Routing

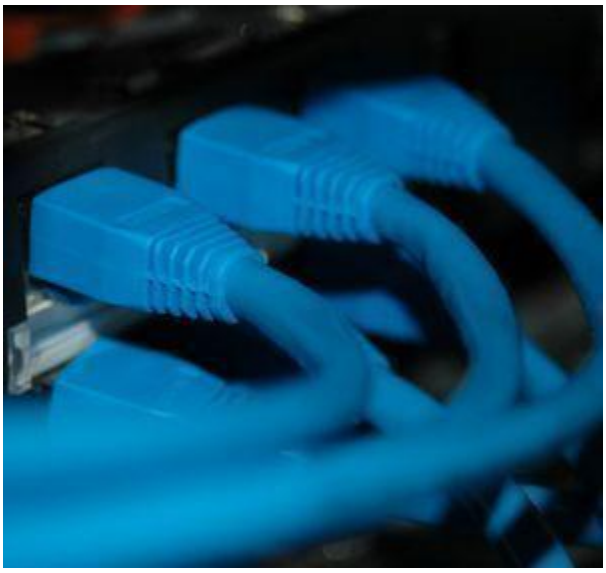
Routing is the process of moving packets through an internetwork, such as the Internet.

Routing actually consists of two separate, but related, tasks:

1. Defining paths for the transmission of packets through an internetwork.
2. Forwarding packets based upon the defined paths.

Routing takes place in IP networks, based on IP routing tables and its entries. The information in the IP routing tables is used by IP hosts to transfer data over the internetwork. Routers are devices operating at the network layer of the OSI model that use the IP routing tables to forward traffic which it receives from a host or from a router.

Before actually configuring LAN routing, one of the first factors to decide on is the connection type that will be used for the remote site connection.



A number of technologies exist that can be used for remote network connections, including:

- *Frame Relay*: This is a WAN technology that uses other hardware components to establish remote site connections. A frame relay connection uses a standard leased line which connects the network site to the frame relay provider's nearest point of presence (POP). The frame relay provider then delivers the connection to the frame relay cloud. In order to use the frame relay provider for a LAN-to-LAN connection, you have to install a leased line at each site which connects the network to the nearest point of presence (POP) of the frame relay provider. The frame relay provider is then responsible for connecting the lines to the same frame relay cloud so that a connection can be established between the two networks.The benefits of using the frame relay WAN technology are:

    - Frame relay provides flexibility.
    - Each of your sites can be connected to a local point of presence (POP) which in turn leads to reduced cost of the leased lines.
    - You can connect to multiple sites using a single frame relay connection.
    - You pay for only the bandwidth that is used.
    - Contracted bandwidth can be exceeded when heavy traffic conditions are present.
- *Leased lines*: Dedicated leased lines are also typically used to connect remote networks. While dedicated leased lines are commonly used for WAN links to enable remote network connectivity, purchasing and maintaining leased lines are expensive. In addition to this, you have to pay for allocated bandwidth all the time. This is due to leased lines being classed as persistent connections. This means that the connections are permanent connections, and remain open all the time.
- *Dial-on demand connections*: While the WAN connections provided by Integrated Service Digital Network (ISDN) and standard asynchronous modems are typically slower than dedicated leased lines, they can be disconnected at any time, and can also be used to enable connectivity to different locations. One of the main characteristics of dial-on demand connections is that you pay for the actual bandwidth that you are using.
- *Virtual private networks (VPNs)*: Remote access VPNs provides a common environment where many different sources such as intermediaries, clients and off-site employees can access information via web browsers or email. Many companies supply their own VPN connections via the Internet. Through their ISPs, remote users running VPN client software are assured private access in a publicly shared environment. By using analog, ISDN, DSL, cable technology, dial and mobile IP; VPNs are implemented over extensive shared infrastructures. Remote access VPNs offer a number of advantages, including the elimination of WAN circuit and modem costs, cable modems enable fast connectivity and are relatively cost efficient, new users can be added with hardly any costs, and information is easily and speedily accessible to off-site users through Internet connectivity.

The components of unicast IP routing are described below:

- *Static IP routing*: You can use the Routing And Remote Access management console to configure and manage static routes. Static routes are manually created, and need to be modified whenever a change occurs to the network configuration.
- *RIP versions 1, RIP version 2*: RIP is a distance-vector routing protocol which is normally used for dynamic routing in small to medium sized internetworks.
- *OSPF*: This is a link-state routing protocol that is used for dynamic routing in medium to large sized internetworks
- *Network address translation (NAT)*: NAT translates private IP addresses to Internet IP addresses that can be routed on the Internet.
- *IP packet filtering*: This is a security feature that enables you to define the traffic types that are allowed to pass over an interface. When you configure IP packet filters, you specify what traffic is allowed/denied, based on the following:
  - Source address
  - Destination address
  - TCP port number
  - UDP port number
  - IP protocol numbers
  - ICMP types and codes
- *DHCP Relay Agent*: This is a relay agent that forwards DHCP messages between the DHCP servers and DHCP clients that are located on different network segments.
- *ICMP router discovery*: ICMP router discovery makes is possible to advertise and reply to router solicitations.

The components of IP multicast routing are described below:

- *Multicast forwarding*: Multicast forwarding is an element of the TCP/IP protocol suite. You can use the Routing And Remote Access management console or the Netsh command-line tool to examine the content of the multicast forwarding table.
- *IGMP version 1 and IGMP version 2*: IGMP is a protocol of the TCP/IP protocol suite that is used to manage and control multicast group membership.

- *Multicast boundaries*: You can configure multicast boundaries, based on the following:
  - Time-To-Live (TTL) specified in the IP header.
  - IP multicast group address.
  - Maximum multicast traffic allowed in kilobytes per second.
- *Specific forwarding and routing*: A Windows 2000 Server or Windows Server 2003 router can support specific multicast forwarding and routing if IGMP Router mode and IGMP Proxy mode are enabled for interfaces.

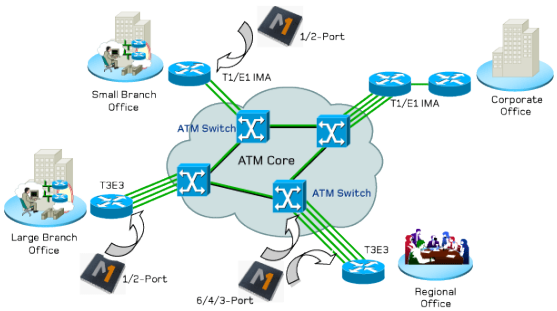
The components of IPX routing are described below:

- IPX packet filtering: This is a security feature that enables you to define the traffic types that are allowed to pass in and out of an interface. When you configure IPX packet filters, you specify what traffic is allowed/denied, based on the following:
  - Source and destination IPX network
  - Packet type
  - Node
  - Socket numbers
- RIP for IPX: This is a distance-vector routing protocol that is used on IPX internetworks. You can configure both static IPX routes and RIP route filters through the Routing and Remote Access Service (RRAS).
- SAP for IPX: This is a distance-vector advertising protocol that advertises services and each service's location on IPX internetworks. Through the Routing and Remote Access Service (RRAS), you can configure:
  - Static SAP services
  - SAP service filters
- NetBIOS over IPX: Through the Routing and Remote Access Service (RRAS), you can configure:
  - RRAS to forward NetBIOS over IPX broadcasts
  - Static NetBIOS names

Routing vs. Bridging and Switching

Routing is distinguished from bridging or switching by operating at the Network Layer of the OSI Model. Bridging and switching occur on the Data Link Layer.

Static vs. Dynamic Routing



Routing can be accomplished by manually entering the information necessary for packets to reach any part of the internetwork into each router. This is called *static routing*. Static routing works reasonably well for very small networks, but does not scale well. When using static routing, the routing tables on each router must be updated each time the network topology changes — such as when a network link fails..

In most networks, routing is managed automatically through the use of dynamic routing. In dynamic routing, routing protocols create and maintain the routing tables automatically. Dynamic routing responds much more quickly to network changes (and network failures) than static routing.

Understanding Static Routing

With static routing, routing protocols are not used to communicate routing information between IP ruters. Administrators have to manually create and modify the routing table entries. Each time a change occurs in the network configuration, the entries in the routing table have to be modified to reflect these changes. Static routing works well in a small network where it is easier to configure a small number of static routes than it is to configure dynamic routing. A few advantages of using static routing are:

- Static routing is easy to deploy and configure.
- Because static routing does not involve routers communicating between each other, it works well for low bandwidth WAN links.
- Static routes can offer support for unnumbered connections.
- Static routes are not as resource intensive as the dynamic routing protocols.

A few disadvantages of using static routing are:

- Static routing only works for small networks where expansion is not likely.
- Maintaining static routes becomes costly as the network expands.
- Static routing provides no fault tolerance. If a route is incorrectly configured, the route remains unavailable until the issue is manually resolved.

Understanding Dynamic Routing

With dynamic routing, the need to manually create and maintain static routes is eliminated. Dynamic routing use routing protocols so that IP routers can communicate with each other. The routing protocols also enable routers to share the information they have in their routing tables. A router that is configured to use dynamic routing forwards its routing table's content to the other routers configured for dynamic routing at regular time periods or intervals. When a router does not send its routing table at the specified time interval, the other routers simply remove the router from their routing tables. This process prevents traffic from being forwarded to the failed router. Once the failed router is online again, the router starts sending dynamic routing messages which enables the other routers to determine that traffic can be forwarded to the router again. This in turn causes the other routers to update their routing tables to include the specific router once more. One of the main factors to consider when deciding on implementing dynamic routing is the actual routing protocol that you will use. The Routing and Remote Access service (RRAS) includes integrated support for the following dynamic routing protocols:

- Routing Information Protocol (RIP) version 2
- Open Shortest Path First (OSPF)

Source: http://www.tech-faq.com/routing.html