



Routing Basics : How Routers Work

In a small-business local-area network (LAN), these are the primary networking devices:

- Network interface cards that connect PCs and servers to the LAN
- The hubs and/or switches that interconnect the various LAN devices and create the Ethernet backbone.

These devices operate at "layer 2" (the data link layer). For the LAN users to connect to the Internet or to a remote branch office, a device called a "router" must be used.

A router passes data between multiple networks. It works at the "layer 3" (the network link layer), which means that it must be able to understand the data packets so that it can route them to their destination.

Routers are essentially computers optimized for handling packets that have to be transferred between separate networks. Routers attempt to send packets from their source to their destination in the fastest way possible, which is not always the absolute shortest path.

On a network, packets with destinations on the LAN go directly from the sending machine to the destination machine without any intermediaries. However, if the destination address of a packet is outside the LAN, the sending machine sends it to the router, which the sending machine knows as the default gateway, and has no further interaction with that packet.

When the router receives a packet destined for a point outside the LAN, it looks to see if it has a route to get the packet to that destination network. If it does (or if it has a default gateway of its own), it will send the packet to the next stop.

Like a postal system or courier

Routing between a LAN and a wide-area network (WAN) is like a postal system or a courier network. A package traveling from New York to San Francisco might travel through a hub in Memphis or Chicago and be re-sorted in Reno before heading to its final destination. If the package had to be hand-delivered quickly, you could do that, but the cost would increase significantly, and hopefully, the package won't get routed the long way around, because that tends to be inefficient and difficult to trace.

In the same manner, routers send packets according to the available routes between networks and try to determine the shortest possible route at any given time.

How does a router do this? Well, inside a router is a set of data called routing tables. Routing tables include:

- All possible routes the router is aware of Information on which connections lead to particular groups of addresses
- Priorities for connections to be used Rules for handling both routine and special cases of traffic

Routing tables are dynamic — they are updated by routing protocols such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) that constantly pass messages between



routers. The router consults them to determine whether or not it has a route to a particular destination address.

The routing table can be as simple as a half-dozen lines of code in small routers but can grow to massive size and complexity in very large routers that handle the bulk of Internet traffic.

Explanation of routing

When a router takes a packet and sends it closer to its final destination, we say it has forwarded a packet. In the simplest terms, that's what a router does; it forwards packets toward their destination and it tries to do so at the least possible "cost."

Cost, for a router, is not measured in dollars and cents, but in "hops." Every time a packet is routed between one router and another, a number in the data packet called the hop count increases by one. If the hop count reaches certain preset limits (for example, RIP allows a maximum of 16 hops), the packet may be discarded as undeliverable since, in 16 hops, the routers have not been able to deliver the packet to the destination address.

For routers, however, cost is not the absolute variable it is in the physical world, because it's not much more expensive to go "the long way" from an origin to a destination when dealing with the Internet. This is because:

- Data moves at the speed of light (or very close to it over copper wires), so any additional distance is not very relevant.
- The Internet was designed to be redundant. If the first route fails, try a second or third.

The design of the Internet is solid because it reroutes data packets all the time as a result of events like natural disasters and power failures.

Other router functions: security

Routers can add security to your WAN. If your WAN is accessed by many users, or if it passes over high-speed digital phone lines or the Internet, your WAN is a potential target for malicious hackers, identity theft, denial of service attacks, virus infections and much more. Today's small to medium-sized business routers can be configured with features such as:

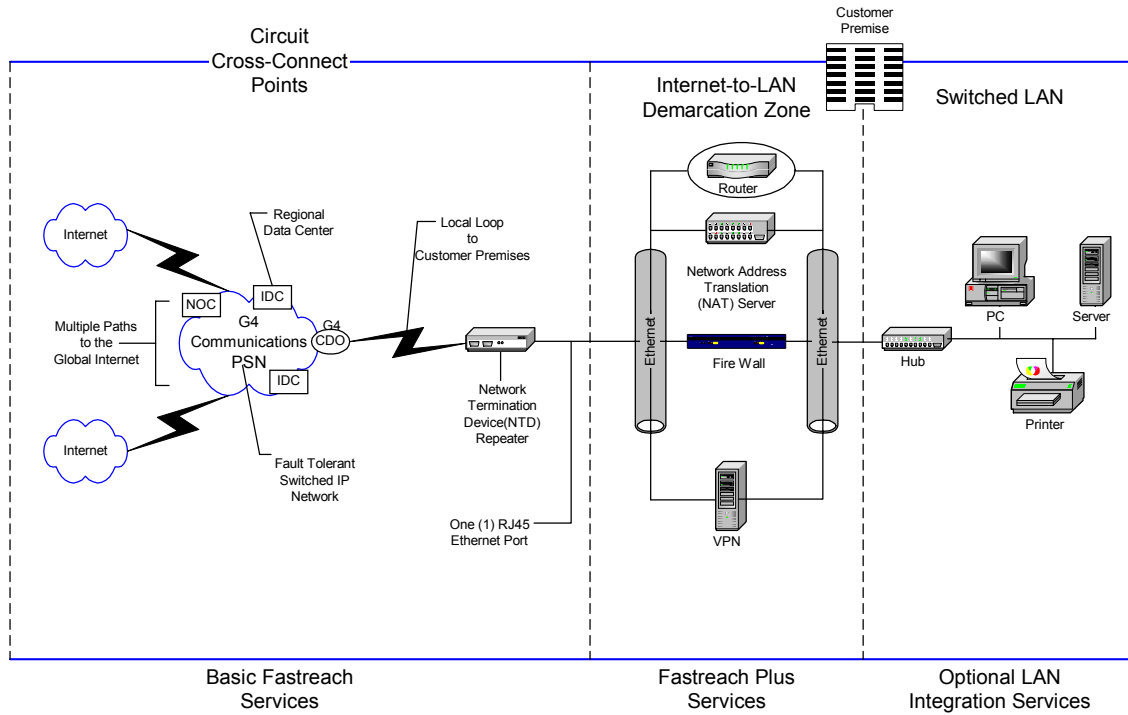
- Built-in firewalls
- Intrusion detection
- Authentication
- Encryption
- VPNs

Summary

Knowing where and how to send data packets is the most important job of a router. Simple routers do this and nothing more. Other routers add additional functions including security features to the jobs they perform. The one constant is that modern networks, including the Internet, could not exist without the router.

A typical Internet Connection Diagram

G4 FastReach



A Router is needed when more than 1 Public IP address has been assigned to a local network to be used by multiple computers.

A NAT Server is needed when 1 public IP address has been assigned and will be used by multiple Private IP addresses to be used by multiple computers.