



Course Title: Accessing the WAN v4.0

Duration: 40 hours

Course Overview

The primary focus of this course is on accessing wide area networks (WAN). The goal is to develop an understanding of various WAN technologies to connect small- to medium-sized business networks.

The course introduces WAN converged applications and quality of service (QoS). It focuses on WAN technologies including PPP, Frame Relay, and broadband links. WAN security concepts are discussed in detail, including types of threats, how to analyze network vulnerabilities, general methods for mitigating common security threats and types of security appliances and applications. The course then explains the principles of traffic control and access control lists (ACLs) and describes how to implement IP addressing services for an Enterprise network, including how to configure NAT and DHCP. IPv6 addressing concepts are also discussed. During the course, you will learn how to use Cisco Router and Security Device Manager (SDM) to secure a router and implement IP addressing services. Finally, students learn how to detect, troubleshoot and correct common Enterprise network implementation issues.

The labs and Packet Tracer activities used in this course are designed to help you develop an understanding of how to configure routing operations while reinforcing the concepts learned in each chapter.

Chapter 1 Introduction to WANs -

In Chapter 1, you will learn the fundamentals enterprise WANs, the technologies available to implement them, and the terminology used to discuss them. You will learn how the Cisco enterprise architecture provides integrated services over an enterprise network and how to select the appropriate WAN technology to meet different enterprise business requirements.

Chapter 2 PPP -

Chapter 2 focuses on serial point-to-point communications and the Point-to-Point Protocol (PPP). Understanding how point-to-point communication links function to provide access to a WAN is important to an overall understanding of how WANs function. Various aspects of PPP are discussed including securing PPP using either Password Authentication Protocol (PAP) or the more effective Challenge Handshake Authentication Protocol (CHAP).

Chapter 3 Frame Relay -

Chapter 3 focuses on the high-performance Frame Relay WAN protocol. You will learn how to implement Frame Relay for use between LANs over a WAN.

Chapter 4 Network Security -

Chapter 4 introduces network security which has moved to the forefront of network management and implementation. The overall security challenge is to find a balance between two important requirements: the need to open networks to support evolving business opportunities, and the need to protect private, personal, and strategic business information. You will learn to identify security threats to enterprise networks and mitigation techniques. You will also learn how to configure basic router security, disable unused resources and interfaces. Finally you will learn to manage configurations and IOS files.

Chapter 5 ACLs -

Chapter 5 builds on the concepts introduced in Chapter 4 and focuses on the application of ACLs. One of the most important skills a network administrator needs is mastery of access control lists (ACLs). You will learn how to create firewalls using standard and extended ACLs. Finally, you learn about advanced ACL features including dynamic, reflexive and timed ACLs.

Chapter 6 Teleworker Services -

Chapter 6 discusses broadband technologies from a telecommuter's perspective. Specifically, you will learn about cable, DSL, and wireless broadband options. You will also explore how VPNs are utilized to secure broadband connections.

Chapter 7 IP Addressing Services -

Chapter 7 discusses how a branch site can provide IP addressing services to users. You will identify teleworker requirements and recommend architectures for providing teleworking services. Specifically, you will learn how to configure a router to be a Dynamic Host Configuration Protocol (DHCP) server and how to integrate private addresses and Network Address Translation (NAT). You will finish with an overview of IPv6 and how to configure routers to exchange IPv6 routes using RIPng.

Chapter 8 Network Troubleshooting -

Chapter 8 is the capstone chapter for this course. You will learn how to establish a network baseline and develop network documentation to help in network troubleshooting. You will also develop your network troubleshooting skills by reviewing troubleshooting methodology. You will learn to identify and troubleshoot common enterprise network implementation issues using a layered model approach.