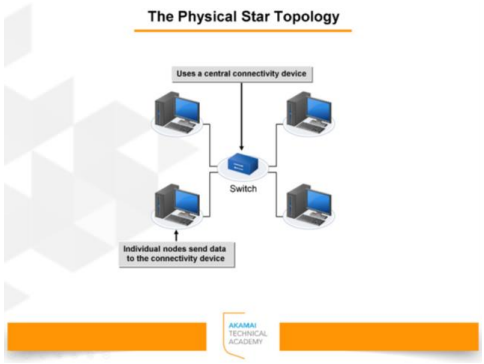
Switches
Hubs

It's possible to connect two devices with a wire (or wireless) like you did in the Network Theory lab. However, networks usually have a lot more than two devices. In Ethernet networks, the network typically uses a central device to connect all the nodes. This redistribution point takes the data coming in and sends it to the receiving nodes. When all the nodes are connected to a central device, this is known as a star physical topology.



Early networks used devices called hubs. Hubs are also known as repeaters. That's because these Layer 1 devices take the incoming signals and send it to all the ports on the hub.

The only problem with hubs is caused by the very nature of how they work. If a node sends data to the hub, it repeats the data to all the ports. That means that if any other node was about to transmit, there will be a collision. Then both nodes will have to wait for a random time delay. The more devices connected to the hub, the more collisions the hub will have. The more collisions on the network, the slower the network runs. "Collision domain" is the term that describes all the nodes who can create a collision with each other. When you use a hub, all the devices are in one big collision domain.

Modern networks don't use hubs, they use switches.

Switches

Switches can also receive incoming data and send it to other nodes. When the switch first turns on, it acts like a hub. It sends all the data to all the nodes. This is called "flooding" the data.

To properly address data, the sending node must find the receiving node's MAC address. Typically, the sending node has only the IP address of the receiving node. To find the MAC address of the NIC with a particular IP address, nodes use a protocol called Address Resolution Protocol (ARP).

To resolve the receiving node's IP address to its MAC address, the sending computer sends out an ARP broadcast. Suppose the sending computer needed to know the MAC address of a receiving computer with an IP address of 192.168.1.10. It would send an ARP broadcast, "192.168.1.10 what is your MAC address?" The switch sends all broadcasts to all ports. If 192.168.1.10 is on the network, the ARP broadcast reaches the device. It responds by providing the sending device with its MAC address.

As ARP broadcasts go through the switch, the switch makes a note of which MAC address(es) are on each port. The switch stores this information in its Content Addressable Memory (CAM) table. When data comes in, the switch looks at the destination MAC address. If the CAM table lists a port for that MAC address, the switch sends the data just to that one port. Because switches send data based on the MAC address, they are Layer 2 devices.

Because switches send the data to just the one port with the receiving node, that is the only device that could have a collision with the data. Therefore, each port on the switch is a separate collision domain.

Replacing a hub, where all the ports are one big collision domain, with a switch, where each port is a collision domain, can really speed up a network.

Managed Switches

Managed switches have firmware. The firmware functions as an operating system that can be used to program the switch with security features.

Packet Sniffers

Packet Sniffers allow administrators to capture network traffic. Then the administrator can examine the actual data passing across the network.

To capture traffic, the switch needs to send the data to the packet sniffer. However, the switch will only send data to the packet sniffer if the sniffer's MAC address is listed as the receiving node.

To allow packet sniffers to collect all the data on a switch, administrators must configure port mirroring on the switch. This tells the switch to copy (mirror) all the data passing through the switch to one port.

By default, NICs ignore data that is not either a broadcast or addressed to their MAC address. When administrators install a packet sniffer on a computer, they must tell the NIC to process all the incoming data even if it's not a broadcast or addressed to the node's NIC. They do this by putting the NIC into promiscuous mode. In promiscuous mode, the NIC sends all the data up the protocol stack to the packet sniffer.