

CCENT Study Guide 5

Section 9.5 Troubleshooting Layer 4 and Upper Layer Services

As you work through this troubleshooting section, you can review the material necessary to prepare you to obtain a CCENT certification. To obtain a CCENT certification, you must pass the 640-822 ICND1 examination. These study guides provide a method to organize your review based on the ICND1 exam objectives.

Network Protocols and Services

Objective: Describe Common Networking Applications, Including Web Applications

Discovery 1 Review Chapters:

Network Services: In this chapter, the common network client/server applications are described. The chapter provides the protocol used, the port assigned to the application, and information about the client functionality for each of the network applications. Be sure to memorize the default TCP or UDP port assigned to each application because it is important for troubleshooting and for creating firewall filter lists.

Discovery 2 Review Chapters:

ISP Services: The section Services and Protocols discusses the different Application Layer services provided by ISPs and contains information about the various protocols used to provide these services. There is more detail in this section than in the material in Discovery 1 on how FTP and email services work.

ISP Responsibility: Methods to secure the common application layer protocols are described in the **Data Encryption** topic.

Objective: Troubleshoot DNS Operation

Discovery 1 Review Chapters:

Network Services: The operation of the Domain Name System is described in topic **Domain Name Service (DNS)**. Without successful DNS resolution of a domain name or URL, no communication can occur. Pay close attention to what must be operational in order for name resolution to occur: 1. There must be a correctly configured DNS server address on the host, configured manually or through DHCP, 2. The DNS server must be reachable from the host, and 3. The DNS server must be configured to resolve the specific destination host name to a valid IP address. Practice how to use nslookup to verify that DNS is functioning correctly on the network.

Troubleshooting Your Network: The topic **Troubleshooting Using Nslookup** describes how to interpret the output of the nslookup command on a Windows PC.

Discovery 2 Review Chapters:

ISP Services: The section **Domain Name System** provides detailed information on the structure of a DNS system and the various components that must function properly for name resolution to be successful. DNS failures cause all of the end user applications that rely on name resolution to fail. It is important to always check DNS availability and functionality when users report the failure of multiple network applications.

Objective: Describe the Impact of Applications (Voice over IP and Video over IP) on a Network

Discovery 1 Review Chapters:

Network Services: In the section *Client/Servers and Their Interaction* the topic *TCP and UDP Transport Protocols* explains why TCP is not a good choice for the transmission of voice and video traffic over the network. The topic *Voice Clients and Servers* describes the functionality of Internet IP Telephony.

Discovery 2 Review Chapters:

ISP Services: The different characteristics of TCP and UDP are described in the topic *Transport Layer Protocols* within the *Protocols that Support ISP Services* section.

Practice Activities:

1. Create a chart listing all of the common network and Internet applications. For each application, list the protocol, default port assignment and whether or not the application uses TCP or UDP. In some cases, such as voice or video, the port may not be known.

Example:

Application	Application Protocol	Port	Transport Protocol
Web Browser	http	80	TCP
Domain Name Lookup	Dns	53	TCP and UDP

2. Identify all of the client applications that are installed on your computer. Determine what type of server each connects to for information.
3. Use the netstat command to see how many TCP connections are initialized when you view a web page or send an email.

Network Security Practices and Devices

Objective: Explain Today's Increasing Network Security Threats and the Need to Implement a Comprehensive Security Policy to Mitigate the Threats

Discovery 1 Review Chapters:

Basic Security: The first three sections in this chapter outline the threats, methods of attack and security policy requirements for home and small business networks. The topic **Common Security Measures** explains the necessity for a comprehensive security policy and what the policy should contain. Be sure to review the material in contained in the interactive graphic associated with this topic.

Discovery 2 Review Chapters:

ISP Responsibility: Denial of service attacks are described in the **Access Control Lists and Port Filtering** topic. Measures to take to mitigate threats to host devices are contained in the **Host Security** topic.

Objective: Explain General Methods to Mitigate Common Security Threats to Network Devices, Hosts, and Applications

Discovery 1 Review Chapters:

Basic Security: The **Security Policy** section of this chapter outlines the recommended security measures to take to prevent many unwanted or malicious attacks on the hosts or network. Pay attention to which type of preventive measure is directed at which type of attack.

Discovery 2 Review Chapters:

ISP Responsibility: Security best practices and the common security issues facing ISPs and their customers are the focus of the first section of this chapter, **ISP Security Considerations**.

Objective: Describe the Functions of Common Security Appliances and Applications

Discovery 1 Review Chapters:

Basic Security: Firewalls and port filtering are introduced in the **Using Firewalls** section. The different methods that firewalls use to determine what traffic is permitted or denied are listed. The animation in the topic **Using a Firewall** illustrates the concept of different security zones. This topic also includes a lab to practice configuring firewall settings.

Discovery 2 Review Chapters:

ISP Responsibility: The section **Security Tools** describes the various types of security technologies used in networks and the types of threats each protects against. Ensuring the security of a network is one of the most important tasks a network technician or engineer performs. Be certain that you understand the function of each type of security measure in detail. The types of security measures necessary to secure wireless LANs are discussed in the **Wireless Security** topic.

Objective: Describe Security Recommended Practices, Including Initial Steps to Secure Network Devices

Discovery 1 Review Chapters:

Wireless Technologies: The section *Security Considerations on a Wireless LAN* contains information on how to secure a wireless access point.

Discovery 2 Review Chapters:

Configuring Network Devices: The topic *Basic Configuration*, in the *Configuring a Router using IOS CLI* describes how to set passwords for access to the user and privileged modes. It also includes the commands to permit Telnet access to the device and set the VTY (Telnet) access login password. Encrypting of all passwords on a device is recommended using the service password-encryption function. The commands to set passwords and banners are the same on a Cisco switch as on the ISR router. Additional security measures necessary on a switch are outlined in topic *Connecting the LAN Switch to the Router*.

Practice Activities:

1. Create a checklist to follow to set basic security on each of the major networking devices: Router, switch, integrated wireless access point. Practice configuring basic security on each of the devices.
2. Create a chart of each of the major network security technologies: firewalls, access lists, IPS, IDS, logging services, authentication, authorization, and encryption methods. Describe the function of each technology and which threats each protects against. Indicate which technologies are host-based and which are implemented on network devices or on network appliances.

Example:

Security Technology	Function	Threat Protection	Host-based	Network-based
Access Lists	Filters traffic based on source or destination address or port.	Prevents unwanted traffic into a network or host process.	Yes	Yes
Virus Protection	Identifies malicious software by traffic pattern or file content	Prevents malicious software from causing damage to host files or creating excess network traffic.	Yes	No

3. List the topics that should be included in a security policy.
4. List best practices for securing networks and hosts.