



Lab 4.1.1 Isolating Physical and Data Link Layer Problems

Objective

Complete this lab to practice what you learned in this lesson. You will be given a problem situation escalated to Level 2 Support. You will analyze user feedback and end-system data, and use Cisco commands and applications to isolate the specific cause of any problems.

In this exercise, you will use a troubleshooting methodology and Cisco commands to isolate the specific causes of any network problems.

After completing this exercise, you will be able to:

- Analyze user feedback and end-system data to decide at which OSI layer to begin isolating problems
- Select the troubleshooting tools to use to isolate the specific causes of any network problems
- Develop a troubleshooting implementation plan for resolving any identified problems

Required Resources

These are the resources and equipment required to complete this exercise:

- A completed baseline topology diagram documenting the laboratory installation
- Network documentation recording the configuration of the laboratory installation

Scenario

You recently joined the Level 2 Network Support team for Acme. This evening you are on-call for network outages. You read the following during your review of the activity log:

Network Support Activity Log

Time	Log Entry
5:30 pm	One Acme user reported that access to the server seemed to be slower than usual. -- Help Desk -- [assigned to network operations]
6:01 pm	We checked and could ping the server. We scanned the configs on all the network devices. They look fine. -- 2 nd shift ops --
6:15 pm	Multiple users started reporting that they can no longer reach anything. - Help Desk -
6:37 pm	We can ping the core devices, but also noticed some network latency from the access router. Escalated to Level One Network Support. -- 2 nd shift ops -- [assigned to Mike]
6:52 pm	I asked network operations if anyone changed anything. They do not think they changed anything important. Not sure what they changed. -- Mike --
7:23 pm	I tried to fix up the configs to resolve the user access and resolve the network latency issues. I am not sure what to back out, but the issues are worse. -- Mike --
7:33 pm	Escalated to Level Two Network Support
7:47 pm	Checked Syslog server messages and noticed that the line protocol on interface port-channel 6 changed state to down from host 172.28.170.2

Command List

As you work through the case study, you may find the following list of commands helpful. The list includes router, switch, and PC commands. The commands used in this exercise should be familiar to you from previous experience or from prior Cisco courses.

Command	Description
ping { <i>host</i> <i>ip-address</i> }	(User or Extended) Sends an echo request packet to an address, then waits for a reply. The <i>host ip-address</i> variable is the IP alias or IP address of the target system
show cdp neighbors [detail]	Displays the device type, IP address, and Cisco IOS version of neighboring devices
show controllers { <i>type number</i> }	Displays current internal status information for the interface controller cards
show etherchannel summary	Displays EtherChannel port-channel summary status, including Layer 2 (L2) or Layer 3 (L3) port and interface information
show frame-relay map	Displays Frame Relay mapping status
show frame-relay pvc	Displays Frame Relay PVC information and status
show interfaces port-channel { <i>interface-number</i> }	Displays port-channel status, including L2 or L3 port and interface information
show interfaces trunk	Shows trunking interfaces
show ip interface brief	Displays a summary of the status of all interfaces on a device
show ip route	Displays IP routing table information
show protocols	Displays Layer 3 addresses and interface status
show running-config	Displays device configuration information
show running-config interface { <i>type number</i> }	Displays configuration information for one interface
show spanning-tree	Displays Spanning Tree Protocol (STP) information, including port status
show version	Displays the Cisco IOS software version and all installed hardware configurations
show vlan	Displays VLAN configurations on a device
show vtp status	Displays VLAN Trunking Protocol (VTP) status, including domain name and revision number
telnet { <i>host</i> <i>ip-address</i> }	Uses Telnet to connect to an IP address
trace [<i>destination</i>]	(User or Privileged) Identifies the path a packet takes through the network. The <i>destination</i> variable is the IP alias or IP address of the target system

Troubleshooting Log: Isolating Physical and Data Link Layer Problems

Problem	Solution
Core Router/Switch	
Distribution Router/Switch	
Access Router	
Access Switch	

Step 1

Where should you look to isolate the specific causes of any problems?

What commands might you use to look for issues?

Step 2

Coordinate with your workgroup to isolate the specific causes of any network problems you identified.

Step 3

On the Troubleshooting Log, document each identified network problem on a specific device. The Troubleshooting Log is divided into four possible areas of concern: core routing and switching, distribution routing, access routing, and access switching.

Step 4

Repeat Steps 1 and 2 as needed to isolate the specific causes of all problems.

Step 5

Develop a plan to correct the identified problems and document the plan in the space provided below.

Step 6

Assign the documented problems to members of your workgroup.

Step 7

Have the instructor review your Troubleshooting Log and correction plan.