



### Lab 5.1.1 Isolating Network Layer Problems

#### Objective

Complete this lab to practice what you learned in this module. You will be given a problem situation that has been 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, you will use a troubleshooting methodology and Cisco commands to isolate the specific causes of any network problems. With other members of your workgroup, complete the following steps:

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

#### Scenario

You are part of the second-level network support team for Acme. This morning, the network support team for Acme implemented multipoint subinterfaces for the distribution layer routers in preparation for the eventual connection of additional access routers. Network support also implemented point-to-point subinterfaces on the access routers. You just received a page to check your email for details on a network outage that was escalated to Level 2 support. Your email displays the following activity log:

**Table 12: Network Support Activity Log**

Time	Log Entry
9:17 am	Acme Sales department reports they can no longer connect to anything. HTTP and ping are not working.
9:44 am	We updated some group parameters on the server for the Sales Department. We believe we have resolved the issue. [MIS]
9:53 am	Acme Sales is complaining about receiving network error messages about address conflicts. Other users are reporting that they can no longer reach anything via their browsers or Telnet sessions. [Joe is working on the problem.]
10:03 am	Network connectivity errors are reported by the network management system on the distribution router. We noticed that the router is not discovering any remote networks. [Mohammed is working on the problem.]
10:04 am	Network connectivity issues are reported between the core devices and the access router. Noticed activity on the Syslog server relating to connectivity issues. [Lynn is working on the problem.]
10:09 am	Request escalation of this ticket to Level 2 support. The network is not functioning. In retrospect, it was probably a bad idea to have Joe, Mohammed, and Lynn simultaneously changing the configurations. We would look at it some more, but we need to leave for a team meeting. [From Lucille, Level 1 team lead]

## Required Resources

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

- An *updated* baseline topology diagram documenting the laboratory installation
- *Updated* network documentation recording the configuration of the laboratory installation

## 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.

**Table 11: Helpful Commands**

Command	Description
<code>ping {host   ip-address}</code>	Pings an IP address
<code>show ip bgp</code>	Displays entries in the BGP routing table
<code>show ip bgp summary</code>	Shows summary BGP status
<code>show ip interface brief</code>	Displays brief form of interface information
<code>show ip protocol interface</code>	Displays the status and parameters of the interfaces configured for a specific protocol. The variable <i>protocol</i> specifies the protocol.
<code>show ip protocol neighbor</code>	Displays information about neighbors for a specific routing protocol.
<code>show ip protocols</code>	Displays values about routing timers and network information associated with the entire router. Use this information to identify a router that is suspected of delivering bad router information.
<code>show ip route</code>	Displays IP routing table information
<code>show protocols</code>	Displays Layer 3 addresses and interface status

## Troubleshooting Log: Isolating Network Layer Problems

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

### Step 1

Modify the Frame Relay interfaces in your existing network diagram.

### Step 2

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

---

---

---

What troubleshooting commands would you use to diagnose network connectivity issues?

---

---

---

### Step 3

On the Troubleshooting Log, document each identified network problem for each specific device. The Troubleshooting Log is divided into four possible areas of concern: core routing and switching, distribution routing, access routing, and access switching. Include the problems discovered by other members of your workgroup. Remember to test ICMP, Telnet, HTTP, and FTP against the new baseline (effected by the newly introduced p2p subinterface on Kingston and multipoint subinterface on Toronto).

### 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:

- You have recorded the Frame Relay subinterface and DLCI numbers on your network diagram.
- The instructor has verified that you have documented all the problems in your workgroup on your troubleshooting log.
- Every member in your workgroup has been assigned one or more problems for resolution from the troubleshooting log.