Understanding Ethernet switches and routers (part 2)

By George Thomas

This is the second of a two-part article on Ethernet switches and routers. The first part dealt with switches (www.isa.org/intech/basics_201102), and this second part deals with routers.

In the first part, we used the example of visiting a computer store to purchase a device that will access the Internet, and we noted they will try to sell us a router. In most instances, the router will come with a built-in switch so you can connect several Ethernet devices using just one device. So again, what is the difference between an Ethernet router and an Ethernet switch? We will refer back to the Open Systems Interconnection Model, which we discussed in part 1.

![Seven-layer model with each layer providing a unique service.](medium)

Routers operate one layer above switches, which are considered bridges.

The figure above illustrates the seven-layer model with each layer providing a unique service. In part 1, we indicated Ethernet provides services at the physical and data link layers through the use of bridges and repeaters. The rules of Ethernet are restricted to a single local-area network (LAN). If we have a collection of interconnected LANs, this is called an inter-network. Communicating between LANs within an inter-network requires routers, which operate one layer above that of a switch at the network layer. The most famous of inter-networks is the Internet with the rules for communication being defined by the Internet Protocol (IP).

It is not necessary that routers support the IP, but this is the most common protocol used by routers, so we will use this in our discussion. In the figure below, you will see a collapsed seven-layer model which is called the Internet Model. The only difference is the functions of presentation and session are lumped into the transport layer. The transport layer provides end-to-end communications between applications with the Transmission Control Protocol.
(TCP) being the one used in the Internet Model. The middle layer is the network layer, which is involved with host addressing and fragmentation, with the most common addressing scheme called IP protocol version 4 or IPv4.

The figure below shows an IPv4 header and datagram encapsulated into an Ethernet frame. The Ethernet frame is shown with a destination address (DA) and a source address (SA) as we would expect. The Type field has a hexadecimal 0800, indicating the Ethernet data field contains an IP packet or a portion of an IP packet. A cyclic redundancy check (CRC) completes the frame. When we refer to the Internet Protocol, we talk in terms of packets. With Ethernet communication, we talk in terms of frames. Ethernet frames pass without issues through Ethernet switches, but hosts and routers on the Internet respond to the data inside Ethernet frames called packets. Switches do not understand the meaning of packets; they just understand frames.
The IPv4 header and datagram is encapsulated into an Ethernet frame.

The data shown here can be very confusing, and it does not get any easier as we move up the Internet Model. We will just point out some fields within the packet that are the most interesting.

With the IPv4, a new addressing scheme is introduced to identify hosts on the Internet. There is a source IP address and a destination IP address just like there are source and destination Ethernet addresses, so what is the difference? IP addresses are 32-bit long addresses while Ethernet addresses are 48-bits long. In the Internet world, a device does not have to be an Ethernet device in order to have an IP address. While an Ethernet device manufacturer supplies a unique 48-bit address to the product it sells, IP addresses are assigned using rules established by the Internet Engineering Task Force. IP addresses are designated as being private and public. Public IP addresses must be unique across the Internet, but private addresses can be duplicated because they will never reach the Internet—thanks to IP routers that block them from appearing on the Internet. Switches would not restrict IP addresses from appearing, and that is one reason why routers are used to access the Internet and not switches.

Other fields that should be pointed out within the IP packet are the IP Datagram Data. Our main purpose is to send data between hosts, and this data is referred to as a datagram. Unlike the transport layer of the Internet Model, which is involved with end-to-end delivery of data, the network layer is only required to make its “best effort.” There are no acknowledgements that a packet sent by a host is received by another. If the packet is too big to fit into one Ethernet frame, it is split up into fragments requiring reassembly at the receiving end.

**Ethernet switch-router combination**

The figure below shows a four-port Ethernet switch as part of an IP Router. Although there are a total of five Ethernet ports on this combination Ethernet switch-router, the five ports are not peers to one another. Certainly, the four clustered ports are peers—they are all part of the internal Ethernet switch, and no one port on the switch has precedence over another. The switch-router is divided into two halves—the LAN side and the WAN side. The Ethernet switch resides on the LAN side, or what is sometimes called the private side. Remember Ethernet is a local-area-network technology, so Ethernet equipment deployment is restricted to either a work group, a building, process line, or possibly a campus. Workstations, printers,
servers, and automation equipment can attach to any of these switch ports. If more LAN ports are needed, external switches can be cascaded to any switch port on the switch-router.

The Ethernet switch-router provides hosts on the LAN side IP addresses, as well as access to the Internet.

The one remaining Ethernet port is not part of the switch fabric. It is called a WAN port for wide-area network. It does not have to be an Ethernet port, but we will use an Ethernet port in our example. This single WAN port is considered to be located on the public side of the switch-router because this is the port that gains us access to the Internet. Between the LAN and WAN sides is logic that controls the routing of messages between the two sides. How can a single Ethernet port connect to the Internet? In our example, we are attaching the Ethernet port to a cable modem, although a Digital Subscriber Line (DSL) modem could be used as well. At the far-end of the modem connection is an Internet Service Provider (ISP) that functions as a gate-keeper to the Internet.

Obtaining IP addresses

In the last figure, the hosts on the private side have been given private IP addresses. These addresses can be statically set in the hosts, or the hosts can receive them dynamically using a process called Dynamic Host Configuration Protocol (DHCP). In the dynamic case, the router functions as a DHCP server providing addresses in a pre-selected range while the attached hosts function as DHCP clients requesting IP addresses. However, the router needs a WAN side address as well and usually obtains a public IP address from the ISP using a similar process. Once addressing is established, connected hosts on the LAN side can have access to the Internet through the switch-router. The translation of the private addresses to that of a public address is another function of a router.

ABOUT THE AUTHOR

George Thomas is president of Contemporary Controls in Downers Grove, Ill. He is a senior ISA member.

Source:

http://www.isa.org/InTechTemplate.cfm?Section=Control_Fundamentals1&template=/ContentManagement/ContentDisplay.cfm&ContentID=85272