Module Practice and Quiz

17.0.1

Lab - Design and Build a Small Business Network

Skills Practice Opportunity

You have the opportunity to practice designing and building a network from scratch. Your design must include a minimum of one Cisco 4321 router, two Cisco 2960 switches, and two PCs. Fully configure the network and use IPv4 or IPv6 (subnetting must be included as a part of your addressing scheme). Verify the network using at least five **show** commands. Secure the network using SSH, secure passwords, and console passwords (minimum).

You can practice these skills using the Packet Tracer or lab equipment, if available.

Packet Tracer - Physical Mode (PTPM)

Design and Build a Small Network - Physical Mode

Design and Build a Small Network - Physical Mode

Lab Equipment

Design and Build a Small Network

17.0.2

Packet Tracer - Skills Integration Challenge

In this Packet Tracer activity, you will use all the skills you have acquired over throughout this course.

Skills Integration Challenge

Skills Integration Challenge

17.0.3

Packet Tracer - Troubleshooting Challenge

In this Packet Tracer activity, you will troubleshoot and resolve a number of issues in an existing network.

Troubleshooting Challenge

Troubleshooting Challenge

17.0.4

What did I learn in this module?

Devices in a Small Network

Small networks typically have a single WAN connection provided by DSL, cable, or an Ethernet connection. Small networks are managed by a local IT technician or by a contracted professional. Factors to consider when selecting network devices for a small network are cost, speed and types of ports/interfaces, expandability, and OS features and services. When implementing a network, create an IP addressing scheme and use it on end devices, servers and peripherals, and intermediary devices. Redundancy can be accomplished by installing duplicate equipment, but it can also be accomplished by supplying duplicate network links for critical areas. The routers and switches in a small network should be configured to support real-time traffic, such as voice and video, in an appropriate manner relative to other data traffic. In fact, a good network design will implement quality of service (QoS) to classify traffic carefully according to priority.

Small Network Applications and Protocols

There are two forms of software programs or processes that provide access to the network: network applications and application layer services. Some end-user applications implement application layer protocols and are able to communicate directly with the lower layers of the protocol stack. Email clients and web browsers are examples of this type of application. Other programs may need the assistance of application layer services to use network resources like file transfer or network print spooling. These are the programs that interface with the network and prepare the data for transfer. The two most common remote access solutions are Telnet and Secure Shell (SSH). SSH service is a secure alternative to Telnet. Network administrators must also support common network servers and their required related network protocols such as web server, email server, FTP server, DHCP server, and DNS server. Businesses today are increasingly using IP telephony and streaming media to communicate with customers and business partners. These are real-time applications. The network infrastructure must support VoIP, IP telephony, and other real-time applications.

Scale to Larger Networks

To scale a network, several elements are required: network documentation, device inventory, budget, and traffic analysis. Know the type of traffic that is crossing the network as well as the current traffic flow. Capture traffic during peak utilization times to get a good representation of the different traffic types and perform the capture on different network segments and devices as some traffic will be local to a particular segment. Network administrators must know how network use is changing. Usage details of employee computers can be captured in a 'snapshot' with such tools as the Windows Task Manager, Event Viewer, and Data Usage.

Verify Connectivity

The **ping** command is the most effective way to quickly test Layer 3 connectivity between a source and destination IP address. The command also displays various round-trip time statistics. The Cisco IOS offers an "extended" mode of the ping command which lets the user create special types of pings by adjusting parameters related to the command operation. Extended ping is entered in privileged EXEC mode by typing ping without a destination IP address. Traceroute can help locate Layer 3 problem areas in a network. A trace returns a list of hops as a packet is routed through a network. It is used to identify the point along the path where the problem can be found. In Windows, the command is **tracert**. In Cisco IOS the command is **traceroute**. There is also an extended **traceroute** command. It allows the administrator to adjust parameters related to the command operation. The output derived from network commands contributes data to the network baseline. One method for starting a baseline is to copy and paste the results from an executed ping, trace, or other relevant commands into a text file. These text files can be time stamped with the date and saved into an archive for later retrieval and comparison.

Host and IOS Commands

Network administrators view the IP addressing information (address, mask, router, and DNS) on a Windows host by issuing the **ipconfig** command. Other necessary commands are **ipconfig /all**, **ipconfig /release** and **ipconfig /renew**, and **ipconfig /displaydns**. Verifying IP settings by using the GUI on a Linux machine will differ depending on the Linux distribution (distro) and desktop interface. Necessary commands are **ifconfig**, and **ip address**. In the GUI of a Mac host, open Network Preferences > Advanced to get the IP addressing information. Other IP addressing commands for Mac are **ifconfig**, and **networksetup -listallnetworkservices** and **networksetup -getinfo** *<network service>*. The **arp** command is executed from the Windows, Linux, or Mac command prompt. The command lists all devices currently in the ARP cache of the host, which includes the IPv4 address, physical address, and the type of addressing (static/dynamic), for each device. The **arp -a** command displays the known IP address and MAC address binding. Common **show** commands are **show running-config**, **show interfaces**, **show ip address**, **show arp**, **show ip route**, **show protocols**, and **show version**. The **show cdp neighbor** command provides the following information about each CDP neighbor device: Identifiers, address list, port identifier, capabilities list, and platform. The **show cdp neighbors detail** command will help determine if one of the CDP neighbors has an IP configuration error. The **show ip interface brief** command output displays all interfaces on the router, the IP address assigned to each interface, if any, and the operational status of the interface.

Troubleshooting Methodologies

Step 1. Identify the problem

Step 2. Establish a theory of probably causes.

Step 3. Test the theory to determine the cause.

Step 4. Establish a plan of action and implement the solution.

Step 5. Verify the solution and implement preventive measures.

Step 6. Document findings, actions, and outcomes.

A problem should be escalated when it requires a the decision of a manager, some specific expertise, or network access level unavailable to the troubleshooting technician. OS processes, protocols, mechanisms and events generate messages to communicate their status. The IOS **debug** command allows the administrator to display these messages in real-time for analysis. To display log messages on a terminal (virtual console), use the **terminal monitor** privileged EXEC command.

Troubleshooting Scenarios

There are two duplex communication modes: half-duplex and full-duplex. If one of the two connected devices is operating in full-duplex and the other is operating in half-duplex, a duplex mismatch occurs. While data communication will occur through a link with a duplex mismatch, link performance will be very poor.

Wrongly assigned IP addresses create a variety of issues, including IP address conflicts and routing problems. Two common causes of incorrect IPv4 assignment are manual assignment mistakes or DHCP-related issues. Most end devices are configured to rely on a DHCP server for automatic IPv4 address assignment. If the device is unable to communicate with the DHCP server, then the server cannot assign an IPv4 address for the specific network and the device will not be able to communicate.

The default gateway for an end device is the closest networking device that can forward traffic to other networks. If a device has an incorrect or nonexistent default gateway address, it will not be able to communicate with devices in remote networks. Because the default gateway is the path to remote networks, its address must belong to the same network as the end device.

DNS failures often lead the user to conclude that the network is down. If a user types in a domain name such as www.cisco.com in a web browser and the DNS server is unreachable, the name will not be translated into an IP address and the website will not display.

17.0.5

Module Quiz - Build a Small Network

1. Which network design consideration would be more important to a large corporation than to a small business?
   - low port density switch
   - **redundancy**
   - internet router
   - firewall

2. A newly hired network technician is given the task of ordering new hardware for a small business with a large growth forecast. Which primary factor should the technician be concerned with when choosing the new devices?
   - devices that have support for network monitoring
   - redundant devices
   - **devices with support for modularity**
   - devices with a fixed number and type of interfaces

3. What type of traffic would most likely have the highest priority through the network?
   - instant messaging
   - **voice**
   - SNMP
   - FTP

4. A network technician is investigating network connectivity from a PC to a remote host with the address 10.1.1.5. Which command, when issued on a Windows PC, will display the path to the remote host?
   - **traceroute 10.1.1.5**
   - **tracert 10.1.1.5**
   - **ping 10.1.1.5**
   - **trace 10.1.1.5**

5. A user is unable to reach the website when typing **http://www.cisco.com** in a web browser, but can reach the same site by typing **http://72.163.4.161**. What is the issue?
   - TCP/IP protocol stack
   - **DNS**
   - default gateway
   - DHCP

6. Where are Cisco IOS debug output messages sent by default?
   - **console line**
   - Syslog server
   - memory buffers
   - vty lines

7. Which element of scaling a network involves identifying the physical and logical topologies?
   - traffic analysis
   - device inventory
   - **network documentation**
   - cost analysis

8. What mechanism can be implemented in a small network to help minimize network latency for real-time streaming applications?
   - AAA
   - ICMP
   - PoE
   - **QoS**

9. Which process failed if a computer cannot access the internet and received an IP address of 169.254.142.57?
   - DNS
   - **DHCP**
   - IP
   - HTTP

10. A small company has only one router as the exit point to its ISP. Which solution could be adopted to maintain connectivity if the router itself, or its connection to the ISP, fails?
    - Purchase a second least-cost link from another ISP to connect to this router.
    - Add more interfaces to the router that is connected to the internal network.
    - Activate another router interface that is connected to the ISP, so the traffic can flow through it.
    - **Have a second router that is connected to another ISP.**

11. When should an administrator establish a network baseline?
    - when the traffic is at peak in the network
    - when there is a sudden drop in traffic
    - at the lowest point of traffic in the network
    - **at regular intervals over a period of time**

12. Which two traffic types require delay sensitive delivery? (Choose two.)
    - [ ] email
    - [x] voice
    - [ ] FTP
    - [x] video
    - [ ] web

13. A network technician suspects that a particular network connection between two Cisco switches is having a duplex mismatch. Which command would the technician use to see the Layer 1 and Layer 2 details of a switch port?
    - **show running-config**
    - **show interfaces**
    - **show ip interface brief**
    - **show mac-address-table**

14. Which statement is true about CDP on a Cisco device?
    - Because it runs at the data link layer, the CDP protocol can only be implemented in switches.
    - To disable CDP globally, the **no cdp enable** command in interface configuration mode must be used.
    - **CDP can be disabled globally or on a specific interface.**
    - The **show cdp neighbor detail** command will reveal the IP address of a neighbor only if there is Layer 3 connectivity.

15. What factor should be considered in the design of a small network when devices are being chosen?
    - traffic analysis
    - ISP
    - redundancy
    - **cost of devices**

Check

Show Me

Reset