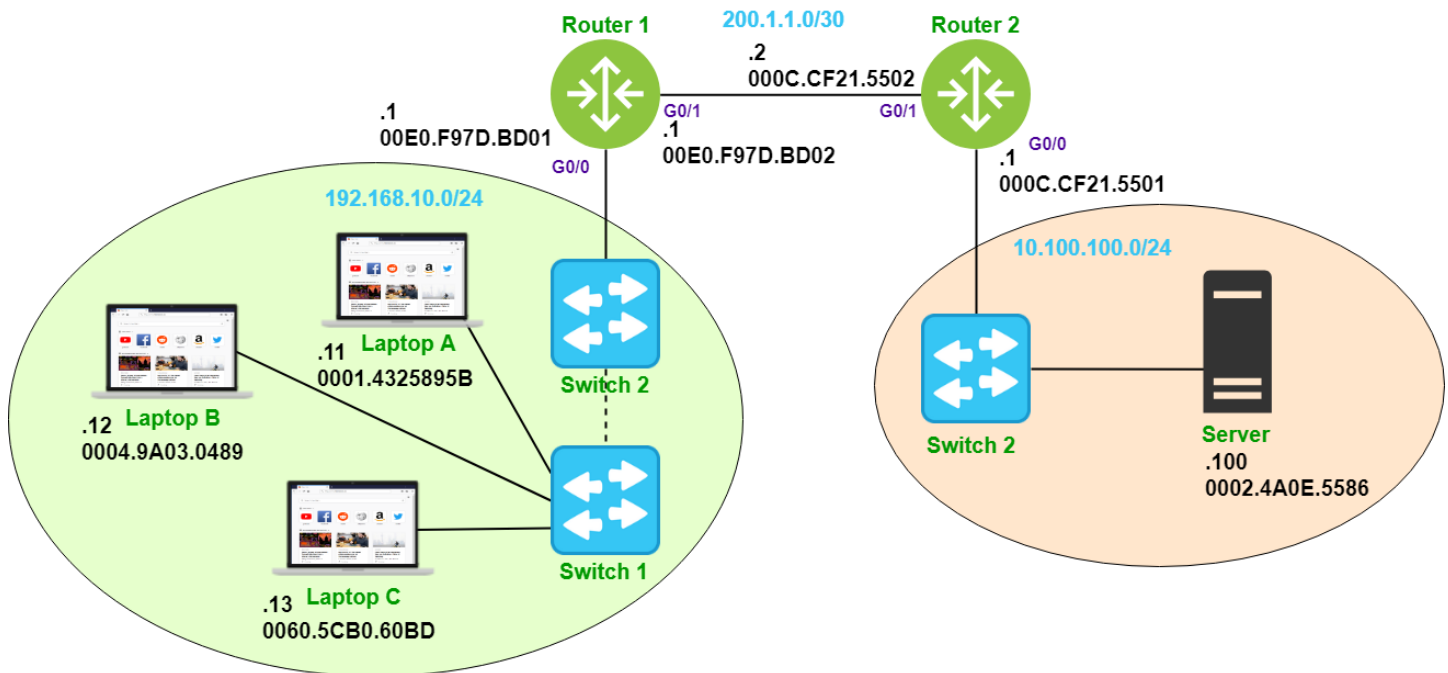


Lab 2 – OSI Model – Layers 2 & 3



Lab Topology and Learning Goals



Networks are often described in terms of layers (layers of the OSI model), in this lab we take a look at how the lower layers of the OSI model and the protocols within operate together to provide network communications.

Lab Instructions and Required Resources

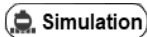
- Complete this lab in the Packer Tracer file: **INFO-6078 – Lab 2 – OSI Model – L2&3.pkz**
- Take Lab Quiz: **Lab 2 - Requires Respondus LockDown Browser**

Lab 2 – OSI Model – Layers 2 & 3



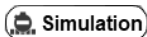
Investigate Unicast, Multicast and Broadcast Traffic

Most traffic that can be seen on networks is unicast (one-to-one), such as when you download a web page from a server. Multicast traffic allows a host to communicate with some, but not all members of a group. Multicast traffic is often used to manage communications for various dynamic routing protocols. Broadcast traffic allows a host to communicate with all members of a group. Broadcast traffic is useful when you don't have a unicast address for the host you are trying to communicate with.



Simulation Observe Unicast Traffic

- Switch Packet tracer to simulation mode
- Edit the Event List Filters and include **ICMP**
- Click on **Laptop A** and switch to the **Desktop** tab
- Open the **Command Prompt**
- At the prompt type: **ping 192.168.10.13**
- Minimize the command prompt and notice the envelope that has appeared next to **Laptop A**
- Click the envelope to open the PDU information and switch to the **Outbound PDU Details**
- Observe the destination and source MAC and IP addresses
- Can you determine the address types from the headers?
- Use the Play Controls to forward the ICMP message from **Laptop A** to **Switch 1**
- Again, click the envelope to open the PDU information and switch to the **Outbound PDU Details**, re-evaluate the destination and source MAC and IP addresses
- Use the Play Controls to forward the ICMP message from **Switch 1** to **Laptop C**
- Again, click the envelope to open the PDU information and switch to the **Outbound PDU Details**, re-evaluate the destination and source MAC and IP addresses
- Has anything changed?
- Use the Play Controls to follow the ICMP messages from **Laptop A** to **Laptop C**



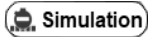
Simulation Observe Multicast Traffic

- Press the **Reset Simulation** button to clear the previous simulation
- Edit the Event List Filters, remove **ICMP** and include **OSPF**

Both R1 and R2 are preconfigured to exchange routing information via OSPF

- Press the Forward Play Control button to observe traffic between **Router 1** and **Router 2**
- Double-click the first packet in the **Event List** pane and switch to the **Outbound PDU Details**
- Notice the destination MAC and IP addresses
- Do an internet search to find out what the addresses represent

Lab 2 – OSI Model – Layers 2 & 3

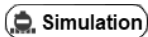


Simulation Observe Broadcast Traffic

- Press the **Reset Simulation** button to clear the previous simulation
- Edit the Event List Filters, remove **OSPF** and include **ICMP**
- Open the Command Prompt on **Laptop B** and send a ping to **192.168.10.255**
- Minimize the **Command Prompt**, open the PDU and switch to the **Outbound PDU Details**
- Observe the destination MAC and IP addresses
- Use the Play Controls to follow the ICMP messages; observe the hosts that respond to the echo request

Investigate Protocol Headers

When troubleshooting networks, it is often helpful to view the details of the underlying protocols to understand the cause of the network disruption. We will investigate the headers of information for layers 2 & 3 of the OSI model.



Simulation Observe Layer 2 & Layer 3 Headers

- Press the **Reset Simulation** button to clear the previous simulation
- Edit the Event List Filters, remove **ICMP** and include **HTTP**
- Open Web Browser on **Laptop C** and navigate to **www.fanshawe.ca**
- Minimize the browser and open the **HTTP** request in the Event List
- Switch to the **Outbound PDU Details** tab
- Observe the fields of the **Ethernet II** and **IP** headers, paying attention to the source and destination MAC and IP addresses, and the TTL
- What device does the destination MAC address describe?
- Advance the simulation so the PDU resides at **Switch 1**, observe the **Outgoing PDU Details**
- How has the Layer 2 header changed?
- Can you determine the VLAN the client devices are on?
- Observe the TTL and compare
- Advance the simulation so the PDU resides at **Switch 2**, observe the **Outgoing PDU Details**
- Notice that the Layer 2 headers have changed again
- Advance the simulation so the PDU resides at Router 1, observe the **Outgoing PDU Details**
- Take notice of the header addressing and the **IP TTL**
- Why has the **TTL** changed?
- Use the Play Controls to follow the HTTP messages to the **Server** and back, observing the changes to the header field at every step