Module Practice and Quiz

12.6.1

Packet Tracer - Troubleshooting Challenge - Document the Network

In this Packet Tracer activity, you will document a network that is unknown to you.

- Test network connectivity.
- Compile host addressing information.
- Remotely access default gateway devices.
- Document default gateway device configurations.
- Discover devices on the network.
- Draw the network topology.

Troubleshooting Challenge

Troubleshooting Challenge

12.6.2

Packet Tracer - Troubleshooting Challenge - Use Documentation to Solve Issues

In this Packet Tracer activity, you use network documentation to identify and fix network communications problems.

- Use various techniques and tools to identify connectivity issues.
- Use documentation to guide troubleshooting efforts.
- Identify specific network problems.
- Implement solutions to network communication problems.
- Verify network operation.

Troubleshooting Challenge

Troubleshooting Challenge

12.6.3

What did I learn in this module?

Network Documentation

Common network documentation includes: physical and logical network topologies, network device documentation recording all pertinent device information, and network performance baseline documentation. Information found on a physical topology typically includes the device name, device location (address, room number, rack location, etc.), Interface and ports used, and cable type. Network device documentation for a router may include the interface, IPv4 address, IPv6 address, MAC address and routing protocol. Network device documentation for a switch may include the port, access, VLAN, trunk, EtherChannel, native, and enabled. Network device documentation for end-systems may include device name, OS, services, MAC address, IPv4 and IPv6 addresses, default gateway, and DNS. A network baseline should answer the following questions:

- How does the network perform during a normal or average day?
- Where are the most errors occurring?
- What part of the network is most heavily used?
- What part of the network is least used?
- Which devices should be monitored and what alert thresholds should be set?
- Can the network meet the identified policies?

When conducting the initial baseline, start by selecting a few variables that represent the defined policies, such as interface utilization and CPU utilization. A logical network topology diagram can be useful in identifying key devices and ports to monitor. The length of time and the baseline information being gathered must be long enough to determine a "normal" picture of the network. When documenting the network, gather information directly from routers and switches using the **show**, **ping**, **traceroute**, and **telnet** commands.

Troubleshooting Process

The troubleshooting process should be guided by structured methods. One method is the seven-step troubleshooting process: 1. Define the problem, 2. Gather information, 3. Analyze information, 4. Eliminate possible causes, 5. Propose hypothesis, 6. Test hypothesis, and 7. Solve the problem. When talking to end users about their network problems, ask both open and closed-ended questions. Use the **show**, **ping**, **traceroute**, and **telnet** commands to gather information from devices. Use the layered models to perform bottom-up, top-down, or divide-and-conquer troubleshooting. Other models include follow-the-path, substitution, comparison, and educated guess. Software problems are often solved using a top-down approach while hardware-based problems are solved using the bottom-up approach. New problems may be solved by an experienced technician using the divide-and-conquer method.

Troubleshooting Tools

Common software troubleshooting tools include NMS tools, knowledge bases, and baselining tools. A protocol analyzer, such as Wireshark, decodes the various protocol layers in a recorded frame and presents this information in an easy to use format. Hardware troubleshooting tools include digital multimeters, cable testers, cable analyzers, portable network analyzers, and Cisco Prime NAM. Syslog server can also be used as a troubleshooting tool. Implementing a logging facility for network troubleshooting. Cisco devices can log information regarding configuration changes, ACL violations, interface status, and many other types of events. Event messages can be sent to one or more of the following: console, terminal lines, buffered logging, SNMP traps, and syslog. The lower the level number, the higher the severity level. The **logging trap** level command limits messages logged to the syslog server based on severity. The level is the name or number of the severity level. Only messages equal to or numerically lower than the specified level are logged.

Symptoms and Causes of Network Problems

Failures and suboptimal conditions at the physical layer usually cause networks to shut down. Network administrators must have the ability to effectively isolate and correct problems at this layer. Symptoms include performance lower than baseline, loss of connectivity, congestion, high CPU utilization, and console error messages. The causes are usually power-related, hardware faults, cabling faults, attenuation, noise, interface configuration errors, exceeding component design limits, and CPU overload.

Data link layer problems cause specific symptoms that, when recognized, will help identify the problem quickly. Symptoms include no functionality/connectivity at Layer 2 or above, network operating below baseline levels, excessive broadcasts, and console messages. The causes are usually encapsulation errors, address mapping errors, framing errors, and STP failures or loops.

Network layer problems include any problem that involves a Layer 3 protocol, both routed protocols (such as IPv4 or IPv6) and routing protocols (such as EIGRP, OSPF, etc.). Symptoms include network failure and suboptimal performance. The causes are usually general network issues, connectivity issues, routing table problems, neighbor issues, and the topology database.

Transport layer problems can arise from transport layer problems on the router, particularly at the edge of the network where traffic is examined and modified. Symptoms include connectivity and access issues. Causes are likely to be misconfigured NAT or ACLs. ACL misconfigurations commonly occur at the selection of traffic flow, order of access control entries, implicit deny any, addresses and IPv4 wildcard masks, selection of transport layer protocol, source and destination ports, use of the established keyword, and uncommon protocols. There are several problems with NAT including misconfigured NAT inside, NAT outside, or ACL. Common interoperability areas with NAT include BOOTP and DHCP, DNS, SNMP, and tunneling and encryption protocols.

Application layer problems can result in unreachable or unusable resources when the physical, data link, network, and transport layers are functional. It is possible to have full network connectivity, but the application simply cannot provide data. Another type of problem at the application layer occurs when the physical, data link, network, and transport layers are functional, but the data transfer and requests for network services from a single network service or application do not meet the normal expectations of a user.

Troubleshooting IP Connectivity

Diagnosing and solving problems is an essential skill for network administrators. There is no single recipe for troubleshooting, and a problem can be diagnosed in many ways. However, by employing a structured approach to the troubleshooting process, an administrator can reduce the time it takes to diagnose and solve a problem.

End-to-end connectivity problems are usually what initiates a troubleshooting effort. Two of the most common utilities used to verify a problem with end-to-end connectivity are **ping** and **traceroute**. The **ping** command uses a Layer 3 protocol that is a part of the TCP/IP suite called ICMP. The **traceroute** command is commonly performed when the **ping** command fails.

Step 1. Verify the physical layer. The most commonly used Cisco IOS commands for this purpose are **show processes cpu**, **show memory**, and **show interfaces**.

Step 2. Check for duplex mismatches. Another common cause for interface errors is a mismatched duplex mode between two ends of an Ethernet link. In many Ethernet-based networks, point-to-point connections are now the norm, and the use of hubs and the associated half-duplex operation is becoming less common. Use the **show interfaces** *interface* command to diagnose this problem.

Step 3. Verify addressing on the local network. When troubleshooting end-to-end connectivity, it is useful to verify mappings between destination IP addresses and Layer 2 Ethernet addresses on individual segments. The **arp** Windows command displays and modifies entries in the ARP cache that are used to store IPv4 addresses and their resolved Ethernet physical (MAC) addresses. The **netsh interface ipv6 show neighbor** Windows command output lists all devices that are currently in the neighbor table. The **show ipv6 neighbors** command output displays an example of the neighbor table on the Cisco IOS router. Use the **show mac address-table** command to display the MAC address table on the switch.

VLAN assignment is another issue to consider when troubleshooting end-to-end connectivity. Use the **arp** Windows command to see the entry for a default gateway. Use the **show mac address-table** command to check the switch MAC table. This may show that not a VLAN assignments are correct.

Step 4. Verify the default gateway. The command output of the **show ip route** Cisco IOS command is used to verify the default gateway of a router. On a Windows *host*, the **route print** Windows command is used to verify the presence of the IPv4 default gateway.

In IPv6, the default gateway can be configured manually, using stateless autoconfiguration (SLAAC), or by using DHCPv6. The **show ipv6 route** Cisco IOS command is used to check for the IPv6 default route on a router. The **ipconfig** Windows command is used to verify if a PC1 has an IPv6 default gateway. The command output of the **show ipv6 interface** *interface* will tell you if a router is or is not enabled as an IPv6 router. Enable a router as an IPv6 router using the **ipv6 unicast-routing** command. To verify that a host has the default gateway set, use the **ipconfig** command on the Microsoft Windows PC or the **ifconfig** command on Linux and Mac OS X.

Step 5. Verify correct path. The routers in the path make the routing decision based on information in the routing tables. Use the **show ip route** | **begin Gateway** command for an IPv4 routing table. Use the **show ipv6 route** command for an IPv6 routing table.

Step 6. Verify the transport layer. Two of the most common issues that affect transport layer connectivity include ACL configurations and NAT configurations. A common tool for testing transport layer functionality is the Telnet utility.

Step 7. Verify ACLs. Use the **show ip access-lists** command to display the contents of all IPv4 ACLs and the **show ipv6 access-list** command to show the contents of all IPv6 ACLs configured on a router. Verify which interface has the ACL applied using the **show ip interfaces** command.

Step 8. Verify DNS. To display the DNS configuration information on the switch or router, use the **show running-config** command. Use the **ip host** command to enter name to IPv4 mapping to the switch or router as shown in the command output.

12.6.4

Module Quiz - Network Troubleshooting

1. Which statement describes the physical topology for a LAN?
   - It depicts the addressing scheme that is employed in the LAN.
   - It defines how hosts and network devices connect to the LAN.
   - It describes whether the LAN is a broadcast or token-passing network.
   - It shows the order in which hosts access the network.

2. A network engineer is troubleshooting a network problem where users cannot access the FTP server at the same IP address where a website can be successfully accessed. Which troubleshooting method would be the best to apply in this case?
   - divide-and-conquer
   - bottom-up
   - comparing IP settings on user workstations
   - top-down

3. A computer technician performed a number of actions to correct a problem. Some actions did not solve the problem, but eventually a solution was found. What should be documented?
   - a description of the problem and solution
   - only the failed attempts, so that future technicians will know what not to try
   - only the solution, because this solved the problem
   - everything that was done to try to solve the problem

4. A network engineer is troubleshooting a network problem and can successfully ping between two devices. However, Telnet between the same two devices does not work. Which OSI layers should the administrator investigate next?
   - from the network layer to the physical layer
   - only the network layer
   - from the network layer to the application layer
   - all of the layers

5. While designing changes to a data center because of a new IoE implementation, a network administrator has the job of diagramming the new physical topology of the area. What should be included in the physical topology diagram?
   - the IP addressing scheme for all workstations in the company
   - cable locations and lengths between servers and switches
   - the service level agreement from the ISP
   - technical specifications of firewalls

6. A network technician is troubleshooting an email connection problem. Which question to the end-user will provide clear information to better define the problem?
   - What kind of equipment are you using to send emails?
   - How big are the emails you tried to send?
   - Is your email working now?
   - When did you first notice your email problem?

7. Which troubleshooting tool can be used to pinpoint the distance to a break in a network cable?
   - network analyzer
   - cable tester
   - digital multimeter
   - network analysis module

8. Which troubleshooting software is an example of a network management system tool?
   - CyberGauge
   - Wireshark
   - LANsurveyor
   - WhatsUp Gold

9. What is the purpose of establishing a network baseline?
   - to document and analyze the network traffic
   - to help monitor and troubleshoot network performance
   - to provide an inventory of network devices
   - to verify the configuration of routers and switches on the network

10. After which step in the network troubleshooting process would one of the layered troubleshooting methods be used?
    - documenting symptoms
    - narrowing the scope
    - gathering symptoms from suspect devices
    - determining ownership

11. A company is setting up a web site with SSL technology to protect the authentication credentials required to access the web site. A network engineer needs to verify that the setup is correct and that the authentication is indeed encrypted. Which tool should be used?
    - protocol analyzer
    - cable analyzer
    - baselining tool
    - fault-management tool

12. When should a network performance baseline be measured?
    - when a denial of service attack to the network is detected and blocked
    - after normal work hours to reduce possible interruptions
    - immediately after the main network devices restarted
    - during normal work hours of an organization

13. A networked PC is having trouble accessing the Internet, but can print to a local printer and ping other computers in the area. Other computers on the same network are not having any issues. What is the problem?
    - The default gateway router does not have a default route.
    - The link between the switch to which the PC connects and the default gateway router is down.
    - The PC has a missing or incorrect default gateway.
    - The switch port to which the PC connects has an incorrect VLAN configured.

14. A technician installed a network adapter in a computer and wants to test network connectivity. The **ping** command can receive responses from workstations on the same subnet but not from remote workstations. What could be causing the problem?
    - The NIC driver is out of date.
    - The default gateway is incorrect.
    - The TCP/IP protocol stack is not loaded.
    - The operating system is not compatible with the remote sites.

15. What network troubleshooting capability is provided by a cable analyzer?
    - discovering VLAN configuration and viewing switch interface details
    - testing and certifying of copper and fiber cables
    - measuring electrical values of voltage, current, and resistance
    - generating reports on traffic that is consuming critical network resources

Check

Show Me

Reset