

How Routers Work

David Davis

Routers are an essential part of the network's plumbing. Organizations depend on routers so that employees can check email or access Web applications. Network engineers must configure these routers correctly to keep all the network traffic flowing smoothly. But how does a router actually work?

How Routing Fits Into The OSI Model

The OSI model is just a theoretical model, but it is a great way to visualize how all of these protocols, addresses and network devices (like routers) fit together.

Layers 2 and 3 of the OSI model are what apply here. Layer 2, the Data Link layer, is where the Ethernet protocol, MAC addresses and switches fit in. Layer 3, the Network layer, is where the IP protocol, IP addresses and routers fit in. Remember that all traffic is sent from your computer starting with Layer 7 (your network application) and going down to Layer 1 (physical). With the physical layer, the traffic is going across your network medium (such as your network cable or your wireless airwaves).

Traffic goes to a router only if it is *not* on your local LAN. Routers work primarily at Layer 3 but must understand Layers 1-3, at a minimum. Many routers understand traffic all the way up to Layers 4-7 in varying ways, but we like to think of them as working only at Layer 3 (network) because that is their primary function.

How Routers Use Ethernet MAC Addresses And IP Addresses

As I said, in Layer 2 is your Ethernet protocol and Ethernet addressing -- the MAC address (a.k.a. physical address or Ethernet address). In Layer 3 is your IP protocol and IP addressing. Today, almost all networking is done using Ethernet and IP. Thus, in general, every packet on your network has an Ethernet MAC address source and destination -- *and* an IP address source and destination. Keep this in mind.

I believe everyone who is interested in computers should, at some time or another, use a network protocol analyzer to really see all the packets that are going to and from the computer. This is true even when you aren't using it! In a protocol analyzer, you would see this Ethernet source/destination and IP address source/destination.

What A Router Does With Your Network Traffic

Routers understand these Ethernet and IP addresses. Routers are primarily interested in the destination IP address of the packet you are sending to the router. The router takes this destination (say it is 63.248.129.2) and looks that up in its routing table. Here is an example of a routing table:

```
Location-A# show ip route
      10.0.0.0/24 is subnetted, 2 subnets
R       10.2.2.0 [120/1] via 63.248.129.2, 00:00:16, Serial0
C       10.1.1.0 is directly connected, Ethernet0
      63.0.0.0/30 is subnetted, 1 subnets
C       63.248.129.0 is directly connected, Serial0
Location-A#
```

Routes in the routing table are learned from either static routes (entered by you) or dynamic routes. Using the routing table, the router tries to find the best route for your traffic. There may be only one

How Routers Work

David Davis

route. Often, this is a "default route" (a.k.a. "gateway of last resort"). The default route just says: "If there are no better routes to send this traffic, send it here."

Just about every home and small business user has just a single Internet connection. In that case, they have a default route and all traffic is sent to their Internet service provider (ISP). In the case of ISPs, however, there may be many places they can send this traffic. Their routers must compare many hundreds of thousands of routes and select the best one for your traffic. This happens in milliseconds. And to get your traffic through the Internet and back, it may pass through hundreds of routers. To you, it appears almost instantaneously (depending on many factors).

If it doesn't find a valid route for your traffic, the router discards (yes, throws away) your traffic and sends an ICMP "destination unreachable" message back to you. When the router does find the best route and is ready to send your traffic, it has to do a number of things:

1. Perform Network Address Translation (NAT). NAT isn't a traditional router function, but many routers today perform NAT. This is especially true for home and small business routers that function as "all in one" devices. Many companies have dedicated firewalls that also perform NAT. With NAT, your private source IP address is translated into a public source IP address. If the router is performing PAT (NAT overload), then the public source IP address is shared among many devices.
2. Replace your source MAC address with the router's MAC address. The ARP protocol is used to connect your computer's source MAC address to your IP address. The ARP protocol is a broadcast-oriented protocol, and routers discard broadcasts. This means that ARP doesn't work through routers. Because of this, the router must replace your source MAC address with the router's MAC address. The router also adds the destination host or next-hop router's MAC address to the data link header.
3. Encapsulate the packet for the protocol of the WAN. Routers often perform protocol conversion. Say, for example, you have a router that has a PPP T1 connection to the Internet and is connected to the LAN using Ethernet. The Ethernet frames must be de-encapsulated, modified, then re-encapsulated in Ethernet, then PPP, before they can be sent across the PPP link.

On the other side of the link, the destination router is performing all of these same tasks, but in reverse. This happens for every packet sent and every response received.

To see a real production routing table from an ISP, you can telnet to public Cisco route servers around the world. From here, you can do a **show ip route** and see what a real ISP's routing table looks like.