

Computer Network

Network Devices

Router

Routers are devices (computers) containing software that help in determining the best path out of the available paths for a particular transmission. They consist of a combination of hardware and software. The hardware includes the physical interfaces to the various networks in the internetwork. The two main pieces of software in a router are the operating system and the routing protocol.

A router between two LANs receives messages from both networks, checks their destinations, and transmits the messages to the required LAN. Since messages are stored in the routers system before re-transmission, routers are said to implement a store-and-forward technique.

Routers use logical and physical addressing to connect two or more logically separate networks. They accomplish this connection by organizing the large network into logical network segments or sub-networks. Each of these sub-networks is given a logical address, which allows the networks to be separate but still access each other and exchange data when necessary. Data is grouped into packets, or blocks, of data. Each packet, in addition to having a physical device address, has a logical network address.

Routing is the function of the network layer of the OSI model. Routing means that finding route or the next hop for a packet. A device called router does the routing function. It uses a table called routing table to find the route to the packet's final destination. Routing tables contain information about the potential paths that a data packet should take to travel through the internetwork and reach its destination. To view the internal routing table type route print at the command prompt.

Routing functions

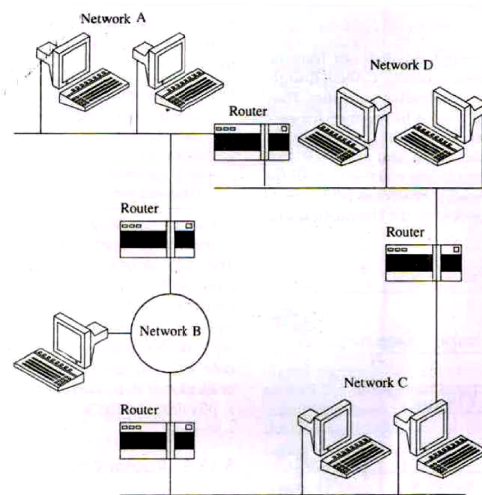
Router has to read the header of each packet that arrives and extract the destination address of the packet. The router then sends the packet out on the appropriate transmission path based on a calculation of the optimum route to that destination. Routing involves two main functions. These are:

- (a) Forwarding Function
- (b) Filtering Function

Forwarding Function

When packets need to be sent to a host or hosts on another network, they are forwarded to a router that is connected to that particular local network. The router to which the packet is forwarded will then check its routing tables to determine the path the packet should take. Packets are usually sent along the path with the lowest cost value or metric. The routing metric mainly includes the following:

- (a) **Hop Count:** The number of intermediate routers between a given network and the local router.



- (b) **Latency:** The time delay in processing a packet through the router or over a given route.
- (c) **Congestion:** The length of the packet queue at the incoming port of the router.
- (d) **Load:** The processor use at the router or the number of packets per second that it is currently processing.
- (e) **Bandwidth:** The available capacity of a route to support network traffic. It decreases as network traffic increases.
- (f) **Reliability:** The relative amount of downtime that a particular router might experience because of malfunctions.
- (g) **Maximum Transmission Unit (MTU):** The largest packet size that the router can forward without needing to fragment the packet.

Routing Process: If a sender on the local network needs to send a packet to a receiver on a remote network, it first checks its own internal routing table to determine which router to contact. It then uses Address Resolution Protocol (ARP) to obtain the MAC address of the router. The sender then sends the packet directly to this local router.

The network layer header of the packet contains the logical network address (the IP address on a TCP/IP internetwork) of the receiver. The router receives the packet, inspects the IP address and compares the address with the route information stored in its routing table. From the information in the routing table, it forwards the packet to another router, which forwards it again until the packet, finally reaches its destination network. The router at the final destination then passes on the packet to the receiver node.

Filtering Function

Filtering is the process of controlling the flow of packets based on attributes such as source address, destination address, type, length, and port number.

Filtering is done to protect the work from unauthorized traffic. Network administrators can create rules for filtering out unwanted packets. A packet that satisfies all the rules is allowed to be transmitted, while a packet that violates any of the rules is dropped. Packet filtering can be implemented in the following two ways:

- (a) Static Filtering
- (b) Dynamic Filtering

Static Filtering: In Static Filtering, ports are configured as either permanently open or permanently closed. For example, to deny outside packets access the company's intranet server on port 80, one can configure the router to block all incoming packets directed towards port 80.

Dynamic Filtering: In Dynamic Filtering, selected ports can be opened for authorized access and closed for others. These ports are opened at the start of a legitimate session and then closed at the end of the session to secure the port against unauthorized attempts. One can configure rules in the router:

- (a) to read the incoming packets,
- (b) dynamically open the two ports to allow a session to be started,
- (c) monitor the flow of packets to ensure that no attempt is made to hijack the session by an unauthorized user
- (d) Close the randomly assigned ports when the session ends.

Routing Methods (Static and Dynamic Routing)

Static Routing: In static routing method, routing tables are manually configured by the network administrator. Static routing is used in smaller networks that contain only a smaller number of routers or where security is a major concern. Routers that use static routing are

called static routers. Each static router must be configured and maintained separately because static routers do not exchange routing information with each other.

The routing table must contain a route for every network in the internetwork. It is more immune to any hampering by hackers since the network administrator controls the configuration of the routing table.

Dynamic Routing: Dynamic Routing is a routing mechanism which is handled by a routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF) Protocol etc described earlier. These protocols dynamically exchange routing information among routers on an internetwork. Routers that use these methods are called dynamic routers.

A routing protocol is installed on each Dynamic Router. The routers periodically exchange their routing information so that if the internetwork is reconfigured or a router goes down, the routing tables of each router are modified accordingly.

Dynamic routers are less secure because routing tables can be hampered by hackers. If the network is reconfigured or a router goes down, it takes time for this information to propagate between the various routers on the network. Routing protocols also create additional network traffic.

Exercise:

Q1: What is Router?

Q2: Write the advantage of Router.

Q3: What is Forwarding Function of router?

Q4: What is Filtering Function of router?

Q5: What is dynamic routing?

Q6: What is static routing?