



Lab 7.1.1 Isolating Problems at the Transport and Application Layers

Objective

Complete this lab to practice what you learned in this module. You are given a problem situation escalated to Level 2 Engineering. 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, the class will use a troubleshooting methodology and Cisco commands to isolate the specific causes of network problems. As a workgroup, complete the following steps:

- Analyze user-feedback and end-system data to decide at which OSI layer to begin isolating a problem
- Isolate the specific cause of any problems using Cisco tools
- Develop a plan for resolving problems

After completing this exercise, you will be able to:

- Analyze user-feedback and end-system data to decide 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

Scenario

After management realized the error of their ways and ordered we move the core routing protocol back to OSPF, you did as you were asked and finished cleaning up the migration mess this morning. The network now is running smoothly with OSPF in the core.

Andrew, the co-op student, asks your boss, Mike, if he can make a baseline of the Acme network for his networking class. Mike tells him this is okay, as long as the passwords are removed from the configurations before he brings them to class.

You went out to Broadway Pizza for lunch with the rest of the Level 2 team. You ordered a sausage roll. Then you receive a page:

"911. Ntwrk dn. Pls rtn. Adrw"

Network done? Network down? Anyway, you ask for your order to go, and drive back to the office.

"What did you do?" you ask Andrew.

"Well, I was just running some `show` commands to get a baseline for my class," he starts. "And I was starting to disguise the corporate passwords. And then Mike stopped by and asked me to implement OSPF authentication strictly in the core."

"Ok, then what?" you ask as you eat the last bite of your sausage roll.

"Well, I jumped right into the OSPF authentication implementation. While I was configuring OSPF, I tested a way to optimize the traffic throughout the network with our routing policy," Andrew stammered. "But then I found I couldn't reach the Internet from the core switch, so I backed out the optimizations."

Andrew continued, "Then MIS called, and said the users couldn't use TFTP to connect to the CCNP4 server. They asked me to check the DHCP configuration. It looked okay to me. Do we have a TFTP application running on the CCNP4 server?"

"No," you respond, "we do not."

"So I then tried to connect to the access router, but I couldn't get in. I asked the network administrators to reboot the network devices," Andrew said. "They did, but I think they first saved my changes. Then MIS and network operations really started calling because the users can't access anything on the Internet or on our corporate server."

Andrew adds, "I did try to back out my changes, but it is hard to concentrate with all those people yelling at me. I couldn't even log into most of the network devices."

He concludes, "So I sent you a page saying the network was down, and I hoped you would return soon."

You need to isolate the causes of each of the problems, and develop a plan for resolving them.

Required Resources

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

- Access to a protocol analyzer (either software or hardware)
- An *updated* network baseline documenting the laboratory installation
- *Updated* network documentation recording the configuration of the laboratory installation
- A troubleshooting log listing isolated physical, data link, or network layer problems

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.

Table 11: Helpful Commands

Command	Description
arp -a	Displays ARP information
debug ip dhcp server	Displays DHCP Server debugging
debug ip eigrp	Enables debugging of EIGRP events
debug ip ospf adj	Enables debugging of OSPF adjacencies
debug ip policy	Enables debugging of the IP policy
debug ip routing	Enables debugging of IP routing events
ipconfig /all	Displays IP information for the PC
ping {host address}	Pings an IP address
route print	Displays active routes for the PC
show access-lists	Displays access list information
show ip bgp	Displays entries in the BGP routing table
show ip bgp summary	Shows summary BGP status
show ip dhcp binding	Displays address bindings on the DHCP server
show ip dhcp server statistics	Displays DHCP server statistics
show ip interface brief	Displays brief form of interface information
show ip policy	Displays which route map is associated with which interface
show ip protocol interface	Displays interface information for a protocol.
show ip protocol neighbor	Displays information about neighbors for a specific routing protocol.
show ip protocols	Displays routing protocol status
show ip route	Displays IP routing table information
show route-map	Displays route map information
show spanning-tree vlan vlan-id	Displays Spanning Tree Protocol information including port status for a specific VLAN
show vlan vlan-id	Displays default and defined VLAN information
telnet {host ip-address}	Connects to an IP address via the Telnet application
tracert {ip-address}	Runs trace to an IP address
tracert {ip-address}	Runs trace from a PC to an IP address

Troubleshooting Log: Isolating Transport and Application 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 identified network problems for each device. The Troubleshooting Log is divided into four possible areas of concern: core routing and switching, distribution routing and switching, 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.

You have completed this activity when you attain these results:

- The problems that you discovered are documented in the troubleshooting log.
- You have isolated the specific causes of all network problems.
- Your workgroup has an implementation plan for correcting the isolated problems.