



### Lab 3.1.1 Applying a Logical Layered Model to a Physical Network

#### Objective

In this exercise, you will use various Cisco IOS commands and a protocol analyzer to map the layers in the OSI model to the encapsulated data flow in the classroom network. You will complete the following tasks:

- Develop a logical diagram for data link layer and network layer functionality in the core noting which MAC addresses relate to which ports.
- Map traffic flows for ping, Telnet, and HTTP traffic from the workgroup PCs
- Capture and analyze background traffic

After completing this exercise, you will be able to:

- Understand the data flow in the classroom network based on the logical network model
- Use a protocol analyzer to review background traffic
- Use Cisco IOS commands to analyze traffic flows in the network and correlate debug messages

#### Required Resources

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

- Access to a protocol analyzer (either software or hardware)
- The network diagram from a previous exercise

#### Job Aids

These job aids are available to help you complete the laboratory exercises:

VLAN Port Status Chart

Device	Port	VLAN ____ Status (Active or Inactive)	VLAN ____ (Description)	VLAN ____ Status (Forwarding or Blocked)

## Command List

You may find the following list of commands helpful although the majority of commands used in this exercise should be familiar from previous experience or from the BSCI, BCMSN, and BCRAN courses. You should ask your instructor to review any unfamiliar commands.

**Table 3: Helpful Commands**

Command	Description
<b>debug ip eigrp</b>	Enables debugging of the EIGRP events
<b>debug ip policy</b>	Enables debugging of the IP policy
<b>debug ip routing</b>	Displays information on routing table updates and route-cache updates
<b>debug serial interface</b>	Enables debugging of the serial interface
<b>ntp server ip-address</b>	Specifies NTP server for a device
<b>ping</b> { <i>host</i>   <i>ip-address</i> }	Sends an echo request packet to an address, then waits for a reply. The <i>host</i>   <i>ip-address</i> variable is the IP alias or IP address of the target system
<b>show access-lists</b>	Displays the contents of all access lists
<b>show clock</b>	Displays current date and time information for device
<b>show etherchannel summary</b>	Displays EtherChannel port-channel summary status, including data link and network layer port and interface information.
<b>show interface status</b>	Displays a tabular status report of the ports on a switch.
<b>show interfaces trunk</b>	Shows information about trunking interfaces
<b>show ntp associations</b>	Displays NTP associations
<b>show ntp status</b>	Displays NTP status
<b>show route-map</b>	Displays information about all configured route maps
<b>show spanning-tree vlan</b> <i>vlan-id</i>	Display Spanning Tree Protocol information including port status for a specific VLAN
<b>show vlan</b>	Displays default and defined VLAN information
<b>telnet</b> { <i>host</i>   <i>ip-address</i> }	Connects to an IP address using the Telnet application
<b>terminal monitor</b>	Displays debug command output and system error messages for the current terminal and session.
<b>traceroute</b> [ <i>destination</i> ]	Identifies the path a packet takes through the network. The <i>destination</i> variable is the hostname or IP address of the target system

## Step 1

The Cisco Catalyst 3550 and 2950 switches in the lab support both Layer 2 and Layer 3 functionality. For this task, gather information about the VLANs and subnets. Complete the VLAN Port Status Chart.

1. Connect to the workgroup switches.
2. Use the `show vlan` and `show spanning-tree vlan vlan-id` commands to determine which VLANs are active and to determine the VLAN port status for all switched ports. Document these results on the VLAN Port Status chart.
3. Connect to core switch.
4. Document VLAN Port status for all interfaces on the core switch.
5. Sketch out the VLAN status, or add details to your network diagram documenting the logical preference for the VLANs for your workgroup.

## Step 2

Use a protocol analyzer to capture and review background LAN traffic.

1. Start the protocol analyzer software on your PC. (This following example describes the process using Ethereal. If applicable, follow the directions from your instructor for a hardware protocol analyzer.)
2. From the Toolbar, choose **View > Time Display Format**.
3. Under Time Display Format, click **Time of Day**.
4. From the Toolbar, choose **Capture > Start**.
5. Select the appropriate adapter under **Interface**.
6. Under Display Options, click **Update List of Packets In Real Time**. Click **OK** to begin capturing data.
7. Capture a few minutes of background traffic without running any additional applications.

What kinds of traffic do you see?

---

---

---

8. At the command prompt for the PC, enter `arp -a` to look for current ARP mappings.

What do you see?

---

---

---

9. Enter `show arp` to look at the ARP table on the access router and the access switch. Enter `show mac-address-table` to look at the MAC addresses and VLANs on the access switch. Clear the ARP table on the PC with the `arp -d` command. Enable `debug ip icmp` and `debug arp` on the access router and the access switch.
10. Coordinate with your workgroup, and `ping` the other PCs in the workgroup. Look for ARPs in the protocol analysis stream. Again check for ARP mappings on your PC.

What do you see?

---

---

---

Is this what you expected? \_\_\_\_\_

Does the access switch generate any debug messages? If so, why?

---

---

---

Does the access router generate any debug messages? If so, why?

---

---

---

11. At the command prompt for the PC, **ping** your default gateway. Look for ARPs in the protocol analysis stream. Check your current ARP mappings.

What do you see?

---

---

---

12. Using Telnet, generate some additional traffic by connecting to a workgroup device.

What do you see in terms of data flow?

---

---

---

Is this what you expected? \_\_\_\_\_

13. Close this Telnet session.

14. Open a browser window, and connect to 172.28.128.9.

What do you see?

---

---

---

Is this what you expected? \_\_\_\_\_

15. Exit the browser session.

16. Have the student with the console session to the 2950 switch (Kingston) adjust the global spanning tree properties by entering the **no spanning-tree portfast bpduguard default** global configuration command. Look for differences in the background traffic.

What do you see?

---

---

---

17. Restore the spanning tree command.
18. Have the student with the console session on the access router remove the passive interfaces under EIGRP. Look for differences in the background traffic.

What do you see?

---

---

---

19. Restore the EIGRP passive interfaces removed in the previous step.
20. In the second Ethereal window, click **Stop** to halt the Ethereal application.
21. As needed, continue your review of the captured traffic by scrolling through the list. Choose **File>Save As** to save the capture file for future reference.
22. List all data flows you saw.

---

---

---

23. Exit the Ethereal protocol analyzer software.

### Step 3

Use Cisco IOS commands to review background WAN traffic.

1. Open console sessions on the workgroup routers.
2. Enable the **debug eigrp packets** command on both routers and the distribution switch. Wait for a minute or so.

Do you see any debug messages? \_\_\_\_\_

Why or why not?

---

---

---

(Leave the **debug eigrp packet** event process running.)

3. If you are not connected to a router with active WAN interfaces, connect to the distribution router via Telnet. Configure your session so that you can also see the debug messages from the distribution router. (Coordinate entering the commands in this task with the other students in your workgroup.)
4. Enable the **debug serial interface** command on the distribution and access routers.

5. Examine the output for a minute or so.

What do you see?

---

---

---

Compare these messages on the distribution and access routers. Do they have matching timestamps? \_\_\_\_\_

Could NTP be useful in debugging?

---

---

---

6. Shut down the S0/1 interface on the access router.

What and when did the access router notice?

---

---

---

What and when did the distribution router notice?

---

---

---

7. Activate the S0/1 interface. To halt the EIGRP event debugging, enter **no debug eigrp packet**.

Activate IP routing debugging, enter **debug ip routing**.

8. On the distribution router, enter the **no keepalive** interface command on S0/1.

What and when does the distribution router see?

---

---

---

What and when does the access router see?

---

---

---

9. Wait at least a minute, and then restore the default keepalive with the **keepalive** interface command on S0/1.

10. On the distribution router, enter the **keepalive 30** interface command on the S0/1 interface.

What does the distribution router see?

---

---

---

What does the access router see?

11. Restore the default keepalive with the **keepalive** interface command on S0/1. Halt the IP routing debug with the **no debug ip routing** command.
12. On the access router, enter the **frame-relay lmi-type cisco** on the S0/1 interface.  
What does the distribution router see?

---

---

---

What does the access router see?

---

---

---

13. Restore the previous lmi type with the **frame-relay lmi-type ansi** command.
14. On all routers and the core switch, halt all the debugging processes with the **undebug all** command.
15. List all data flows you saw.

---

---

---

#### Step 4

Use Cisco commands to map traffic flows in the network.

1. Enable **debug ip icmp** on all workgroup routers and switches.
2. All students should go to the console session on the access router. (Coordinate entering the commands in this task with the other students in your workgroup.)
3. Use the **ping** command from the access router to verify connectivity to CCNP4\_Server at 172.28.128.9.
4. Use an extended **ping** command to verify connectivity from the FastEthernet 0/0.2 subinterface to CCNP4\_Server at 172.28.128.9.

Do you notice any differences?

---

---

---

5. Use the **traceroute** command to verify connectivity to the core 2950 from the access router.
6. Use an extended **traceroute** command to verify connectivity from the FastEthernet 0/0.2 subinterface to the core 2950.  
Do you notice any differences? \_\_\_\_\_
7. Use the **show ip route** command to review the routes to the core 2950.
8. Use the **show ip policy**, **show route-map**, and **show access-list** commands to review policy routing on the access router.



What do you notice?

---

---

---

9. Enable `debug ip policy` on the access router.
10. At a PC command line, `ping` an address on the core 2950. Review the policy routing debug output.

What do you notice?

---

---

---

11. From the access router, `ping` an address on the core 2950. Review the policy routing debug output.

What do you notice?

---

---

---

12. On all routers and switches, halt all the debugging processes with the `undebug all` command.
13. List all data flows you saw.

---

---

---