Interconnecting the LANs

- Bridges
- Switches
- Routers
- Linking LANs
- Network Interfaces and Autonegotiation

Network Hardware

- In this chapter, we will be looking at three primary pieces of networking hardware:
  - Bridges
  - Hubs/*Switches*
  - Routers
- What each of these have in common is that they allow us to form linkages between separate *local area networks* (LANs)

Network Hardware

- We are starting to move upwards in the conceptual models.
  - Earlier, we have been dealing mostly with the OSI ***Physical*** layer, along with some references to the ***Data Link*** layer.
  - Now, we will be dealing more explicitly with the ***Data Link*** and ***Network*** Layers, corresponding largely to the ***Internet*** layer in the TCP/IP model

Bridges (Layer 2)

- A **bridge** is a Layer 2 (Data Link) device that allows us to forward data -- within and between two LANs -- based on MAC addresses.
- Imagine you have two segments of a network:
  - **Segment A:** Computers 1 through 4
  - **Segment B:** Computers 5 through 8
- Between those two segments is a bridge, with two ports.
  - ***Port I*** is connected to ***Segment A***
  - ***Port II*** is connected to ***Segment B***

Bridges (Layer 2)

- Each port will have certain *MAC addresses* associated with it, so that it knows to send a data packet to the correct segment.
  - This mapping of MAC addresses to port numbers is called a **bridging table** -- see, for example, Table 5-2 in the textbook.
  - The MAC address is stored when a device first communicates on the LAN *-- i.e., by transmitting a data packet.*
  - The record of a MAC address paired to a port number is called an **association**.

Bridges (Layer 2)

- A bridge will only forward data packets when there is an association, which reduces network traffic.
- The **Address Resolution Protocol** (ARP) is used to associate IP addresses (Network Layer) with MAC addresses (Data Link Layer) on a network.
  - First, an IP will be looked up in a host's **ARP table** or **cache**, which contains a list of associations. If the IP is present, then the packet will be forwarded to the associated MAC

Bridges (Layer 2)

- *Otherwise*, a **broadcast** will be sent out to all connected hosts, to see which machine has that IP.
  - If it is *found*, then a pairing will be recorded in the host's ARP table/cache.
  - Only a matching machine will respond to the ARP request.

- Types of bridges:
  - A **transparent bridge** connects two LANs running the same protocol
  - A **translation bridge** connects two LANs running different protocols. See, for example, ***Figure 5-3***

Bridges (Layer 2)

Advantages:

- Easy to install
- Excellent jobs in isolating network segments
- Inexpensive
- Can interconnect LANS with different protocols
- Reduces collision domains

Disadvantages:

- Works best in low-traffic areas
- Forwards broadcasts
- Susceptible to **broadcast storms**, leading to **network slowdowns**

Switches (Layer 2)

- In the previous section of the chapter, we examined the notion of a bridge - a Layer 2 networking device that forwards data based on MAC addresses
- As a reminder, there is also a Layer 1 device, called a *repeater*, that forwards a (strengthened) raw signal.
- A hub, as you recall, receives a transmission and broadcasts (i.e., repeats) it to all other connected devices.
  - For that reason, it is also called a multiport repeater. (Layer 1)
  - It has basic capability for connecting multiple hosts together, but all computers end up receiving all messages.

Switches (Layer 2)

- However, a hub is a *primitive* device; for that reason, it is no longer used much.
- A ***switch*** is a great improvement over a hub because it provides more direct links between hosts on a LAN. Like a bridge…
  - A switch is (usually) a Layer 2 device, so it uses MAC addresses to decide where to send data packets
  - It maintains a table of MAC addresses mapped to ports
  - It isolates data traffic to minimize congestion

Switches (Layer 2)

- For these reasons, a Layer 2 switch is also called a **multiport bridge**.
  - It can form *multiple, concurrent* data connections between hosts.
  - Because packets are not always broadcast to every host…
    - Less LAN bandwidth is used.
    - Transmission collisions are minimized.
  - There are the occasional cases of **multicast** and **broadcast** messages, which are sent to either a group of hosts or all hosts within the LAN

Switches (Layer 2)

- Our previous examples have looked at simple switches; you just plug them in, and they will do the rest.
- However, we also have a more complex variation in the form of **managed switches**.
- With a *managed* switch, the network administrator may have more oversight and control over who accesses -- or can access -- the LAN.
- Consider textbook example: A *Cisco Catalyst 2900 series* switch, along with the **Cisco Network Assistant (CNA)** software.

Switches (Layer 2)

- This allows the administrator to see which devices (i.e., their MAC addresses) are associated with which ports on the managed switch.
- The associations can be made in three ways:
  1. **Dynamic assignment** allows an association to be formed between a MAC address and a port on the switch upon connection.
  2. With **static addressing**, you can set the association manually.
  3. Finally, a **secure address** is one where only the device with the associated MAC address can successfully connect to the port. Otherwise, the port will be disabled.

Switches (Layer 2)

- If an association produces no data activity after a certain length of time, then it will be removed.
  - That time is called the **aging time**.
  - If you are administering the switch, you can adjust the aging time or disable it entirely.
- A **collision domain** is a part of a network where data packets can collide -- i.e. two or more devices try to send over the same segment, simultaneously.

Switches (Layer 2)

- Different kinds of devices handle this differently:
  - Hubs, for example, present this problem because they repeat data to all connected devices.
  - However, switches are able to alleviate this problem by providing direct data connections between networked devices.
  - This is called **isolating the collision domains**.
  - Depending on half- and full-duplex capabilities, using a switch may drastically reduce – or even *eliminate* – collisions.

Switches (Layer 2)

- Like bridges, a switch will maintain a table of associations between MAC addresses and ports.
  - As data packets come through, the switch will extract the MAC address and map it to the appropriate port.
  - This table is called **Content Addressable Memory (CAM)**.
  - When communication comes into the switch, the table will be used to direct data to the appropriate destination.
  - Again, an association that has no data traffic before its aging time elapses will be deleted. This allows the table associations to remain *fresh*.

Switches (Layer 2)

- **Flooding** is when the switch does not have the destination in CAM and, therefore, forwards the packet to all other ports.
- While switches minimize collision domains, they do not minimize **broadcast domains**.
- A broadcast sent over the network will still be forwarded by the switch to all networked devices.

Switches (Layer 2)

- A switch forwards data frames in two primary modes, along with a third "hybrid" mode:
  - **Store-and-forward**: Switch waits for entire data packet before deciding where to forward it.
    - This way, the switch can check for errors.
    - However, this creates the problem of **switch latency**, the delay between a packet entering the switch and then leaving.
    - **Video:** https://youtu.be/ALrnFnPyY-A

Switches (Layer 2)

- **Cut-through**: This will send the packet along as soon as the switch reads the destination MAC address
  - It is faster, but more errors can get through.
  - **Video:** **https://youtu.be/i_mLGmx1lVY**
- *Adaptive* cut-through**:** Here, the switch starts off using cut-through switching, but then changes to store-and-forward once the **error threshold** -- a number of errors in data packets -- has been reached.

Switches (Layer 2)

- Although switches are normally Layer 2 devices, a **multilayer switch (MLS)** can function in layers above that -- 3 and even higher.
  - It will forward packets based on IP addresses (Layer 3)
  - The forwarding is hardware-based -- allowing for **wire-speed routing**, where the data is processed as fast as it arrives at the switch.

Routers (Layer 3)

- In computer technology, we may speak of physical vs logical components:
  - ***Physical*** tends to be concrete; often referring to the actual material objects.
  - ***Logical*** often refers to something more abstract or virtual.
  - <u>Example:</u> A computer may have a physical hard drive, but…
    - It could be partitioned into two or more logical volumes…
    - Which the computer would treat like entirely separate drives

Routers (Layer 3)

- For a host on a network:
  - The physical address is the MAC address of the network adapter connecting that host to that network
  - The **logical address** is its IP address -- a.k.a., **network address** -- which identifies the locations of the network and of the host within it.
- This is where routers are distinguished from switches.
- *Switches* (working at Layer 2) forward data packets within a LAN, based on MAC (*physical*) addresses.

Routers (Layer 3)

- A ***router***, however, functions at Layer 3, forwarding data based on network (logical) addresses.
- Whereas switches (and hubs) establish LANs by interconnecting host devices, *routers interconnect LANs into larger networks*:
  - Different parts of a campus network (e.g. **`it.cs.umb.edu`** and **`cs.umb.edu`**)
  - **`Enterprise networks`** -- networks of large companies
  - Home networks to ISP

Routers (Layer 3)

- As a physical object, the **router interface** is where the router forms physical connections with a network.
  - It will have many different types of ports, but we will focus here on two types:
    - **Fast Ethernet (FA0/0, FA0/1 etc.)**: This is where you could provide Ethernet connections between the router and other network devices. We will use these in our lab exercises.
    - **Serial (S0/0, S0/1, etc.)**: These may be used in providing WAN connectivity
    - See ***Figures 5-15*** and ***5-16***, but don't get overwhelmed by the detail.

Routers (Layer 3)

- A router will essentially work in these steps:
  1. Receive data packet from host on network.
  2. Examine network address in packet.
  3. Consult its routing table to determine a path (via a particular port) to send it.
     - A **routing table** is an ongoing record of paths for forwarding data packets
     - The device on the other end (of the port) may be one of several types of devices: another router, a switch, a host, etc.
  - See ***Figure 5-19*** for an example

Routers (Layer 3)

- An inter-networked LAN will have a **gateway**, a device that allows them to communicate outside of the LAN.
  - This is the destination for IP addresses not inside the LAN
  - It will often be one of the router's network interfaces.
- The links between the LANs are called **network segments**.
  - They are often defined by links between internetworking devices, such as routers, hubs, switches.
  - They will be defined by, associated with, a *gateway address*, such as a router port.

Auto-Negotiation

- Different networked devices may be capable of *transmitting* and *receiving* at different speeds.
- For this reason, many internetworking devices -- hubs, switches, routers, etc. -- will engage in **auto-negotiation**.
  - Here, a data link speed is negotiated.
  - Configuration information -- i.e., possible connection speeds -- are communicated between devices over **fast link pulses (FLP)**.
  - They will agree upon the fastest speed that they are mutually capable of supporting.
- The connected devices will also negotiate **full-duplex** vs. **half-duplex** transmission modes.