Data-link Layer Devices

In this lecture we will focus on some of the most important layer 2 devices. These include:

1- Network Interface Cards
2- Bridges
3- Switches
4- Access Points

1- Network Interface Cards (NICs)

The Network Interface Card (NIC) or Network Interface Adapter is the component that provides the link between a computer and the network of which it is a part.

The network interface adapter, in cooperation with its driver, is a data- link layer device that is responsible of performing most of the functions of the data-link layer and the physical layer.

NIC Functions

NIC perform a variety of functions that are crucial to get data to and from the computer over the network. These functions include:-

- **Data encapsulation** : Data-link layer protocol of the NIC is responsible for building the frame around the data generated by the network layer protocol in preparation for transmission.
- **encoding and decoding:** The network interface adapter implements the physical layer encoding scheme. NIC converts the binary data generated by the network layer—now encapsulated in the frame—into proper electrical voltages, light pulses, or RF signals that the network medium uses, and converts received signals to binary data for use by the upper layer protocols.

- **Data buffering:** NICs have built-in buffers that enable them to store data arriving either from the computer or from the network until a frame is complete and ready for processing.
- **Serial/parallel conversion:** The communication between the computer and the network interface adapter usually runs in parallel (that is, either 16, 32 or 64 bits at a time), depending on the bus the adapter uses. (Only USB adapters communicate with the computer serially.) Network communications, however, usually serial, so the NIC is responsible for performing the conversion between the two types of transmissions.
- **Media Access Control (MAC):** Data-link layer protocol of the NIC also implements the MAC mechanism that the data-link layer protocol uses to regulate access to the network medium such as CSMA/CD and CSMA/CA

2- Bridges

Bridging is a technique used to connect networks at the data-link layer. A bridge is a physical unit, typically a box with two ports. It can be used to connect two existing LANs or to split one LAN into two segments.

Because a bridge functions at the data-link layer, it is capable of interpreting the information in the data-link layer protocol header. Data packets enter the bridge through either one of the ports, and the bridge then reads the destination address in each packet header and decides how to discard or relay the packet.

The use of the bridge (theoretically) cuts the unnecessary traffic passing over each network segment in half because packets not needed on the other network segment don't go there.

Bridges and Collisions

A collision domain is a network (or network part) that is constructed so that when two computers transmit packets at precisely the same time, a collision occurs. When you add a new hub to an existing network, the computers connected to that hub become part of the same collision domain as the original network because hubs relay the signals that they receive immediately upon receiving them, without filtering packets.

Bridges, on the other hand, relay signals to the other network depending on the MAC addresses. The two network segments connected by the bridge are thus said to be in different collision domains. On an Ethernet network, collisions are a normal and expected part of network operations, but when the number of collisions grows too large, the efficiency of the network decreases because more packets must be retransmitted. When the network is split into two collision domains with a bridge, the reduction in traffic on the two network segments results in fewer collisions, fewer retransmissions, and an improved efficiency.

Bridges and Broadcasts

The broadcast domain is another important concept in bridging technology. A broadcast message is a packet with a special destination address that causes it to be read and processed by every computer that receives it. A broadcast domain is a group of computers that all receive a broadcast message transmitted by any one of the computers in the group.

Adding a bridge separates a network into two different collision domains, but the segments on either side of the bridge remain part of the same broadcast domain because the bridge always relays all broadcast messages from both sides. This behavior mitigates the benefit of the bridge somewhat because a portion of the broadcast traffic being relayed is not utilized by the systems on the other side of the network. However, the retention of a single broadcast domain is what enables the two network segments to remain part of the same LAN.

Address tables

Bridges can forward or discard incoming packets by maintaining an internal address table that lists the hardware addresses of the computers on both segments. The bridge gets its information about the locations of the computers in different ways.

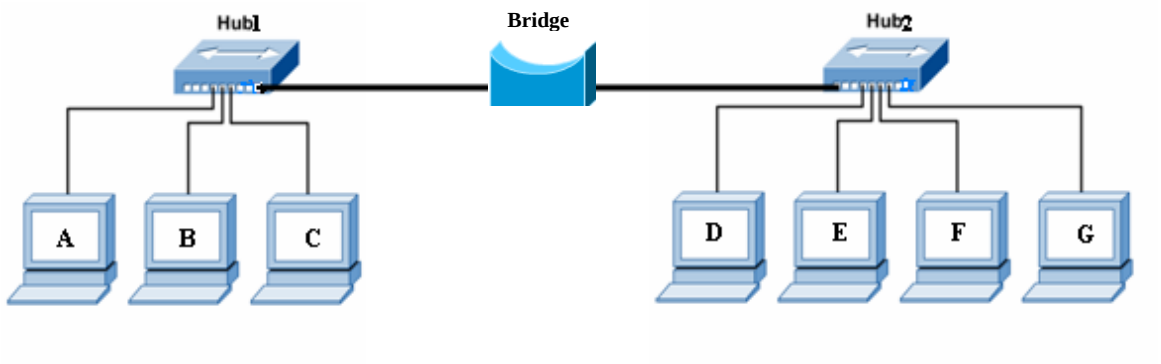
- **Manually:** Originally, network administrators had to manually create the lists of hardware addresses for each segment connected to the bridge and this was obviously an onerous chore.
- **Transparent Bridging**: bridges use a technique called transparent bridging to automatically or dynamically obtain their own address lists. Bridge operation can be understood via the following four processes:

  - **Learning:** When you activate a transparent bridge for the first time, it begins processing packets. For each incoming packet, the bridge reads the source address in the data-link layer protocol header and adds it to the address list for the network segment over which the packet arrived. This process is called learning.
  - **Packet filtering:** When a sufficient number of packets passes through the bridge to enable the compilation of the address tables, the bridge begins using them to selectively forward or discard packets. This process is known as packet filtering
  - **Aging**: A transparent bridge continuously updates its address table. It put a time stamp for each entry in the address table that when expired this entry is removed from the table. This is called aging.
  - **Flooding:** A frame that it is targeted to all nodes in the network (broadcast frame) or that have a destination address that is not in the address table is forwarded to the other segment, this process is known as flooding.

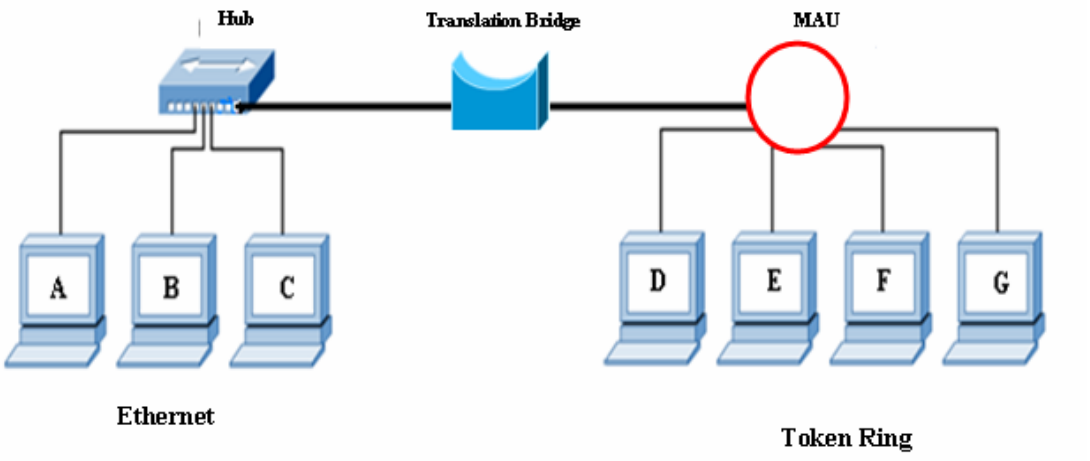
Note: It should be noticed that learning process depends on the source physical (MAC) address while filtering and flooding processes depends on the destination MAC address.

Types of Bridges

1- **Local Bridge**: it is a type of bridge used to connect network segments of the same type at the same location. This is the simplest type of bridge because it doesn't modify the data in the packets; it simply reads the addresses in the data-link layer protocol header and passes the packet on or discards it.



2- **Translation Bridge**: it connects network segments using different network media or different protocols. This bridge is more complicated than a local bridge because, in addition to reading the headers in the packet, the bridge strips the data-link layer frame off the packets to be relayed to other network segments and packages them in a new frame for transmission on the other segment. Because of the additional packet manipulations, translation bridging is slower than local bridging, and translation bridges are more expensive as well.



3- **Remote Bridge:** is designed to connect two network segments at distant locations using some form of WAN link such as modem connection. The advantage of using a bridge in this manner is that you reduce the amount of traffic passing over the WAN link.

3- Switches

The switch is another type of data-link layer connection device, which has largely replaced the bridge in the modern network. Switch indeed is a multiport bridge.

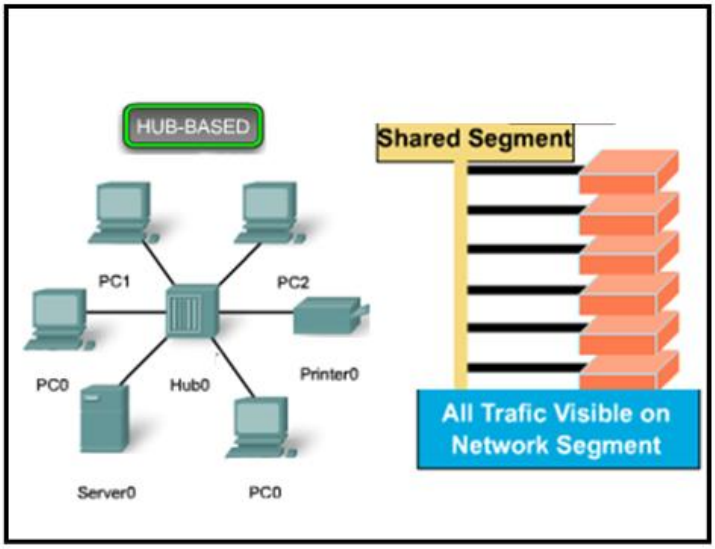
The difference between a hub and a switch is that a hub forwards every incoming packet out through all of its ports except the port connected to the source of the frame while the switch forwards each incoming packet only to the port that provides access to the destination system.

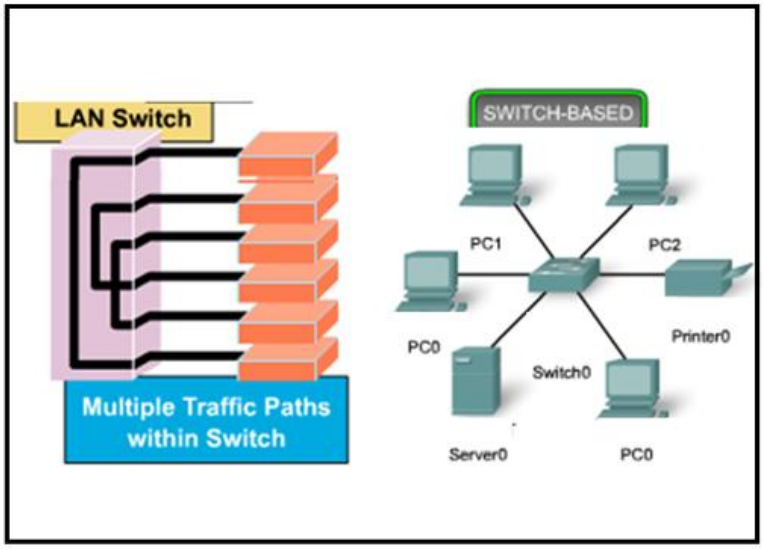
Broadcast and Collision Domains

Because they forward data to a single port only, switches essentially convert the LAN from a shared network medium to a dedicated one. If you have a small network that uses a switch instead of a hub (such a switch is sometimes called a switching hub), each packet takes a dedicated path from the source computer to the destination. Switches still forward broadcast messages to all of their ports, but not unicasts and multicasts.

Note

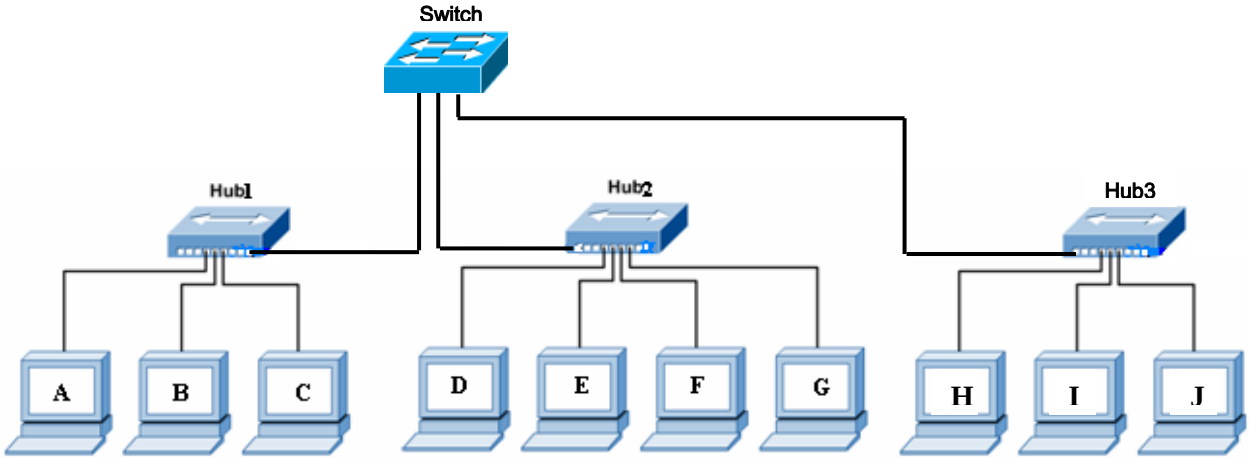
Switches usually provide inter connections to more than two pairs of devices at the same time. An *(N)* port switch can theoretically *(N/2)* simultaneous connections.



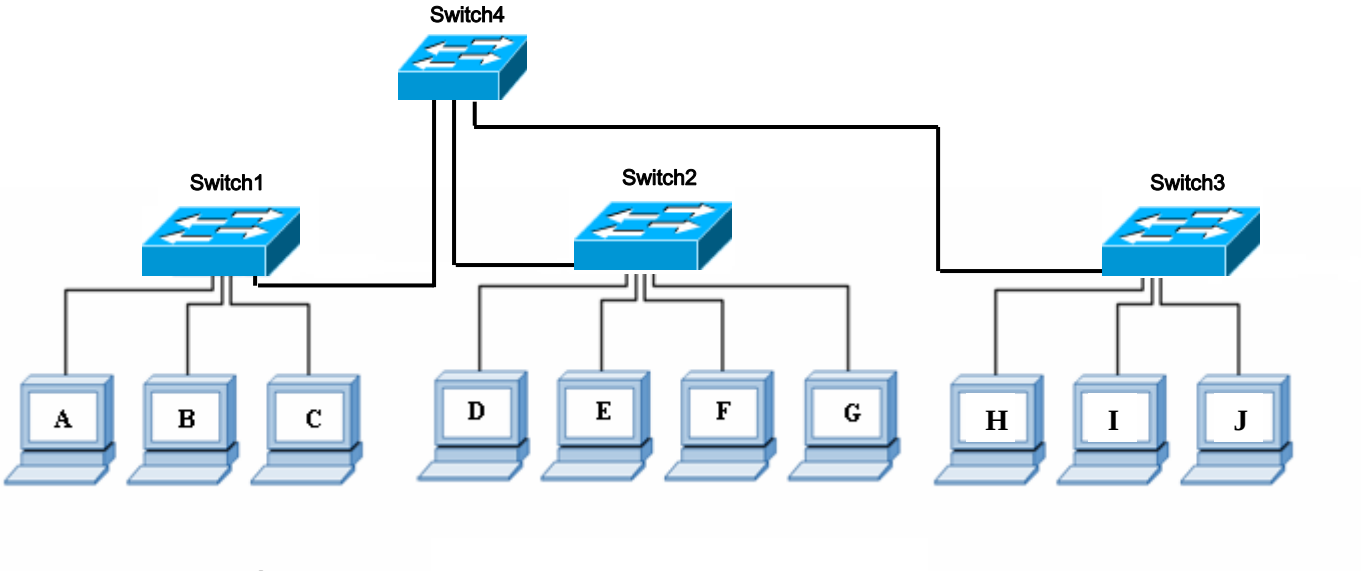


Installing Switches

There are many different ways to install switches. For example, you don't have to replace all of the hubs with switches at one time. For example, you can continue to use your standard shared network hubs and connect them all to a switch. This increases the efficiency of your internetwork traffic.



On the other hand, if your network tends to generate more traffic within the individual LANs, you can replace the workgroup hubs with switches to increase network efficiency.



Types of Switches

There are two basic types of switches:

1- **Cut-through Switch**: which forwards packets immediately by reading the destination address from their data-link layer protocol headers as soon as they're received and relaying the packets out through the appropriate port with no additional processing. The switch doesn't even wait for the entire packet to arrive before it begins forwarding it. This type of switch is relatively inexpensive and minimizes the delay incurred during the processing of packets by the switch (which is called latency).

2- **Store-and-forward Switch**: that waits until an entire packet arrives before forwarding it to its destination. This type of unit can be a shared-memory switch, which has a common memory buffer that stores the incoming data from all of the ports, or a bus architecture switch, with individual buffers for each port, connected by a bus. While the packet is stored in the switch's memory buffers, the switch takes the opportunity to verify the data by performing a CRC. This checking naturally introduces additional delay into the packet forwarding process, and the additional functions make store-and-forward switches more expensive than cut-through switches.

4- Access Point

AP is Data-link Layer device that connects wireless communication devices together to create a wireless network.

A wireless access point acts as the network's arbitrator, negotiating when each nearby client device can transmit.

At the same time Access points are bridges between the wireless world and the wired world. As Bridges, all access points have features that one would expect to see on a network bridge. They have at least two network interfaces: a wireless interface that understands the details of 802.11 and a second interface to connect to wired networks. To take advantage of the installed base, the wired interface is almost always an Ethernet port.

Many access points also offer the option of using external antennas to further boost range. Bridges have some buffer memory to hold frames as they are transferred between the two interfaces, and they store MAC address associations for each port in a set of internal tables as mentioned in bridges section of this lecture.