Routers

Whereas switches and bridges operate at OSI Layer 2 (the data link layer), *routers* primarily operate at OSI Layer 3 (the network layer). Like bridging, the primary act of routing involves moving packets across a network from a source to a destination. The difference involves the information that is used to make the forwarding decisions. Routers make decisions based on network layer protocols such as Internet Protocol (IP) and Novell NetWare Internetwork Packet Exchange (IPX).

Routing gained popularity in the mid- to late 1980s as a result of internetworks growing beyond the capability of bridges. Before this popularity, networks were relatively small and isolated, and bridges could handle the jobs of forwarding and segmentation. However, as networks grew, routers facilitated larger scaling and more intelligent growth across wider physical distances. Although routers are more expensive and complex than bridges, routing is the core of the Internet today.

Routers Talk Among Themselves to Find Routes

Routing involves two processes: determining optimal routing paths through a network, and forwarding packets along those paths. Routing algorithms make the optimal path determination. As they determine routes, tables on the router store the information. Routers communicate with each other and maintain their routing tables through the exchange of messages over the network. Routing updates are one particular type of message. A *routing update* contains all or part of another router's routing table and allows each router to build a detailed picture of the overall network topology.

Routing algorithms fill routing tables with various types of information. The primary piece of information relevant to routing is the *next hop*. Next-hop associations tell a router that it can reach a particular destination by sending a packet to a particular router representing the next hop on the way to its final destination.

The process of exchanging information between routers is done using a routing protocol. Put simply, a routing protocol is a series of messages that routers use to exchange information about whether particular links are up or down, and about other next-hop routers in the network. Three of the most common routing protocols in use today are Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), and Border Gateway Protocol (BGP).

Routers Route Packets

When a router receives a packet, it attempts to associate the destination network address in the packet to an appropriate next hop in its routing table. In addition to next-hop associations, routers store other pertinent information in routing tables. For multiple paths to a destination, a routing table might contain information that allows the router to determine the desirability of one path over another.

After a router determines an optimal path for a packet, it must forward the packet toward the destination. The process of a router moving a packet from its received port to the outgoing destination port is called *switching*. Although the process of switching a packet on a router is similar to that of a Layer 2 switch, the decision criteria and the actual handling of the packet are different. When a computer determines that it must send a packet to another host, it specifies in the packet how to reach the destination network. If the destination is unknown, the router typically drops the packet. If the destination is known, the router changes the destination physical address in the packet to contain that of the next hop. The router then transmits the packet out the destination interface.

The next hop can be either the final destination or another router. Each router in the process performs the same operation. As the packet moves through the network, each router modifies the physical address stored in the packet but leaves the network address untouched (because it determines the final destination).

Routers Bridge and Switches Route

In an ideal world, everything does what it is defined to do. This is not the case with network devices. Routers can provide bridging functionality, and switches are quickly becoming the high-density port, high-speed router of the campus. Network devices, including switches and routers, make forwarding decisions on OSI layers higher than the network layer. For example, routers can provide firewall functionality in which the router inspects Layer 4 packet information, and switches such as content switches can perform forwarding decisions based on Layer 5 through 7 packet information (such as the URL in an HTTP packet).

At-a-Glance: Routing

Why Should I Care About Routing?

Routing is one of the fundamental aspects of networking. Routers can learn possible routes (rather than having to have the route manually configured and constantly updated). This is one of the primary reasons that ARPANET, which originally connected seven sites, was able to scale exponentially into the modern Internet in only a few years. Many routers today have address tables with more than 100,000 entries, and they are updated constantly.

What Problems Need to Be Solved?

Routed networks are often large and complex, and it would be prohibitively difficult to manage and update network information on all routers all the time. To account for this, several algorithms have been developed. These algorithms allow the routers to learn about the network and then make decisions based on that information.

To learn paths (or routes) through a network and then decide where to send packets, a router must know the following information:

- **Destination address:** This is typically the IP address of the data's (packet) destination.
- **Source address:** The router also needs to know where the information came from (typically an IP address).
- **Possible routes:** These are likely routes that can get information from the present location or source to some other location (the destination or closest known point).
- **Best route:** Routers also must know the best ("best" can mean many things) path to the intended destination.
- **Status of routes:** Routers also keep track of the current state of routes to ensure timely delivery of information.

What Exactly Does "Best" Mean?

Routers often make decisions about the best possible path to get information from a source to a destination. "Best" is loosely defined; it depends on what the network values. These measurements of value are called metrics. The network administrator determines which metrics the network values. Here are several metrics:

- **Hop count:** How many times a packet goes through a router.
- **Delay:** The amount of time required to reach the destination.
- **Reliability:** The bit error rate of each network link.
- **Maximum Transmission Unit (MTU):** The maximum message length (or packet size) allowed on the path.
- **Cost:** An arbitrary value based on a network administrator-determined value. Usually some combination of other metrics.

Static Versus Dynamic

Routers must learn about the network around them to determine where to send packets. This information can be either manually entered (static routes) or learned from other routers in the network (dynamic routes):

- **Static routes:** When a network administrator manually enters information about a route, it is considered a static route. This information can be changed only by a network administrator (in other words, the router doesn't learn about network events). Static routes allow for tight control of packets but become difficult to maintain and are prone to human error. However, static routes may be used to work around a temporary problem or for performance enhancement.
- **Dynamic routes:** Routers on a network can learn about possible routes and current route status from other routers in the network. Routes learned in this way are called dynamic routes. Unlike static routes, any changes in the network are learned without administrative intervention and are automatically propagated throughout the network.

Flat Versus Hierarchical

With flat networks, all routers must keep track of all other routers on the network. As networks grow, the amount of information contained in the routing tables becomes larger and larger.

At-a-Glance: Routing

Although this method is simple, it can result in poor network performance as the number of routing updates grows exponentially with each new router.

Hierarchical networks segment routers into logical groupings. This simplifies routing tables and greatly reduces overheard traffic.

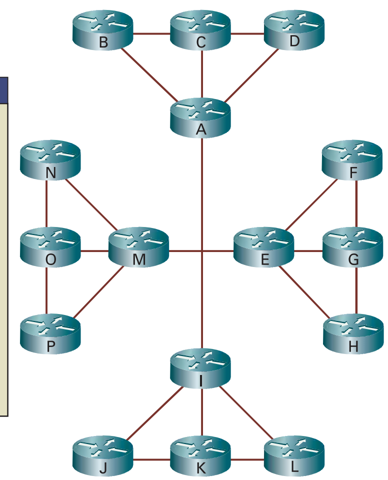
Intradomain Versus Interdomain

Intradomain and interdomain routing can be easily understood in the context of large-scale hierarchical networks. In this regard, think of each segment as its own autonomous network. Within each autonomous network, intradomain routing protocols (also called Interior Gateway Protocols [IGP]) are used to exchange routing information and forward packets. Interdomain routing protocols (also called Exterior Gateway Protocols [EGP]) are used between autonomous networks. This distinction is made because there are different performance requirements for internal and external networks.

Distance Vector Versus Link-State

The two main classes of routing are distance vector routing and link-state routing.

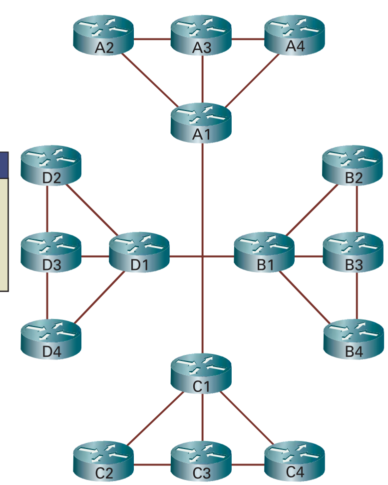
With distance vector routing, also called "routing by rumor," routers share their routing table information with each other. Each router provides and receives updates from its direct neighbor. In the figure, Router B shares information with Routers A and C. Router C shares routing information with Routers B and D. A distance vector describes the direction (port) and the distance (number of hops or other metric) to some other router. When a router receives information from another router, it increments whatever metric is being used. This process is called distance accumulation. Routers using this method know the distance between any two points in the network, but they do not know the exact topology of an internetwork.



Routing Table O		
Router	Next Hop	Hops
A	M	1
B	M	1
C	M	1
D	M	1
E	M	2
F	M	2
G	M	2
H	M	1
I	M	2
J	M	2
K	M	2
L	M	1
M	M	2
N	N	2
P	O	

Routing Table A		
Router	Next Hop	Hops
B	B	1
C	C	1
D	D	1
E	E	1
F	E	2
G	E	2
H	E	2
I	I	1
J	I	2
K	I	2
L	I	2
M	M	1
N	M	2
O	M	2
P	M	2

Routing Table I		
Router	Next Hop	Hops
A	A	1
B	A	1
C	A	1
D	A	1
E	E	2
F	E	2
G	E	2
H	E	1
J	J	2
K	K	2
L	L	2
M	M	1
N	M	2
O	M	2
P	M	2



Routing Table A1		
Router	Next	Hops
A2	A2	1
A3	A3	1
A4	A4	1
Any B	B1	1
Any C	B2	1
Any D	B3	1

Routing Table D3		
Router	Next	Hops
D1	D1	1
D2	D2	1
D4	D4	1
All Others	D1	1

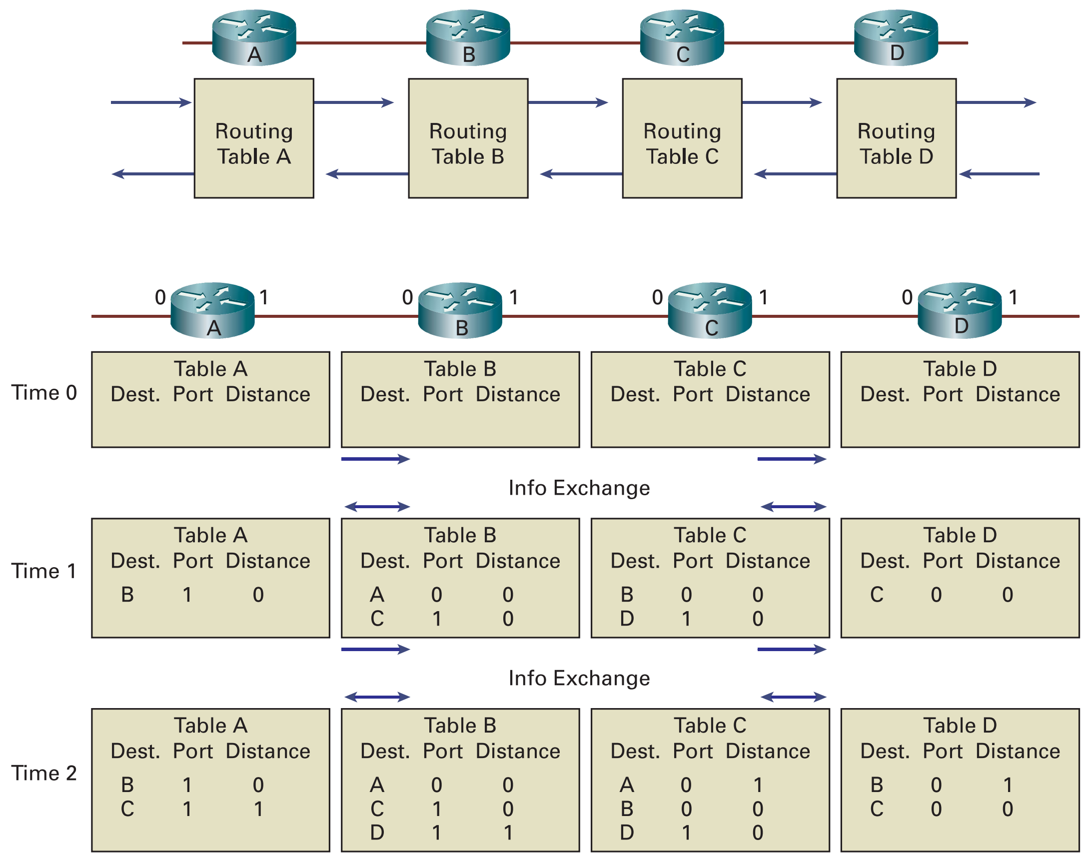
Routing Table C3		
Router	Next	Hops
C2	C2	1
C3	C3	1
C4	C4	1
Any A	A1	1
Any B	B1	1
Any D	D1	1

At-a-Glance: Routing

How Information Is Discovered with Distance Vectors

Network discovery is the process of learning about nondirectly connected routers. During network discovery, routers accumulate metrics and learn the best paths to various destinations in the network. In the figure, each directly connected network has a distance of 0. Router A learns about other networks based on information it receives from Router B. Routers increment the distance metric for any route learned by an adjacent router. In other words, Router A increments by 1 any distance information it learns about other routers from Router B.

As more time goes by, the router learns more about the network and can process packets more efficiently.



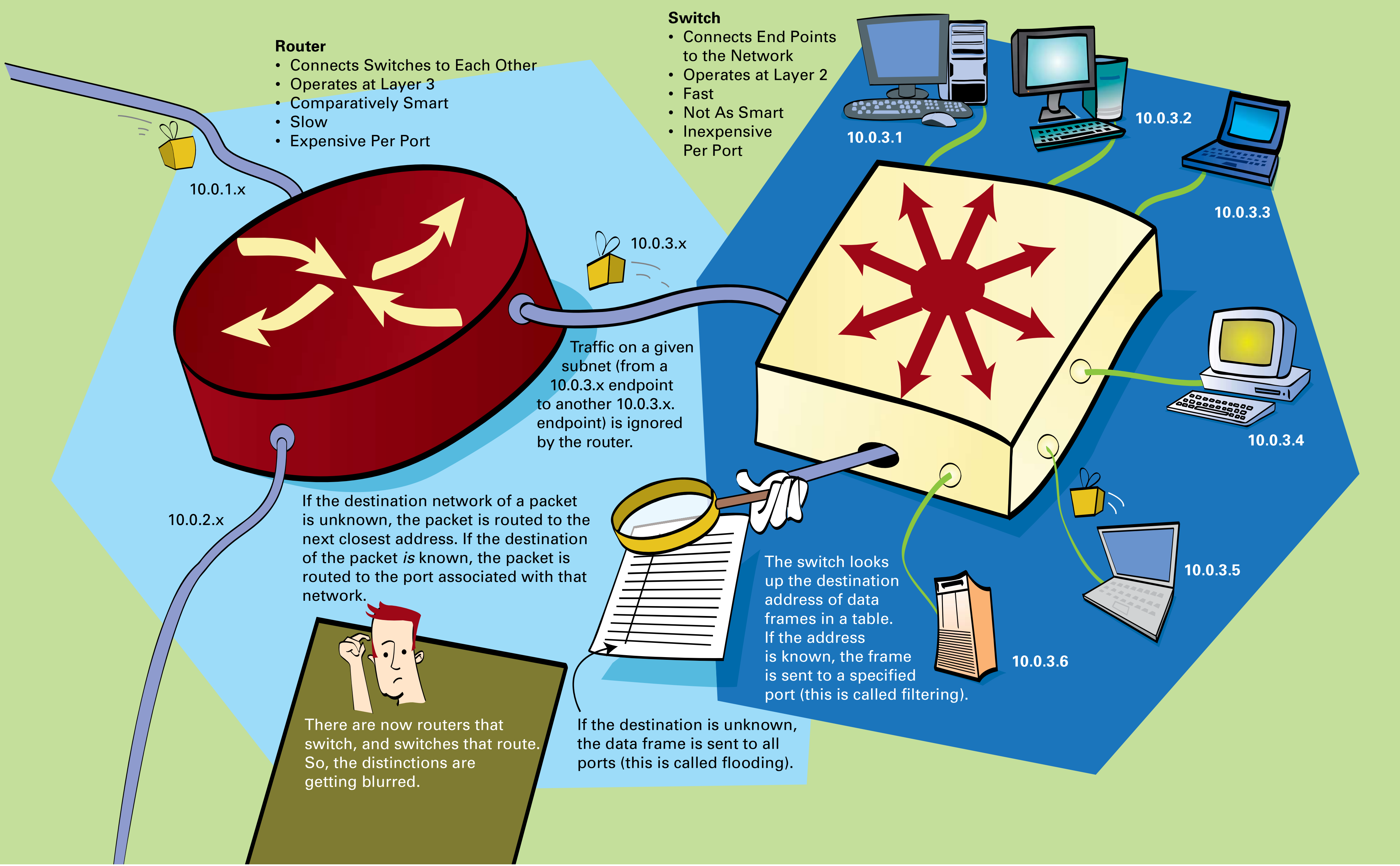
Link-State Routing

With link-state routing (also known as shortest path first [SPF]), each router maintains a database of topology information for the entire network.

Link-state routing provides better scaling than distance-vector routing, because it sends updates only when there is a change in the network, and then it sends only information specific to the change that occurred. Distance vector uses regular updates and sends the whole routing table every time. Link-state routing also uses a hierarchical model, limiting the scope of route changes that occur.

Routing and Switching

Routers and Switches



Routing and Switching