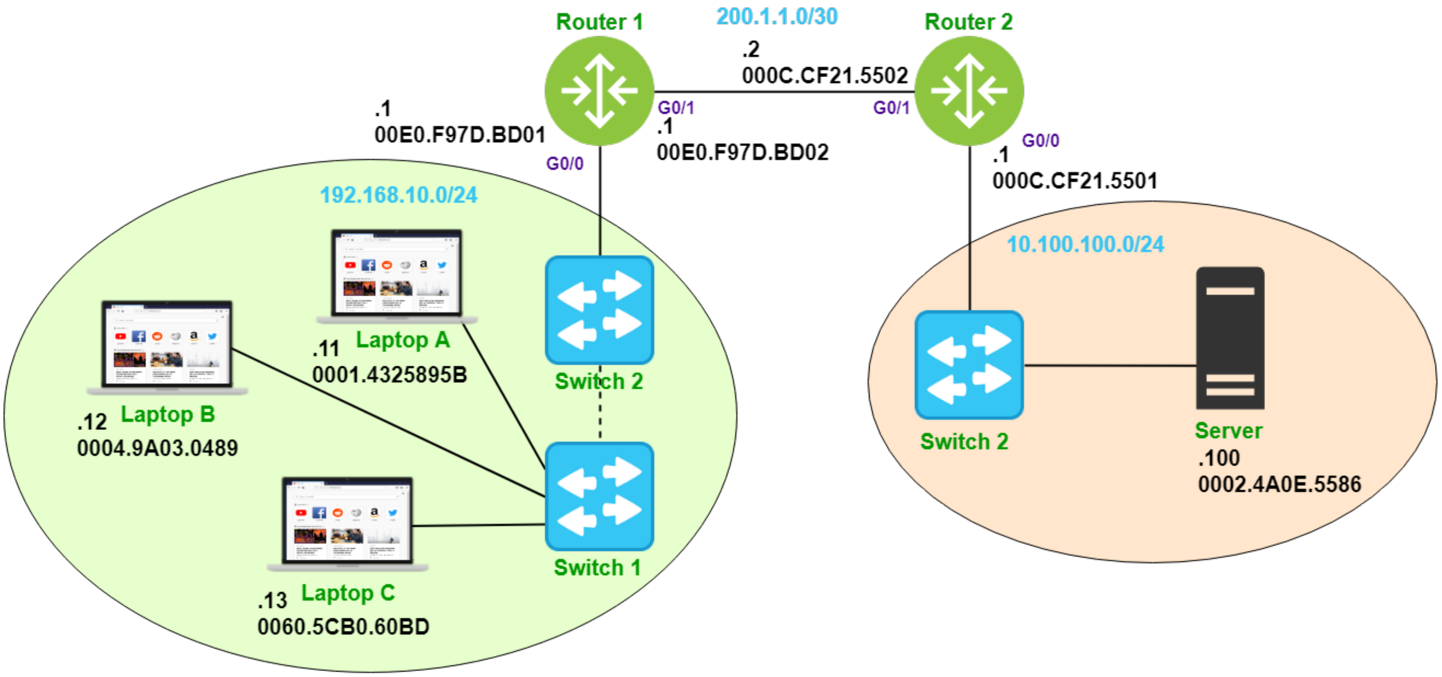
Lab 4 – ARP, LAGs & LLDP

Lab Topology and Learning Goals



Protocols are essential to network communications. Operating at every layer of the OSI model, protocols allow equipment from different vendors to interoperate. In this lab we explore protocols operating at layers 2 & 3 of the OSI model.

Lab Instructions and Required Resources

- Complete this lab in the Packer Tracer file: **INFO-6078 – Lab 4 – ARP, LAGs & LLDP.pkz**
- Take Lab Quiz: **Lab 4 - Requires Respondus LockDown Browser**

Lab 4 – ARP, LAGs & LLDP

Address Resolution Protocol (ARP) Operation

In most circumstances we reference network devices by logical (IP) addresses; however, network hosts send and receive communications using physical (MAC) addresses. ARP is used to find the MAC address of a provided IP address.

Simulation

- Edit the Event List Filters and include **ARP, ICMP** and **HTTP**
- On ALL laptops, open the command prompt and enter **arp -d** to clear the ARP tables
- Verify the ARP tables have been cleared with the **arp -a** command
- Press the Reset Simulation button to clear the **Event List** pane
- Open the **Command Prompt** on **Laptop A** and ping **Laptop B**
- Minimize the **Command Prompt** and open the ARP request in the **Event List**
- Switch to the **Outbound PDU Details** tab
- Observe the **Ethertype** field in the layer 2 header, as well as the details of the ARP request, paying attention to the MAC and IP addresses
- What does the target MAC address represent?
- Advance the simulation two steps, so the ARP request travels to the switch and then to the other hosts, notice the difference on behavior on **Laptop B** and **Laptop C**
- Advance the simulation two more steps so the response arrives at **Laptop A**
- Examine the ARP reply in the **Incoming PDU Details**
- The **ICMP** message is now ready for transmission
- Advance the simulation until all of the **ICMP** responses have been received
- View the ARP tables on **Laptop A** & **B**

Simulation

- On ALL end devices, open the command prompt and enter **arp -d** to clear the ARP tables
- Verify the ARP tables have been cleared with the **arp -a** command
- Press the Reset Simulation button to clear the **Event List** pane
- Open the **Web Browser** on **Laptop B** and open the web site located at www.fanshawe.ca
- Minimize the **Web Browser** and open the ARP request in the **Event List**
- Switch to the **Outbound PDU Details** tab
- Observe the details of the ARP request, paying attention to the MAC and IP addresses
- Why are these different to the previous simulation?
- Does the IP address represent the web server?
- Advance the simulation two steps, so the ARP request travels to the switch and then to the other hosts, notice the difference to the last simulation
- Advance the simulation and follow the HTTP traffic
- Can you find the servers MAC address in the ARP cache on **Laptop B**

Observe the effects of ARP on Intermediary Devices

Return to Realtime mode and generate some traffic on **Laptops A** & **C** by pinging the sever
Open the console on **Switch 1** and enter **privileged EXEC mode**

```
Switch1> enable
```

View the contents of the MAC address table on **Switch 1**

```
Switch1# show mac-address-table
```

Why does the switch not track IP addresses as the end devices do?

View the contents of the MAC address table on **Switch 2**

```
Switch2# show mac-address-table
```

Why are multiple MAC addresses associated with the same port?

View the contents of the MAC address table on **Router 1**

```
Router1# show mac-address-table
```

How many MAC addresses are listed? Why is this so?

View the ARP cache for **Router 1**

```
Router1# show arp
```

How does this differ from the MAC address table?

View the ARP cache for **Switch 1**

```
Switch1# show arp
```

Is the output what you would expect from a switch?

Configure Link Aggregation Group with Link Aggregation Control Protocol (LACP)

Networks are often designed with redundant links. In the event of a device failure or a damaged cable, redundant links can ensure the network continues to operate. Redundant link can however cause layer 2 loops in networks and normally Spanning Tree Protocol (STP) will disable one of the redundant links to prevent a loop forming. When a link is disabled, we lose the bandwidth that the link provides. Link aggregation can take multiple physical links and present them as a single logical link to the network, satisfying STP need for only a single live link between devices, while allowing more bandwidth for network traffic.

Observe the Effects of Spanning Tree Protocol (STP)

On Switch 1 & 2, observe the effects of Spanning Tree Protocol

```
Switch1# show spanning-tree
Switch2# show spanning-tree
```

Notice that **F0/24** will be in the **BLK** (blocking) state on Switch 2, this means that the port cannot send regular traffic and the bandwidth is restricted to that of a single link

Configure Link Aggregation Control Protocol (LACP)

Use the **interface range** command to create an LACP link aggregation group (EtherChannel) between Switch 1 and Switch 2

```
Switch1(config)# interface range f0/23-24
```

Explore the link aggregation configuration options

```
Switch1(config-if-range)# channel-group 1 mode ?
```

Configure LACP in active mode

```
Switch1(config-if-range)# channel-group 1 mode active
```

Configure Switch 2 in passive mode

```
Switch2(config)# interface range f0/23-24
Switch2(config-if-range)# channel-group 1 mode passive
```

Verify the Configuration of the LAG

Use the **show etherchannel summary** command to verify operation of the LAG

```
Switch1# show etherchannel summary
```

Using the legend at the top of the command results, verify that the pool is in use, and that both interfaces are participating in the pool.
For a link to participate in the pool, all links must share the same configuration.
Once a LAG is configured, all configuration changes should occur on the port-channel interface.

Configure the Load Balancing Method

By default, a Catalyst 2960 switch will load balance LAG traffic based on the source MAC address. Load balancing can be configured on a per-switch basis, with all LAGs using the same load balancing method.

Verify the Default Load Balancing Method

```
Switch1# show etherchannel load-balance
```

Modify the Load Balancing Method for Switch 1

View the available load balancing methods

```
Switch1(config)# port-channel load-balance ?
```

Set the load balancing method to source IP address

```
Switch1(config)# port-channel load-balance src-ip
```

Verify the load balancing method configured on both switches

(Lab Challenge): Add a Third Interface to the LAG

Connect a third cable using interface F0/22 on both switches. Add the interface to the LAG and troubleshoot as necessary.

Link Layer Discovery Protocol (LLDP) Operation

Link Layer Discovery Protocol (LLDP) is a tool used to assist with network management on Cisco and non-Cisco devices. LLDP allows network devices to advertise information about the device and features to neighboring devices.

View LLDP configuration

Cisco devices prefer the proprietary Cisco Discovery Protocol (CDP) over LLDP; as such LLDP is disabled by default on Cisco devices and needs to be enabled globally. For the purpose of our lab, LLDP has been enabled on all devices except Switch 2.

Enable LLDP on Switch 2

```
Switch2(config)# lldp run
```

On Switch 2 view the LLDP configuration

```
Switch2# show lldp
```

Note the values of the lldp configuration

View Neighbor Information Shared by LLDP

LLDP can display various details about neighboring devices such as hostnames, device type, local and remote interfaces and more

```
Switch2# show lldp neighbors
```

Observe the contents of the output. How could this command help you in your networking labs?

The **show lldp neighbor** command provides a summary of the information shared by the neighbor; to view the full extent of the information add the detail parameter to the command

```
Switch2# show lldp neighbors detail
```

Compare the output of the two commands

Compare CDP and LLDP Output

On Switch 2, compare the output of the **show LLDP neighbors** and **show CDP neighbors** commands

```
Switch2# show lldp neighbors
Switch2# show cdp neighbors
```

```
Switch2# show lldp neighbors detail
Switch2# show cdp neighbors detail
```

One benefit of CDP is that the IP address of neighboring devices is shared

Disable LLDP on a Per-Interface Basis

LLDP could cause security concerns if it is sharing device information on the wrong interface. It is considered a best practice to disable LLDP on interfaces at the network edge. LLDP can be disabled from transmitting, receiving or both.

On Router 1, disable LLDP on G0/0

Use the no lldp receive and no lldp transmit interface configuration commands to disable LLDP entirely on G0/0

```
Router1(config-if)# no lldp receive
Router1(config-if)# no lldp transmit
```

Verify LLDP has been disabled on G0/0 (this may take some time)

```
 Router1# show lldp neighbors
```