Chapter 4: Network Layer

Internetworking & Devices: Repeaters, Hubs, Bridges, Switches, Router, Gateway

Repeaters are used in transmission systems to replicate or regenerate analog or digital signals distorted by transmission loss. Analog Repeaters frequently can only amplify the signal while Digital Repeaters can reconstruct a signal to near its original quality. In a data network, a repeater can relay messages between subnetworks that use different protocols or cable types. Hubs can operate as repeaters by relaying messages to all connected computers. A repeater cannot do the intelligent routing performed by bridges and routers.

Hubs are very similar to repeaters. A Hub is essentially a multiport repeater. Any electrical signal that comes into one port, goes out all other ports. Hubs are fundamentally used in networks that use twisted pair cabling to connect devices. They act as pathways to direct electrical signals to travel along. Hubs can be categorized into Passive Hubs and Active Hubs. A passive hub is just a connector, it just splits the signal. No need for a power supply. An active hub is actually a multiport repeater, which can amplify or regenerate the information signal.

Switches are more advanced than hubs. A switch, when compared to a bridge, has multiple ports. Switches can perform error checking before forwarding data. They are very efficient by forwarding good packets selectively to correct devices only by checking MAC address in a table, otherwise, they transmit to all. Switches can support both layer 2 (based on MAC Address) and layer 3 (Based on IP address) depending on the type of switch. Usually, large networks use switches instead of hubs to connect computers within the same subnet.

Bridges are Data Link Layer devices. A bridge is more complex than a hub. A bridge maintains a MAC address table for both LAN segments it is connected to. A bridge has a single incoming and outgoing port. It filters traffic on the LAN by looking at the MAC address. Data filtering is done by the bridge, which looks at the destination address before forwarding, unlike a hub. It restricts transmission on other LAN segments if the destination is not found. Bridges are used to separate parts of a network that do not need to communicate regularly but need to be connected.

Routers are devices that forward packets based on address. A router uses the IP address to forward packets. This allows the network to go across different protocols. Routers forward packets based on software while a switch (Layer 3 for example) forwards using hardware called ASIC (Application Specific Integrated Circuits). Routers support different WAN technologies but switches do not. Wireless Routers have Access Points built in. The most common home use for routers is to share a broadband internet connection. The router has a public IP address, and that address is shared with the network. When data comes through the router, it is forwarded to the correct computer.

Gateways are also routers, which forward the traffic of a subnetwork to other networks or to the internet. A gateway acts as an intermediary device between computers in the subnet with other computers outside the subnet. All the traffic to the outside of the subnet must go through the gateway. Gateways are also useful in forwarding traffic from one ISP (AS) to the other; those are called border gateways.

Addressing: Internet Address, Classful Address

An Internet address uniquely identifies a node on the Internet. Internet address may also refer to the name or IP of a Web site (URL), someone's e-mail address. In classless addressing, variable-length blocks are assigned that belong to no class. In this architecture, the entire address space (232 addresses) is divided into blocks of different sizes.

Classful addressing is based on the default Class A, B, or C networks. All devices in the same routing domain must use the same subnet mask. Since routers running a classful routing protocol do not include subnet mask information with routing updates, the router assumes either its own subnet mask or defaults to the classful subnet mask.

Classless addressing, on the other hand, allows the use of variable-length subnet masks, or Variable-Length Subnet Masking (VLSM), because subnet mask information is included with routing updates. You can have a mixture of different subnet masks in the same routing domain.

Subnetting

Subnetting is a process of dividing a large network into smaller networks known as subnets based on layer 3 IP address. Every computer on the network has an IP address that represents its location on the network. Two versions of IP addresses are available: IPv4 and IPv6.

Routing: Techniques, Static vs. Dynamic Routing, Routing Table for Classful Address

Routing is the process of selecting a path for traffic in a network, or between or across multiple networks. Routing is performed for many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), computer networks, such as the Internet, as well as in networks used in public and private transportation, such as the system of streets, roads, and highways in national infrastructure.

Routing Protocols: RIP, OSPF, BGP, Unicast and Multicast Routing Protocols

RIP (Routing Information Protocol) is the distance vector routing protocol which means that each router may not know where the final destination network is, but it does know in which direction it exists and how far away it is. It employs the hop count as the routing metrics. Hop count is the number of a router the packet must travel till it reaches its destination. RIP uses the hop count to determine the best path between the router/location. Each router contains the RIP table, and the table is updated every 30 seconds. Each router broadcasts its entire RIP table to its neighbor.

OSPF (Open Shortest Path First) is the routing algorithm that uses the link state routing algorithm. It is the shortest path algorithm to calculate the best path from the source to the destination. OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks. It falls into the group of interior routing protocols, operating within a single autonomous system (AS). OSPF doesn't need high memory and high-speed processor.

BGP (Border Gateway Protocol) is the Exterior Gateway Protocol which is used for communicating information among autonomous systems (AS is the unit of router policy, either a single network or a group of networks that is controlled by a common network administrator (or group of administrators) on behalf of a single administrative entity (such as a university, a business enterprise, or a business division),) on the Internet. BGP is the routing method that enables the Internet to function. Without it, we wouldn't be able to do a Google search or send an email. Neighboring BGP routers i.e. BGP peers

exchange detailed path information. It is also called the path vector routing algorithm. The protocols are more concerned with reachability than optimality.

Routing Algorithms: Shortest Path Algorithm, Flooding, Distance Vector Routing, Link State Routing; Protocols: ARP, RARP, IP, ICMP

Flooding is the simplest method of packet forwarding. When a packet is received, the routers send it to all the interfaces except the one on which it was received. This creates too much burden on the network and lots of duplicate packets wandering in the network. Time to Live (TTL) can be used to avoid infinite looping of packets. There exists another approach for flooding, which is called Selective Flooding to reduce the overhead on the network. In this method, the router does not flood out on all the interfaces, but selective ones.

The shortest path algorithm is a technique that uses various algorithms to decide a path with a minimum number of hops. Common shortest path algorithms are Dijkstra's algorithm and Bellman Ford algorithm. The shortest path algorithm finds the shortest paths between routers/nodes in a graph. The widely used shortest path algorithm is Dijkstra's shortest path algorithm.