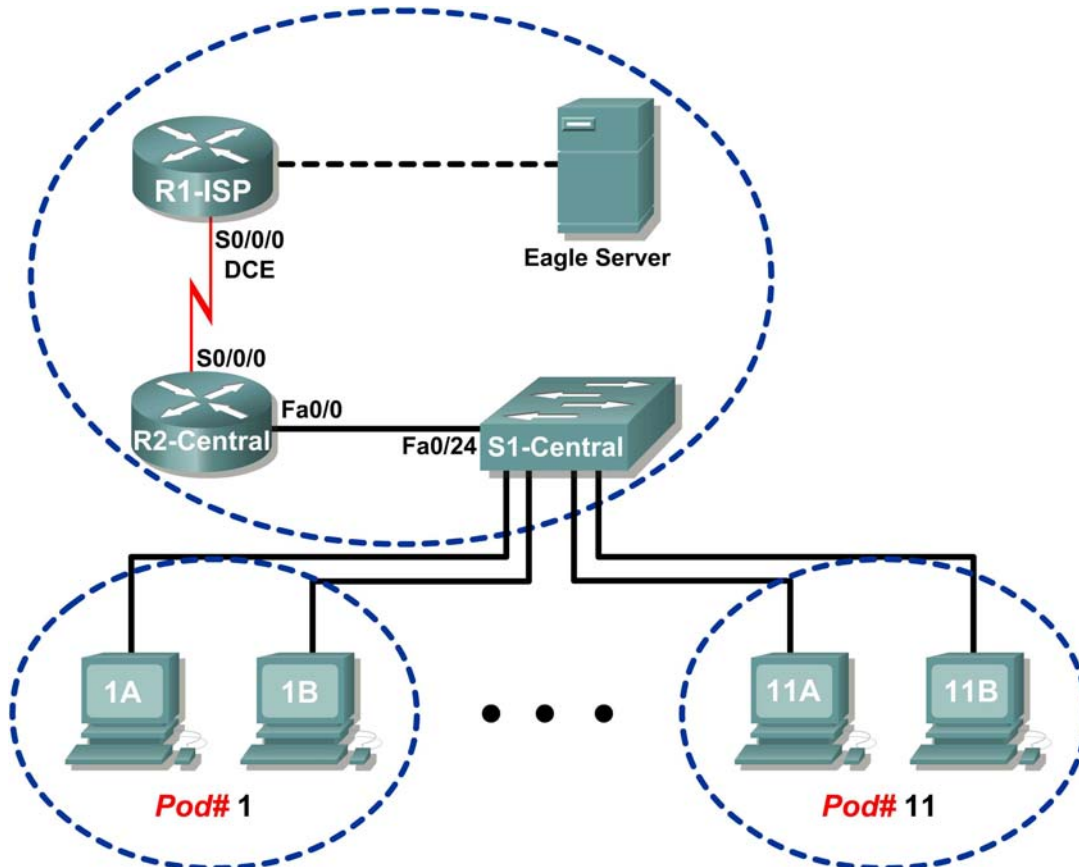# Lab 9.8.3: Intermediary Device as an End Device

## Topology Diagram



## Addressing Table

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|---|
| R1-ISP | S0/0/0 | 10.10.10.6 | 255.255.255.252 | N/A |
| | Fa0/0 | 192.168.254.253 | 255.255.255.0 | N/A |
| R2-Central | S0/0/0 | 10.10.10.5 | 255.255.255.252 | 10.10.10.6 |
| | Fa0/0 | 172.16.255.254 | 255.255.0.0 | N/A |
| Eagle Server | N/A | 192.168.254.254 | 255.255.255.0 | 192.168.254.253 |
| | N/A | 172.31.24.254 | 255.255.255.0 | N/A |
| host*Pod#*A | N/A | 172.16.*Pod#*.1 | 255.255.0.0 | 172.16.255.254 |
| host*Pod#*B | N/A | 172.16.*Pod#*.2 | 255.255.0.0 | 172.16.255.254 |
| S1-Central | N/A | 172.16.254.1 | 255.255.0.0 | 172.16.255.254 |

## Learning Objectives

Upon completion of this lab, you will be able to:

- Use Wireshark to capture and analyze frames originating from network nodes.
- Examine the origination of frames in a small network.

## Background

A switch is used to route frames between network devices. A switch does not normally originate the frame to node devices. Rather, a switch efficiently passes the frame from one device to another in the LAN.

## Scenario

Wireshark will be used to capture and analyze Ethernet frames. If Wireshark has not been loaded on the host pod computer, it can be downloaded from URL `ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter9/`, file `wireshark-setup-0.99.4.exe`.

In this lab you will ping a neighbor's pod host computer.

Write down the IP address and port connection on S1-Central for the neighbor's pod host computer:

IP Address: _____ S1-Central port number: _____

### Task 1: Use Wireshark to Capture and Analyze Frames Originating From Network Nodes.

#### Step 1: Configure Wireshark for packet captures.

Prepare Wireshark for captures.

1. Click **Capture > Options**.
2. Select the Interface that corresponds to the LAN.
3. Check the box to Update list of packets in real time.
4. Click **Start**.

This will begin the packet capture. During this capture there will probably be more than 200 captures, making analysis a bit tedious. The critical Telnet conversation between the pod host computer and S1-Central will be easy to filter.

#### Step 2: Use the Windows Telnet client to access S1-Central.

S1-Central has been configured with 11 student accounts, `ccna1` through `ccna11`. To provide access to each student, use the userid corresponding to your pod. For example, for host computers on pod 1, use userid `ccna1`. Unless directed otherwise by your instructor, the password is `cisco`.

1. From the Windows terminal, issue the Telnet command, **telnet** *destination-ip-address*:

   C:/> **telnet 172.16.254.1**

2. Enter the appropriate user name and password, **cisco**.
   The S1-Central prompt should be returned, `S1-Central#`.

**Step 3: Clear the MAC address table.**

1. Examine the switch MAC address table with the command `show mac-address-table`. In addition to several static CPU entries, there should be numerous dynamic address table entries.

2. To clear dynamic MAC address table entries, use the `clear mac-address-table dynamic` command.

3. List the dynamic MAC address entries:

| MAC Address | Switch Port |
|---|---|
|  |  |
|  |  |
|  |  |

4. Open a second terminal window. Ping your neighbor's IP address, which was recorded earlier:

   ```
   C:>\ ping –n 1 ip-address
   ```

5. The MAC address for this computer should be dynamically added in the S1-Central MAC address table.

6. Again list the dynamic MAC address entries:

| MAC Address | Switch Port |
|---|---|
|  |  |
|  |  |
|  |  |

   What conclusion can be made about how a switch learns MAC addresses connected to switch interfaces?

   _____

   _____

   .

7. Close Wireshark capture.

   The capture will be analyzed in the next task.


## Task 2: Examine the Origination of Frames in a Small Network.

**Step 1: Examine a Telnet session to S1-Central.**

1. Highlight one of the Telnet session packets. On Wireshark menu, click **Analyze | Follow TCP Stream**. A stream content window will open, default display ASCII. If the username and passwords are not visible, switch to HEX Dump.

2. Verify the username and password that you entered:
   Username: _____ Password: _____

3. Close the stream content window.

**Step 2: Examine output of the `show mac-address-table command.`**

1. Open Notepad. Captured data will be transferred to Notepad for analysis. There may be numerous packets that were captured.

2. In the top Wireshark Packet List pane, scroll down to the captured ICMP request. If the bottom Wireshark Packet Byte window is not visible, click **View > Packet bytes**.
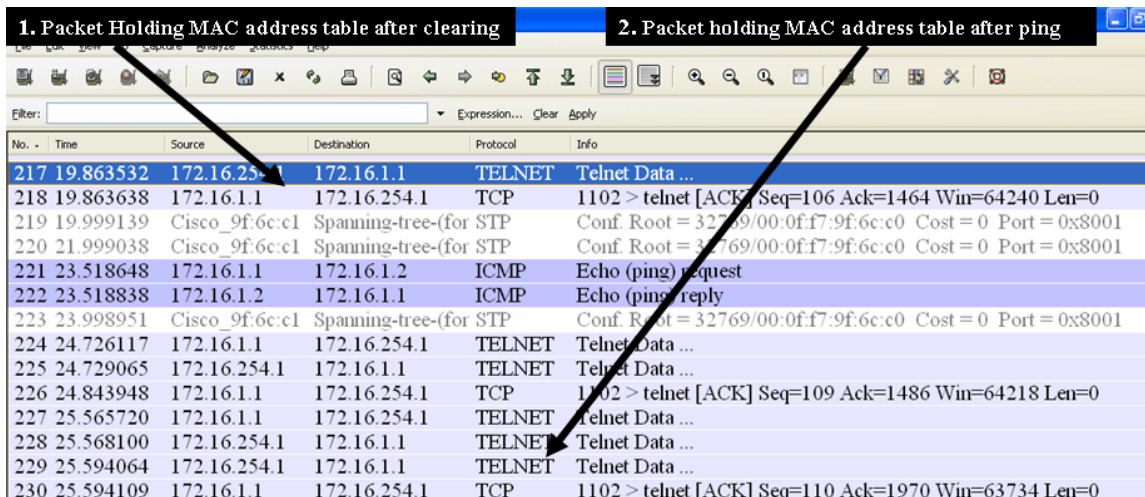
**Figure 1. Wireshark Capture of Telnet**

See Figure 1, a partial output of the Wireshark capture:

**1** Select the last Telnet data packet from S1-Central before the `ping` command. Next, select the corresponding Packet byte. Right-click the Packet byte and click **Copy > Text only**. In Notepad, click **Edit > Paste**. Dynamic mappings should be similar to the following output:

```
{_lEMaNL;RPC              Mac Address Table
------------------------------------------

Vlan    Mac Address        Type        Ports
----    -----------        --------    -----
 All    000f.f79f.6cc0     STATIC      CPU
 All    0100.0ccc.cccc     STATIC      CPU
 All    0100.0ccc.cccd     STATIC      CPU
 All    0100.0cdd.dddd     STATIC      CPU
   1    0010.a47b.015f     DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 5
S1-Central#
```

3.  Write down the MAC address and Port number displayed in the output. Does the switch port correspond to your pod host computer? _____

| MAC Address | Type | Port |
|-------------|------|------|
|             |      |      |

Why is your pod host computer mapping still in the MAC address table, despite having been cleared? _____

_____

**2**   Select the last Telnet data packet immediately after the ping reply. Next, select the corresponding Packet byte. Right-click the Packet byte and click **Copy > Text only**. In Notepad, click **Edit > Paste**. Text should be similar to the following Paste action:

```
{_lEPaNM;VP           Mac Address Table
    ------------------------------------------

    Vlan    Mac Address       Type         Ports
    ----    -----------       --------     -----
     All    000f.f79f.6cc0    STATIC       CPU
     All    0100.0ccc.cccc    STATIC       CPU
     All    0100.0ccc.cccd    STATIC       CPU
     All    0100.0cdd.dddd    STATIC       CPU
      1     0010.a47b.015f    DYNAMIC      Fa0/1
      1     0016.76ac.a76a    DYNAMIC      Fa0/2
    Total Mac Addresses for this criterion: 6
    S1-Central#
```

4.  Write down the MAC address and Port number for the second dynamic displayed in the output. Does the switch port correspond to your neighbor's pod host computer? _____

| MAC Address | Type | Port |
|---|---|---|
|  |  |  |

## Task 3: Reflection

The Wireshark capture of a Telnet session between a pod host computer and S1-Central was analyzed to show how a switch dynamically learns about nodes directly connected to it.

## Task 4: Challenge

Use Wireshark to capture and analyze a Telnet session between the pod host computer and the Cisco switch. Use the Wireshark menu option **Analyze > Follow TCP Stream** to view the login user ID and password. How secure is the Telnet protocol? What can be done to make communication with Cisco devices more secure?

_____

_____

_____

_____

_____

## Task 5: Clean Up

Wireshark was installed on the pod host computer. If Wireshark needs to be uninstalled, click **Start > Control Panel**. Open **Add or Remove Programs**. Select Wireshark, and click **Remove**.

Remove any files created on the pod host computer during the lab.

Unless directed otherwise by the instructor, turn off power to the host computers. Remove anything that was brought into the lab, and leave the room ready for the next class.