model command
- 11.2.2 Configuring TACACS+ and RADIUS clients
- 11.2.3 Configuring AAA authentication
- 11.2.4 Configuring login authentication
- 11.2.5 Enabling password protection at the privileged level
- 11.2.6 Configuring PPP authentication using AAA
- 11.2.7 Configuring AAA authorization
- 11.2.8 IOS command privileged levels
- 11.2.9 Configuring command authorization

11.3 Lab Exercises

- 11.3.1 Lab: Router security and AAA authentication
- 11.3.2 Lab: AAA authorization and accounting
- 11.3.3 Lab: AAA TACACS+ server

Summary

Module 12. Broadband Connections

Overview

12.1 Broadband Overview

- 12.1.1 Why broadband?
- 12.1.2 Cable options
- 12.1.3 DSL options
- 12.1.4 Satellite options
- 12.1.5 Wireless options

12.2 Cable Technology

- 12.2.1 The original cable plant
- 12.2.2 Data over cable - Why fiber?
- 12.2.3 Data over cable - How a cable system works
- 12.2.4 Data over cable - Cable system components
- 12.2.5 Hybrid Fiber Coaxial (HFC) architecture
- 12.2.6 Digital Signals over RF Channels (EM Spectrum)
- 12.2.7 Digital Signals over RF Channels (DOCSIS)
- 12.2.8 Identifying cable technology terms, standards, RF signaling terms
- 12.2.9 Putting cable technology together
- 12.2.10 How a cable modem initializes
- 12.2.11 Configuration of a router with a cable modem

12.3 DSL Technology

- 12.3.1 What is DSL?
- 12.3.2 Types of DSL
- 12.3.3 DSL limitations
- 12.3.4 ADSL
- 12.3.5 ADSL and POTS coexistence
- 12.3.6 ADSL channels and encoding
- 12.3.7 Data over ADSL: Bridging
- 12.3.8 PPP over Ethernet
- 12.3.9 How PPPoE works
- 12.3.10 Data over ADSL: PPPoA

12.4 Configuring the CPE as the PPPoE Client

- 12.4.1 Configuration tasks for DSL
- 12.4.2 Configure PPPoE in a VPDN group

- 12.4.3 Configure a PPPoE client
- 12.4.4 Configure the PPPoE DSL dialer interface
- 12.4.5 Configuring PAT
- 12.4.6 PAT for use with DSL example
- 12.4.7 Configure a DHCP server
- 12.4.8 Configuring a static route
- 12.4.9 PPPoE sample configuration
- 12.5 Configuring DSL with PPPoA
 - 12.5.1 Configuration tasks for PPPoA DSL
 - 12.5.2 DSL Modulation configuration
 - 12.5.3 Configure the DSL ATM interface
 - 12.5.4 Configure the DSL dialer interface
 - 12.5.5 Configuring PAT
 - 12.5.6 PAT configuration example
 - 12.5.7 Configure a DHCP server
 - 12.5.8 Configuring a static route
 - 12.5.9 Sample PPPoA configuration
- 12.6 Troubleshooting DSL
 - 12.6.1 Is the 827 trained to the DSLAM?
 - 12.6.2 Layer 1 issues
 - 12.6.3 Is the ATM interface in an administratively down state?
 - 12.6.4 Is the correct power supply being used?
 - 12.6.5 Is the DSL operating mode correct?
 - 12.6.6 Layer 2 Issues -- Correct PVC values
 - 12.6.7 Is data being received from the ISP?
 - 12.6.8 Is PPP negotiating properly?
- 12.7 Lab Exercise
 - 12.7.1 DSL e-Lab

Summary

Module 13. Virtual Private Networks

Overview

- 13.1 VPN Overview: Types, Tunnels, and Terms
 - 13.1.1 Virtual private networks
 - 13.1.2 Why have VPNs?
 - 13.1.3 VPN tunnels and encryption

- 13.1.4 VPN usage scenarios
- 13.1.5 VPN types
- 13.1.6 Selecting VPN Technologies: Encryption and tunneling protocols)
- 13.1.7 VPN protocols
- 13.1.8 Selecting Layer 3 VPN tunnel options
- 13.1.9 Identifying VPN and IPSec terms
- 13.2 Cisco IOS Cryptosystem Overview
 - 13.2.1 Cryptosystem overview
 - 13.2.2 Symmetric encryption
 - 13.2.3 Asymmetric encryption
 - 13.2.4 Key Exchange - Diffie Hellman
 - 13.2.5 Hashing
- 13.3 IPSec Technologies
 - 13.3.1 IPSec
 - 13.3.2 Tunnel versus transport mode
 - 13.3.3 Security association
 - 13.3.4 Five steps of IPSec
 - 13.3.5 How IPSec uses IKE
 - 13.3.6 IKE and IPSec flowchart
 - 13.3.7 Tasks to configure IPSec
- 13.4 Task 1: Prepare for IKE and IPSec
 - 13.4.1 Task 1 -- Prepare for IKE and IPSec
 - 13.4.2 Step 1 - Determine IKE (IKE Phase 1) policy
 - 13.4.3 IKE Phase 1 policy parameters
 - 13.4.4 Determine IPSec (IKE Phase 2) policy
 - 13.4.5 IPSec Transforms supported in Cisco IOS software
 - 13.4.6 IPSec policy example
 - 13.4.7 Identify IPSec peers
 - 13.4.8 Step 3 - Check current configuration
 - 13.4.9 Step 4 - Ensure the network works
 - 13.4.10 Step 5 - Ensure access lists are compatible with IPSec
- 13.5 Task 2: Configure IKE
 - 13.5.1 Task 2 - Configure IKE
 - 13.5.2 Step 1 - Enable IKE
 - 13.5.3 Step 2 - Create IKE policies

- 13.5.4 Create IKE policies with crypto isakmp command
- 13.5.5 IKE policy negotiation
- 13.5.6 Step 3 - Configure ISAKMP identity
- 13.5.7 Step 3 - Configure Pre-Shared keys
- 13.5.8 Step 4 - Verify IKE configuration
- 13.6 Task 3: Configure IPSec
 - 13.6.1 Task 3 - Configure IPSec
 - 13.6.2 Step 1 - Configure transform set suites
 - 13.6.3 Transform set negotiation
 - 13.6.4 Step 2 - Configure global IPSec security association Lifetimes
 - 13.6.5 Step 3 - Purpose of crypto access lists
 - 13.6.6 Step 3 - Create crypto ACLs using extended access lists
 - 13.6.7 Configure symmetrical peer crypto access lists
 - 13.6.8 Step 4 - purpose of crypto maps
 - 13.6.9 Crypto map parameters
 - 13.6.10 Step 4 - Configure IPSec crypto maps
 - 13.6.11 Example crypto map commands
 - 13.6.12 Step 5 - Apply crypto maps to interfaces
 - 13.6.13 IPSec configuration examples
- 13.7 Task 4: Test and Verify IPSec
 - 13.7.1 Task 4 - Test and verify IPSec
 - 13.7.2 The show crypto isakmp policy command
 - 13.7.3 The show crypto ipsec transform-set
 - 13.7.4 The show crypto ipsec sa command
 - 13.7.5 The show crypto map command
 - 13.7.6 The debug crypto commands
 - 13.7.7 Crypto system error messages for ISAKMP
- 13.8 Lab Exercise
 - 13.8.1 Configuring a site-to-site IPSec VPN using pre-shared keys

Summary

Case Study: Remote Access