Internetworking devices

We are used to the jargon of networking devices like Repeaters, Hubs, Bridges, Routers, Brouters, Gateways, Switches. What are these devices? Whar is the difference between these devices? Let's checkout these devices in detail.

Repeaters are Internetworking devices which operate at the physical layer. It deals with signal reproduction and retransmission of data. A simple amplifier will amplify not only the signal but also any noise accompanying the signal. But a repeater strips the digital data & saves it. It then reconstructs and retransmits the signal. The new signal is an exact duplicate of the original transmitted signal, able to travel over the new network segment. A repeater does not incorporate any changes to, or even analysis of, the addressing or structure of the data associated with other layers (higher). It simply reconditions received data & passes it on.

Ethernet Hubs: Hubs are nothing but multiport repeaters. Any signal received on one port gets retransmitted on the other ports of the Hub. In general hubs are stable devices that perform signal regeneration, packet forwarding, routing and other functions adequately. Some hubs even have a management module which have an added function of a network manager.

Ethernet Hubs can also be used as repeaters which extend the segment length of the particular type of cable that is used. For thinnet it is used primarily for extending the segment length. But in the case of Twisted Pair the repeater or the Hubs are a must. IEEE has specified standards for the Repeater or Hub functions.

The major characteristics of the Hubs are:

? The Hub should **regenerate** and **retime** the signals on its ports.

? When Two or more ports connected to the Hub go active then the Hub should detect the collisions and transmit a **Jamming Signal** on all other ports.

? When there is a excess collision on one of the ports, the Hub should monitor that port and disconnect the port. At the same time it should monitor that particular port and should reconnect that as soon as that excess collision activity is stopped. This is called as **Partitioning** of a port.

In addition, **twisted pair hubs** have the following characteristics:

? **Link Test Function**: Sending and detecting the Link Test Pulses to monitor the connectivity of a node to the Hub.

? **Polarity Reversal Correction**: or the capability to detect the receive cable reversal and correct the fault.

HCL-HP's **BeeHub-XL** which has eight twisted pair, one BNC/AUI port. This is compatible to IEEE 802.3 repeater standard. This also has Auto Partitioning, Reconnect-ion & Auto Polarity Reversal Correction.

Intelligent/Manageable Hubs have CPUs that allow Net Managers to control/modify the setting of the Hub. These Hubs have 8-16 ports and are typically stand-alone type. The on-board CPUs do the diagnostics and display the status. Most of them support SNMP management and the management control can be through Ethernet or Serial ports. These are used for large to medium size Enterprise networks.

Stackable Hubs are similar to Intelligent hubs but due to the capability of stacking they can logically form a single Hub with ports ranging up to 96. The stackability is implemented in terms of stacking the modules or pluggable daughter board on to a mother board. SNMP in supported by default on these types of hubs. These hubs are used in large enterprise networks.

Bridge is used to connect two LAN segments at the Data Link Layer. Bridges can determine the **physical addresses** of the source and destination stations involved. Once determined, bridges can permit or deny access to the new segment based on physical address. Unlike repeaters, Bridges are selective about the traffic they allow through.

Bridges are usually used to divide a too-busy network into separate segments. After such a division, the bridge prevents traffic internal to one segment, from reaching other segments. As long as inter segment traffic is not too heavy, this effectively reduces traffic on each segment. Since the Bridges store & forward data, they can analyse address fields in the frames and forward the data based on the database contained in the Bridge.

Routers have access to information from all three lower OSI layers (Physical, Data Link & Network).Routers offer more functionality as compared to Bridges, in being to do, routing and management of traffic & filtering the data across the network. Routers send information using **logical** address information. Logical addresses are assigned normally

by the network administrators whereas physical addresses are assigned by the hardware manufacturer.
Routers use one (or more) specific routing algorithms to calculate the best path. Paths may be calculated in real time, so that they can constantly adjust to changing network conditions. Routers are typically much more processing intensive than bridges. As a result, their processing speeds(measured in packets forwarded/sec) are not usually as high.

Many modern routers are really **Brouters**. Brouters are essentially routers that can also bridge. A brouter will first check a packet to see if it supports the packet's routing algorithm. If not, rather than simply dropping the packet, the packet is bridged using layer 2 information.

Some bridge manufacturers have attempted the opposite compromise by adding some router capabilities to their bridges. These devices are usually called **routing bridges**. They can perform some minimal intelligent path selection and can also offer some of the increased security of routers. Since they still do not have access to layer 3 information, however, they can't really route in the same way that routers can.
It is better to use routers for segmenting WANs & Switches for segmenting LANs.

Ethernet Switches

When the number of nodes on a particular Ethernet segment goes up, the available bandwidth comes down for each node. This is because of the fact that Ethernet works on shared medium rule. An Ethernet Switch provides dedicated bandwidth to every port connection. It improves performance through micro-segmentation - reducing the number of users per segment and so increasing the available bandwidth of the LAN for each user. Delay from input to output of a switch is very less when compared to Bridges.

It achieves this by routing the data to the port that connects the Node whose address is in the destination address portion of the Ethernet packet. Using this address, the switch can send the packet to the desired destination port only. This results in reduced traffic on the other ports and higher total throughput. In the traditional hubs and repeaters, the data packets are sent to all ports that is, similar to connecting nodes on the same segment.
A switch automatically learns the identity of attached end-stations, so no configuration is necessary. This makes switches much simpler to install and use than routers. Since the decision making is hardware-based, it results in higher performance.

Port Switches: In this type of switch, every port is intended to connect to a single end station or a server. Port switching is merely an electronic patch panel function, not the genuine switching capability that provides a performance boost. Port switching lets administrators configure their networks to allocate any port to any backplane segment on their hub. Unlike true switching, it does not increase the bandwidth available to the users or servers. What is more, changing users from one backplane segment to another can be dangerous, particularly in routed networks. The path that the user's data needs to take may be increased by moving from one segment to another, or data transmissions may be stopped altogether if a device has moved from one routed subnet to another.
Port Switching is useful for data intensive applications such as Client-Server computing, imaging, CAD/CAM, desktop video conferencing and multimedia.

Segment switching: In this type of switch, each port is connected to a Ethernet segment directly or through Hub(if the nodes have a 10base T interface). Since each port of the Ethernet switch is connected to a segment, each port has to support large number of Ethernet addresses. Normally it is 256 to 1024. The advantage of the segment switch is that it increases the bandwidth available to the nodes, by providing "on-the-fly" 10Mbps link on a packet basis to the respective segments. The process of splitting a large segment into smaller segments but still maintaining the whole as a logical segment is called as "segmentation".

Gateway: Gateway interconnects two or more subnetworks that use different protocols above the network layer. Gateways can connect any network to any other network.
They provide full range of functionality from bit handling at the physical level up through framing, error detection routing, flow control, etc.

Suppose a PC network using Netware is to be connected to an SNA network consisting of several terminals. Not only is the hardware different, but the entire structure of the data and many of the protocols used are different. A Gateway translates between the different Transport, Session, Presentation, & Application Layer Protocols, altering as much of the entire data message as needed.