ANNEXURE-2

SearchNetworking.com

router

By Margaret Rouse

A router is a physical or virtual appliance that passes information between two or more packet-switched computer networks. A router inspects a given data packet's destination Internet Protocol address (IP address), calculates the best way for it to reach its destination and then forwards it accordingly.

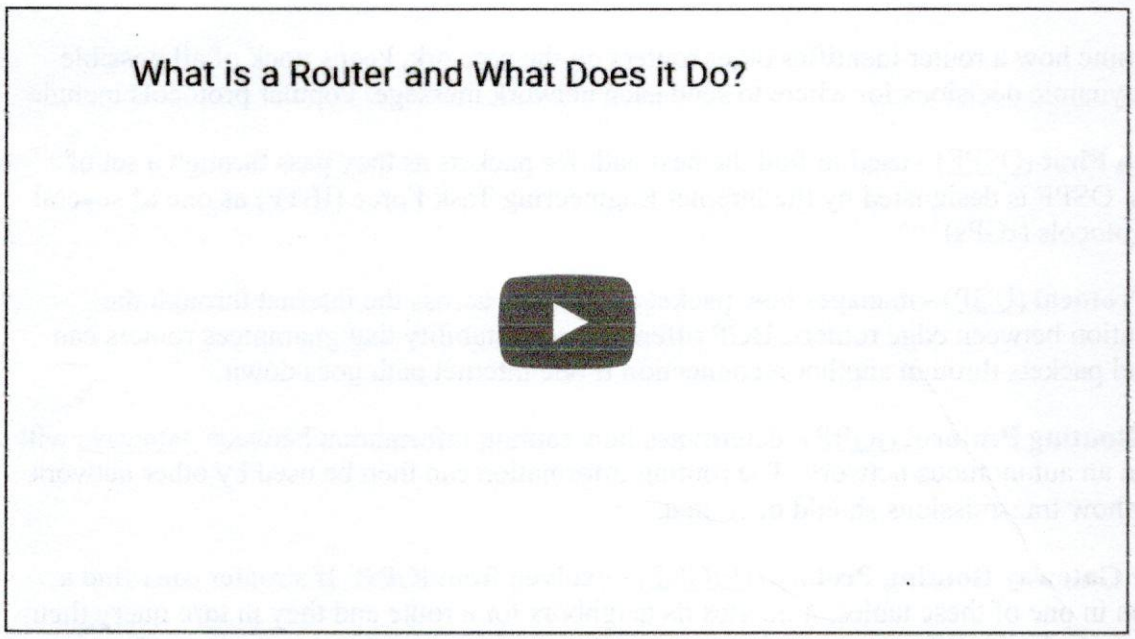
A router is a common type of gateway. It is positioned where two or more networks meet at each point of presence on the internet. Hundreds of routers might forward a single packet as it moves from one network to the next on the way to its final destination. In the Open Systems Interconnection (OSI) model, routers are associated with the network layer (Layer 3).

Traditional routers are stand-alone devices that use proprietary software. In contrast, a virtual router is a software instance that performs the same functions as a physical router. Virtual routers typically run on commodity servers, either alone or packaged with other virtual network functions, like firewall packet filtering, load balancing and wide area network (WAN) optimization capabilities.

Other network devices, such as wireless access points and switches may include built-in router functionality.

How a router works

A router examines a packet header's destination IP address and compares it against a routing table to determine the packet's best next hop. Routing tables list directions for forwarding data to particular network destinations, sometimes in the context of other variables, like cost. They amount to an algorithmic set of rules that calculate the best way to transmit traffic toward any given IP address.



A routing table often specifies a default route, which the router uses whenever it fails to find a better forwarding option for a given packet. For example, the typical home office router directs all outbound traffic along a single default route to its internet service provider (ISP).

Routing tables can be static -- i.e., manually configured -- or dynamic. Dynamic routers automatically update their routing tables based on network activity, exchanging information with other devices via routing protocols.

Many routers also perform network address translation (NAT), shielding the private IP addresses of a local area network (LAN) by readdressing all outgoing traffic with a single shared public IP address. NAT helps both conserve globally valid IP addresses and improve network security.

Types of routers

Core routers used by Internet Service Providers (ISPs) are the fastest and most powerful, sitting at the center of the internet and forwarding information along the main fiber optic backbone. Enterprise routers connect large organizations' networks to these core routers.

An edge router, also known as an *access router*, is a lower-capacity device that resides at the boundary of a LAN and connects it to a the public internet or a private wide area network (WAN) and/or external local area network (LAN). Home and small office routers are considered subscriber edge routers.

Branch routers link an organization's remote office locations to its WAN, connecting to the primary campus network's edge routers. Branch routers often provide additional features, like time-division multiplexing, wireless LAN management capabilities and WAN application acceleration.

A logical router is a configured partition of a traditional network hardware, or physical, router. It replicates the hardware's functionality, creating multiple routing domains within a single router. Logical routers perform a subset of the tasks that can be handled by the physical router, and each can contain multiple routing instances and routing tables.

A wireless router works in the same way as the router in a hard-wired home or business local area network (LAN), but allows greater mobility for notebook or portable computers. Wireless routers use the 802.11g specification, a standard that offers transmission over short distances.

Router Protocols

Routing protocols determine how a router identifies other routers on the network, keeps track of all possible destinations and makes dynamic decisions for where to send each network message. Popular protocols include:

Open Shortest Path First (OSPF) - used to find the best path for packets as they pass through a set of connected networks. OSPF is designated by the Internet Engineering Task Force (IETF) as one of several Interior Gateway Protocols (IGPs)

Border Gateway Protocol (BGP) - manages how packets are routed across the internet through the exchange of information between edge routers. BGP offers network stability that guarantees routers can quickly adapt to send packets through another reconnection if one internet path goes down.

Interior Gateway Routing Protocol (IGRP)- determines how routing information between gateways will be exchanged within an autonomous network. The routing information can then be used by other network protocols to specify how transmissions should be routed.

Enhanced Interior Gateway Routing Protocol (EIGRP) - evolved from IGRP. If a router can't find a route to a destination in one of these tables, it queries its neighbors for a route and they in turn query their neighbors until a route is found. When a routing table entry changes in one of the routers, it notifies its neighbors of the change instead of sending the entire table.

Exterior Gateway Protocol (EGP) - determines how routing information between two neighbor gateway hosts, each with its own router, is exchanged. EGP is commonly used between hosts on the Internet to