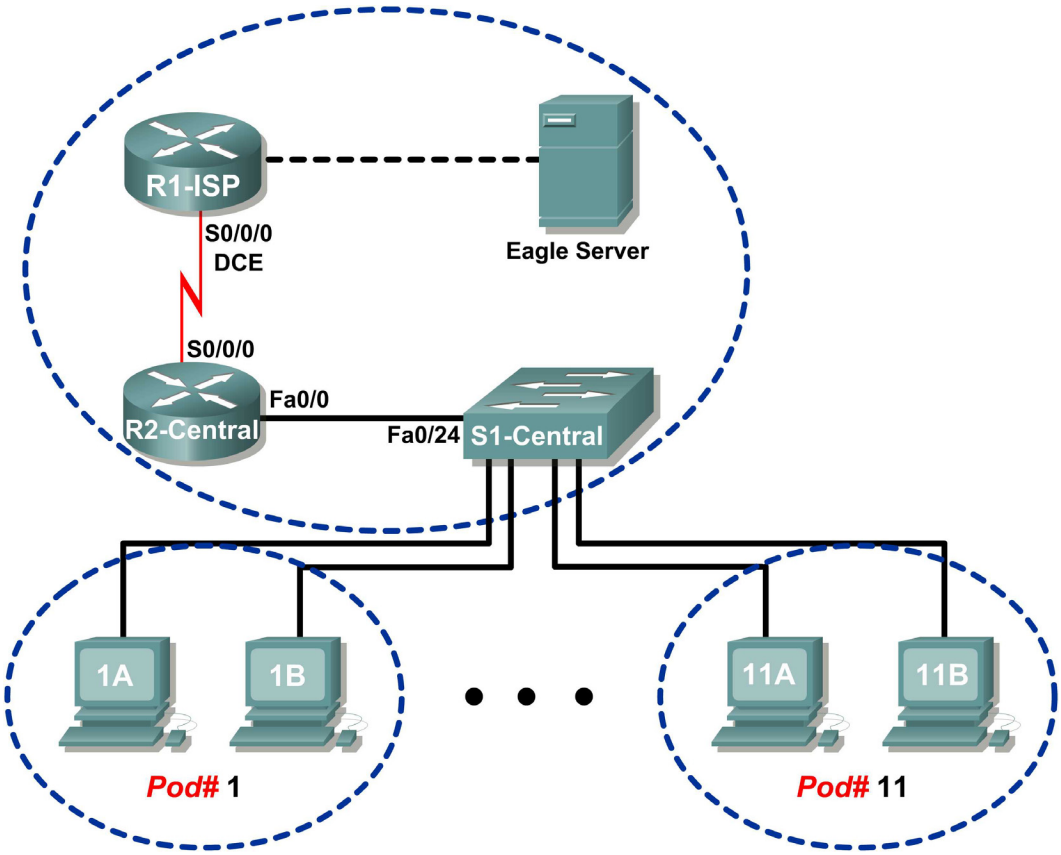
Lab 9.8.1: Address Resolution Protocol (ARP)

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	N/A
	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 Windows **arp** command.
- Use Wireshark to examine ARP exchanges.

Background

Address Resolution Protocol (ARP) is used by TCP/IP to map a Layer 3 IP address to a Layer 2 MAC address. When a frame is placed on the network, it must have a destination MAC address. To dynamically discover the MAC address to the destination device, an ARP request is broadcast on the LAN. The device that contains the destination IP address responds, and the MAC address is recorded in ARP cache. Every device on the LAN keeps its own ARP cache, or small area in RAM that holds ARP results. An ARP cache timer removes ARP entries that have not been used for a certain period of time. Depending on the device, times differ. For example, some Windows operating systems store ARP cache entries for 2 minutes. If the entry is used again during that time, the ARP timer for that entry is extended to 10 minutes.

ARP is an excellent example in performance tradeoff. With no cache, ARP must continually request address translations each time a frame is placed on the network. This adds latency to the communication and could congest the LAN. Conversely, unlimited hold times could cause errors with devices that leave the network or change the Layer 3 address.

A network engineer needs to be aware of ARP but may not interact with the protocol on a regular basis. ARP is a protocol that enables network devices to communicate with the TCP/IP protocol. Without ARP, there is no efficient method to build the datagram Layer 2 destination address. Also, ARP is a potential security risk. ARP spoofing, or ARP poisoning, is a technique used by an attacker to inject the wrong MAC address association in a network. An attacker forges the MAC address of a device, and frames are sent to the wrong destination. Manually configuring static ARP associations is one way to prevent ARP spoofing. Finally, an authorized MAC address list may be configured Cisco devices to restrict network access to only approved devices.

Scenario

With a pod host computer, use the Windows **arp** utility command to examine and change ARP cache entries.

In Task 2, Wireshark will be used to capture and analyze ARP exchanges between network devices. 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`.

Task 1: Use the Windows `arp` Command.

Step 1: Access the Windows terminal.

```
C:\> arp
Displays and modifies the IP-to-Physical address translation tables
used by address resolution protocol (ARP).
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
-a          Displays current ARP entries by interrogating the current
            protocol data. If inet_addr is specified, the IP and
            Physical addresses for only the specified computer are
            displayed. If more than one network interface uses ARP,
            entries for each ARP table are displayed.
-g          Same as -a.
inet_addr   Specifies an internet address.
-N if_addr  Displays the ARP entries for the network interface
            specified by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
            wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
            with the Physical address eth_addr.  The Physical address
            is given as 6 hexadecimal bytes separated by hyphens. The
            entry is permanent.
eth_addr    Specifies a physical address.
if_addr     If present, this specifies the Internet address of the
            interface whose address translation table should be
            modified. If not present, the first applicable interface
            will be used.
Example:
 > arp -s 157.55.85.212 00-aa-00-62-c6-09  .... Adds a static entry.
 > arp -a                                  .... Displays the arp table.
C:\>
```

Figure 1. `arp` Command Syntax

1. Open a Windows terminal by clicking **Start > Run**. Type **`cmd`**, and click **OK**.
   With no options, the **`arp`** command will display useful help information. See Figure 1.
2. Issue the **`arp`** command on the pod host computer, and examine the output.
3. Answer the following questions about the **`arp`** command:

   What command would be used to display all entries in ARP cache?
   arp -a

   What command would be used to delete all ARP cache entries (flush ARP cache)?
   arp -d*

   What command would be used to delete the ARP cache entry for 172.16.255.254?
   arp -d 172.16.255.254

Step 2: Use the `arp` command to examine local ARP cache.

```
C:\> arp -a
No ARP Entries Found
C:\>
```

Figure 2. Empty ARP Cache

Without any network communication, the ARP cache should be empty. This is shown in Figure 2.

Issue the command that displays ARP entries. What are the results?

No ARP Entries Found

Step 3: Use the `ping` command to dynamically add entries in the ARP cache.

The **`ping`** command can be used to test network connectivity. By accessing other devices, ARP associations are dynamically added to ARP cache.

```
C:\> ping 172.16.1.2
Pinging 172.16.1.2 with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Figure 3. `ping` Command to a Pod Host Computer

1. Use the command **`ipconfig /all`** to verify the pod host computer's Layer 2 and Layer 3 information.
2. Issue the **`ping`** command to another pod host computer, shown in Figure 3. Figure 4 shows the new ARP cache entry.

```
C:\> arp -a
Interface: 172.16.1.1 --- 0x60004
  Internet Address      Physical Address      Type
  172.16.1.2            00-10-a4-7b-01-5f     dynamic
C:\>
```

Figure 4. Display of ARP Cache

How was the ARP entry added to the ARP cache? Hint: review the Type column.

dynamic

What is the physical address of the destination pod host computer?

10.100.5.188.

What is the physical address of the destination pod host computer?

IP Address	Physical Address	How Discovered?
10.100.5.188	mac	dynamic

3. Do not send any traffic to the computer accessed previously. Wait between 2 and 3 minutes, and check ARP cache again. Was the ARP cache entry cleared? ____yes____

4. Issue the **ping** command to the Gateway, R2-Central. Examine ARP cache entry. What is the physical address of the Gateway? _____

IP Address	Physical Address	How Discovered?
172.16.255.254	172.16.255.94	

5. Issue the **ping** command to Eagle Server, eagle-server.example.com. Examine ARP cache entry. What is the physical address of Eagle Server? _____

_____

_____

Step 4: Manually adjust entries in the ARP cache.

To delete entries in ARP cache, issue the command **arp –d {inet-addr | *}**. Addresses can be deleted individually by specifying the IP address, or all entries can be deleted with the wildcard *.

Verify that the ARP cache contains two entries: one for the Gateway and one to the destination pod host computer. It may be easier to ping both devices more than once, which will retain the cache entry for approximately 10 minutes.

```
C:\> arp –a
Interface: 172.16.1.1 --- 0x60004
  Internet Address      Physical Address      Type
  172.16.1.2            00-10-a4-7b-01-5f     dynamic
  172.16.255.254        00-0c-85-cf-66-40     dynamic
C:\>
C:\>arp -d 172.16.255.254
C:\> arp -a
Interface: 172.16.1.1 --- 0x60004
  Internet Address      Physical Address      Type
  172.16.1.2            00-10-a4-7b-01-5f     dynamic
C:\>
```

Figure 5. Manually Removing an ARP Cache Entry

See Figure 5, which shows how to manually delete an ARP cache entry.

1. On your computer, first verify that the two entries are present. If not, ping the missing entry.
2. Next, delete the entry for the pod host computer.
3. Finally, verify your change.
4. Record the two ARP cache entries:

Device	IP Address	Physical Address	How Discovered?
host	172.16.254.92	mac	
gateway	172.16.255.254		

5. Write the command that will delete the entry for the pod host computer:
_____arp -d inet-addr_____

6. Issue the command on your pod host computer. Record the remaining ARP cache entry:

Device	IP Address	Physical Address	How Discovered?
gateway	172.16.255.254		

7. Simulate removing all entries. Write the command that will delete all entries in ARP cache: arp -d*
8. Issue the command on your pod host computer, and examine the ARP cache with the command **arp -a**. All entries should be removed. no arp entries found
9. Consider a secure environment where the Gateway controls access to a web server that contains Top Secret information. What is one layer of security that can be applied to ARP cache entries that could aid in countering ARP spoofing? static gateway address
10. Write the command that will add a static ARP entry for the Gateway to ARP cache: arp -s 172.16.255.254
11. Examine the ARP cache again, and fill in the following table:

IP Address	Physical Address	Type

For the next task, Wireshark will be used to capture and examine an ARP exchange. Do not close the Windows terminal—it will be used to view the ARP cache.

Task 2: Use Wireshark to Examine ARP Exchanges .

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.

Step 2: Prepare the pod host computer for ARP captures.

1. If not already completed, open a Windows terminal window by clicking **Start > Run**. Type **cmd**, and click **OK**.
2. Flush the ARP cache, which will require ARP to rediscover address maps. Write the command that you used: arp -d*

Step 3: Capture and evaluate ARP communication.

In this step, one ping request will be sent to the Gateway, and one ping request will be sent to Eagle Server. Afterward, Wireshark capture will be stopped and the ARP communication evaluated.

1. Send one ping request to the Gateway, using the command **ping –n 1 172.16.255.254.**
2. Send one ping request to Eagle Server, using the command **ping –n 1 192.168.254.254**.

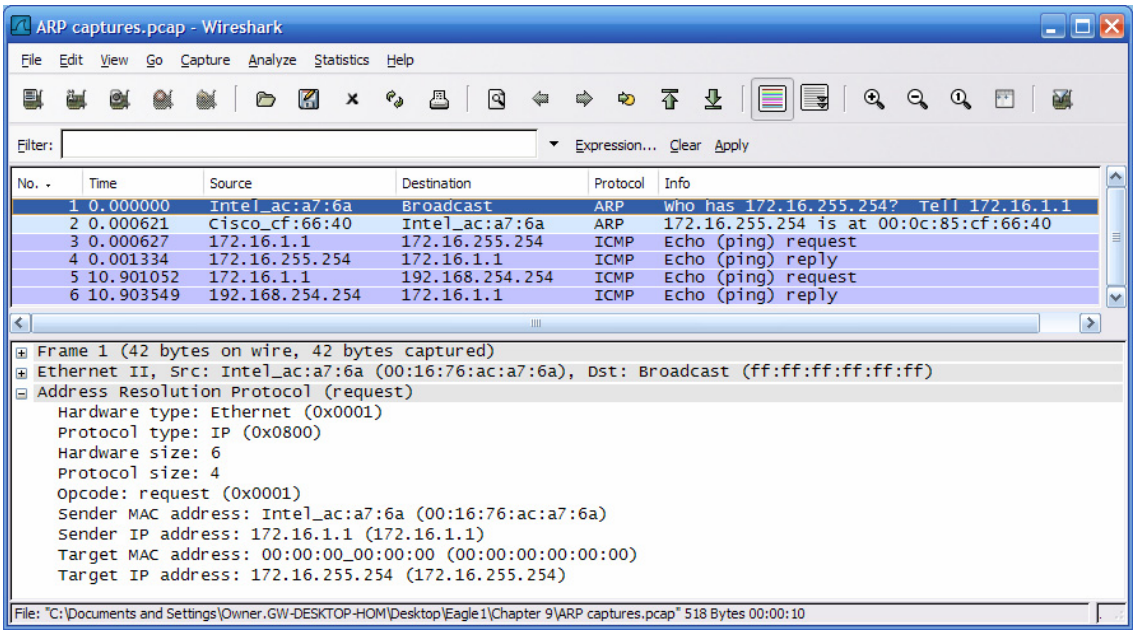


Figure 6. Wireshark Capture of ARP Communication

3. Stop Wireshark and evaluate the communication. You should see a Wireshark screen similar to the screen shown in Figure 6. The Wireshark Packet list window displays the number of packets captured. The Packet Details Window shows ARP protocol contents.

4. Using your Wireshark capture, answer the following questions:

   What was the first ARP packet? request

   What was the second ARP packet? reply

   Fill in the following table with information about the first ARP packet:

Field	Value
Sender MAC address	
Sender IP address	
Target MAC address	
Target IP address	

   Fill in the following table with information about the second ARP packet:

Field	Value
Sender MAC address	
Sender IP address	
Target MAC address	
Target IP address	

   If the Ethernet II frame for an ARP request is a broadcast, why does the Target MAC address contain all 0s? arp is set yet

   Why was there no ARP request for the ping to Eagle Server? tcp/ip sends to the physical address

How long should the Gateway mapping be stored in ARP cache on the pod host computer? Why?

2 minutes

_____

_____

Task 3: Reflection

The ARP protocol maps Layer 3 IP addresses to Layer 2 MAC addresses. If a packet must move across networks, the Layer 2 MAC address changes with each hop across a router, but the Layer 3 address never changes.

ARP cache stores ARP address mappings. If the entry was learned dynamically, it will eventually be deleted from cache. If the entry was manually inserted in ARP cache, it is a static entry and will remain until the computer is turned off or the ARP cache is manually flushed.

Task 4: Challenge

Using outside resources, perform a search on ARP spoofing. Discuss several techniques used to counter this type of attack.

Most wireless routers support wireless network access. Using this technique, MAC addresses that are permitted access to the wireless network are manually added to the wireless router. Using outside resources, discuss the advantages of configuring wireless network access. Discuss ways that attackers can circumvent this security.

Task 5: Clean Up

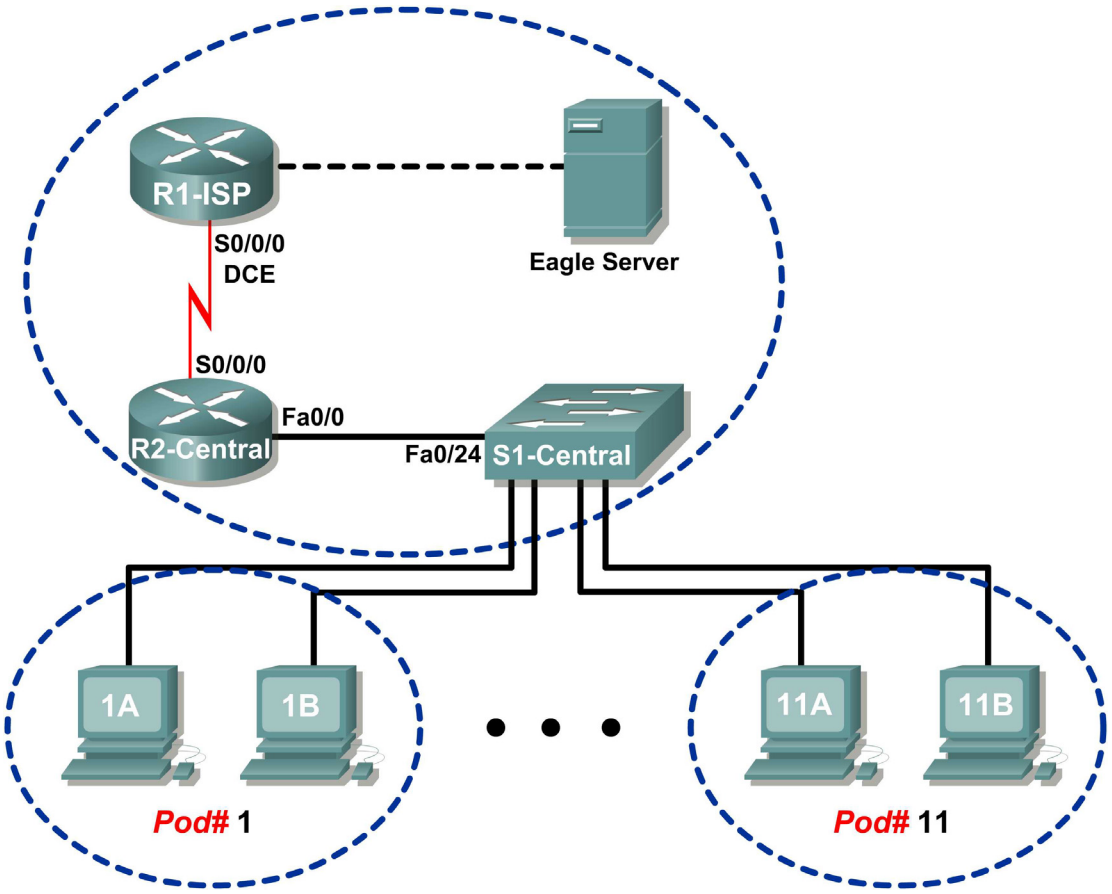
Wireshark was installed on the pod host computer. If Wireshark needs to be uninstalled, click **Start > Control Panel**. Open **Add or Remove Programs**. Highlight Wireshark, and click **Remove**.

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.

Lab 9.8.2: Cisco Switch MAC Table Examination

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	N/A
	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 the Telnet protocol to log into a Cisco Switch.
- Use the Cisco IOS **show mac-address-table** command to examine MAC address and port associations.

Background

Switches maintain a table of MAC addresses and associated switch port. When a switch receives a frame, the destination MAC address is checked against the table, and the corresponding port is used to route the frame out of the switch. If a switch does not know which port to route the frame, or the frame is a broadcast, then the frame is routed out all ports except the port where it originated.

Access to Cisco devices can be accomplished through several means. A console port can be used if the Cisco router or switch is within the same physical proximity of a computer. Using Windows hyperterm utility, a serial connection can be established. For devices physically distant from the network engineer, network connectivity can be established through two means. If the network is not secure, a modem configured on the AUX port enables telephone access. For secure networks, the Cisco device can be configured for a Telnet session. In this lab, the student will connect to the switch via a Telnet session.

Lab

- Telnet to S1-Central.
- Log in with student account.
- Use **show mac-address-table** command to examine the mac addresses and association to ports.

Scenario

Use the Cisco IOS **show mac-address-table** command to examine the switch MAC address table and other address-related information.

Telnet is a network service that uses a client-server model. Cisco IOS devices provide a default Telnet server, and operating systems such as Windows have built-in Telnet clients. Using Telnet, network engineers can log into network devices from anywhere across a secure network. The Cisco device must be configured for Telnet access, otherwise it is denied. In Eagle 1, limited privileges have been configured for student use.

Task 1: Use the Telnet Protocol to Log in to a Cisco Switch.

Step 1: Access the Windows terminal.

Open a Windows terminal by clicking **Start > Run**. Type **cmd**, and click **OK**.

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**

   An access prompt will be displayed, similar to the one shown in Figure 1.


```
**************************************************************************
                This is Lab switch S1-Central.
                Authorized access only.
**************************************************************************
User Access Verification
Username: ccna1
Password: cisco  (*hidden*)
S1-Central#
```

Figure 1. Telnet Client

2. Enter the applicable user name. When the password prompt appears, type `cisco <ENTER>`.

   The `S1-Central#` prompt should appear.

Task 2: Use the Cisco IOS `show mac-address-table` Command to Examine MAC Addresses and Port Associations.

Step 1: Examine the switch MAC address table.

1. Issue the command **`show mac-address-table ? <ENTER>`**. This will output all options for the command.
2. Use the following table to fill in the command options:

Option	Description
address	address
aging-time	aging time
count	count
dynamic	dynamic entry
interface	interface
multicast	send info for wildcard
notification	MAC parameters
static	static entry
vlan	vlan
|	output
<cr>	

Step 2: Examine dynamic MAC address table entries.

1. Issue the command **`show mac-address-table`**.
   This command will display static (CPU) and dynamic, or learned, entries.

2. List the MAC addresses and corresponding switch ports:

MAC Address	Switch Port

Suppose there was a hub with five active hosts connected to switch port `gi0/0`. How many MAC addresses would be listed for switch port `gi0/0`? _____5_____

Step 3: Examine MAC address table aging time.

1. Issue the command **`show mac-address-table aging-time`**.
   This command will display the default time, in seconds, that MAC address entries are stored.
2. What is the default aging time for VLAN 1? _____300_____

Task 3: Challenge

What would be the result if the MAC address table was flushed of dynamic entries?

_____broadcast through all ports requesting mac addresses from devices._____

_____

Task 4: Reflection

Using the Telnet protocol, network engineers can access Cisco devices remotely across secure LANs. This has the benefit of permitting access to remote devices for troubleshooting and monitoring purposes.

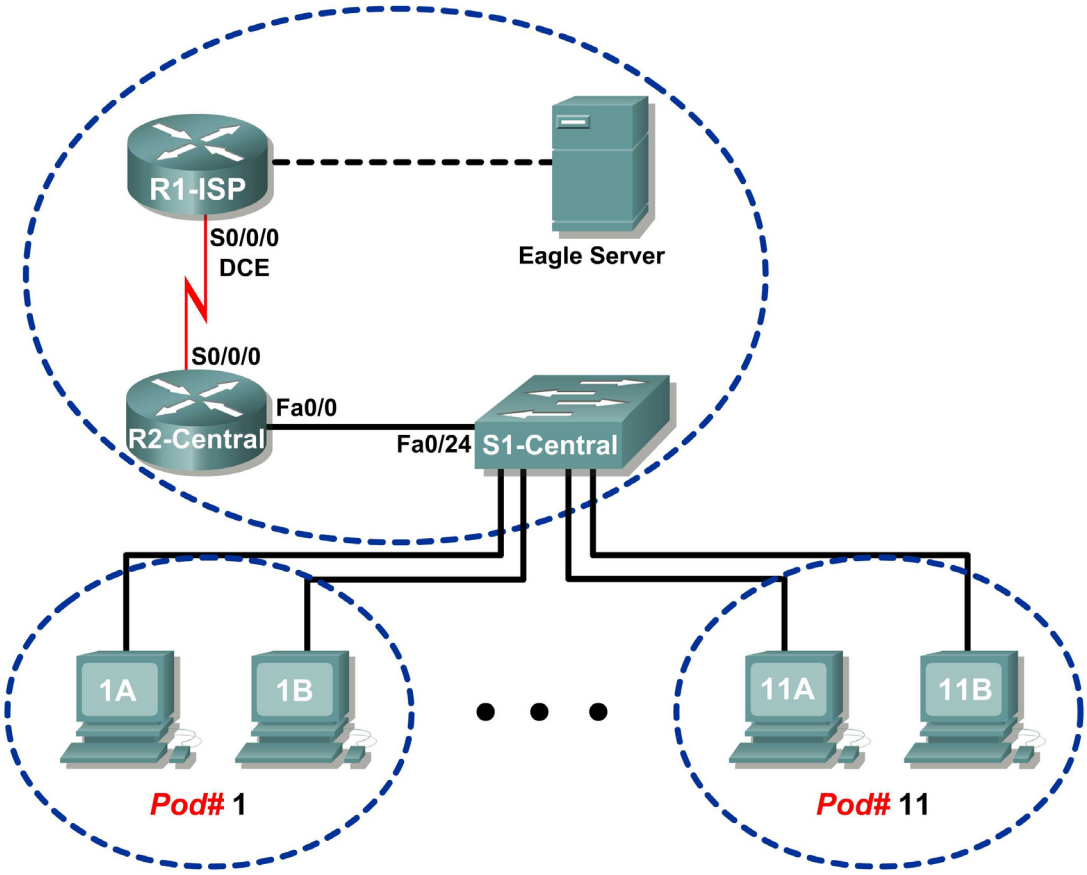
A switch contains a MAC address table that lists the MAC address connected to each switch port. When a frame enters the switch, the switch performs a lookup of the frame destination MAC address. If there is a match in the MAC address table, the frame is routed out the corresponding port. Without a MAC address table, the switch would have to flood the frame out each port.

Task 5: Clean Up

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.

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	N/A
	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?

   The device talks to the switch first.

   .

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: cisco
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**.

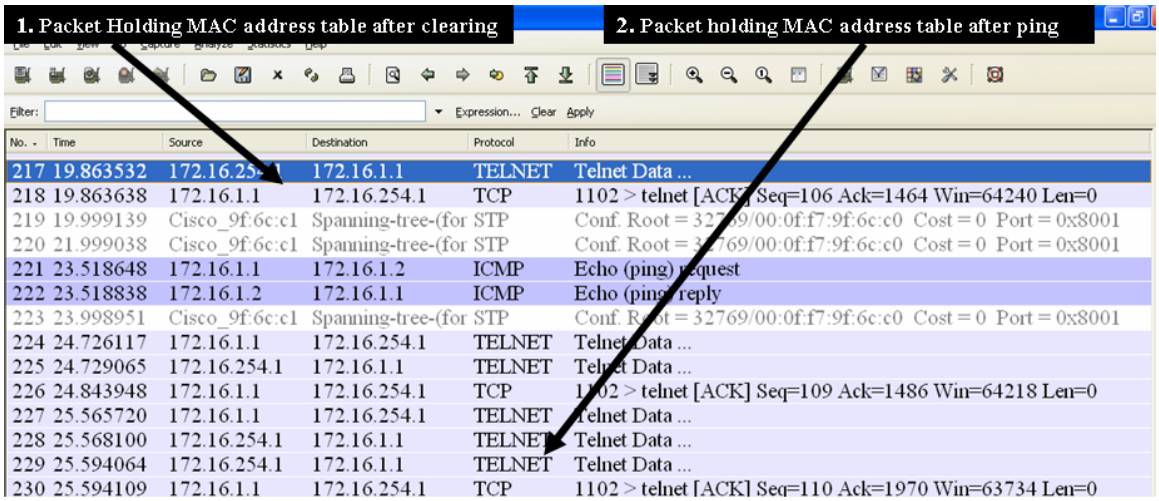


Figure 1. Wireshark Capture of Telnet

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? ____yes____

MAC Address	Type	Port
	dynamic	

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

_____

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? ____yes____

MAC Address	Type	Port
	dynamic	

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.

