OPINION

What is a network switch, and how does it work?

Switches connect network segments, providing full-duplex communication, valuable network performance data and efficient use of network bandwidth.

By Keith Shaw
Contributing Writer, Network World
OCT 6, 2020 2:01 PM PDT

Networks today are essential for supporting businesses, providing communication, delivering entertainment—the list goes on and on. A fundamental element networks have in common is the network switch, which helps connect devices for the purpose of sharing resources.

What is a network switch?

A network switch is a device that operates at the Data Link layer of the OSI model—Layer 2. It takes in packets being sent by devices that are connected to its physical ports and sends them out again, but only through the ports that lead to the devices the packets are intended to reach. They can also operate at the network layer--Layer 3 where routing occurs.

Switches are a common component of networks based on ethernet, Fibre Channel, Asynchronous Transfer Mode (ATM), and InfiniBand, among others. In general, though, most switches today use ethernet.

How does a network switch work?

Once a device is connected to a switch, the switch notes its media access control (MAC) address, a code that's baked into the device's network-interface card (NIC) that attaches to an ethernet cable that attaches to the switch. The switch uses the MAC address to identify which attached device outgoing packets are being sent from and where to deliver incoming packets.

So the MAC address identifies the physical device as opposed to the network layer (Layer 3) IP address, which can be assigned dynamically to a device and change over time.

When a device sends a packet to another device, it enters the switch and the switch reads its header to determine what to do with it. It matches the destination address or addresses and sends the packet out through the appropriate ports that leads to the destination devices.

To reduce the chance for collisions between network traffic going to and from a switch and a connected device at the same time, most switches offer full-duplex functionality in which packets coming from and going to a device have access to the full bandwidth of the switch connection. (Picture two people talking on a cell phone as opposed to a walkie-talkie).

While it's true that switches operate at Layer 2, they can also operate at Layer 3, which is necessary for them to support virtual LANs (VLAN), logical network segments that can span subnets. In order for traffic to get from one subnet to another it must pass between switches, and this is facilitated by routing capabilities built into the switches.

Switches vs. hubs

A hub can also connect several devices together for the purpose of sharing resources, and the collection of devices attached to a hub is known as a LAN segment.

A hub differs from a switch in that packets sent from one of the connected devices is broadcast to all of the devices that are connected to the hub. With a switch, packets are directed only to the port that leads to the device that packets are addressed to.

Switches typically connect LAN segments, so hubs attach to them. Switches filter out traffic destined for devices on the same LAN segment. Because of this intelligence, switches make more efficient use of their own processing resources as well as network bandwidth.

Switches vs. routers

Switches are sometimes confused with routers, which also offer forwarding and routing of network traffic, hence their name. But they do this with a different purpose and location.

Routers operate at Layer 3—the network layer—and are used to connect networks to other networks.

An easy way to think about the difference between switches and routers is to think about LANs and WANs. Devices connect locally through switches, and networks are connected to other networks through routers. If you think about the general path a packet might take to reach the internet—for example: device > hub > switch > router > internet—that should help as well.

Of course, there are cases where switching functionality is built into a router hardware, and the router performs as the switch as well.

The easiest case here is to think of your home wireless router. It routes to a broadband connection through its WAN port, but it usually also has additional ethernet ports that you can use to connect an ethernet cable for a computer, television, printer or even a gaming console. While other devices on the network, such as other notebooks and phones, connect through the Wi-Fi router, it still offers switching functions through the LAN. So the router, in effect, is also a switch. And you can even connect a separate switch to the router to provide both internet and LAN access for additional devices.

Types of switches

Switches vary in size, depending on how many devices you need to connect in a specific area, as well as the type of network speed/bandwidth required for those devices. In a small office or home office, a four- or eight-port switch usually suffices, but for larger deployments you generally see switches up to 128 ports. The form factor of a smaller switch is an appliance that you can fit on a desktop, but switches are also rack-mountable for placement in a wiring closet or data center or server farm. Sizes of rack-mountable switches range from 1U to 4U, but larger ones area also available.

Switches also vary in the network speed they offer, ranging from Fast ethernet (10/100 Mbps), Gigabit ethernet (10/100/1000 Mbps), 10 Gigabit (10/100/1000/10000 Mbps) and even 40/100 Gbps speeds. Which speed to choose depends on the throughput needed for the tasks being supported.

Switches also differ in their capabilities. Here are three types.

Unmanaged

Unmanaged switches are the most basic, offering fixed configuration. They are generally plug-and-play, which means they have few if any options for the user to choose from. They may have default settings for features such as quality of service, but they cannot be changed. The upside is that unmanaged switches are relatively inexpensive, but their lack of features make them unsuitable for most enterprise uses.

Managed

Managed switches offer more functionality and features for IT professionals and are the type most likely seen in business or enterprise settings. Managed switches have command-line interfaces (CLI) to configure them. They support simple network management protocol (SNMP) agents that provide information that can be used to troubleshoot network problems.

They can also support virtual LANs, quality of service settings and IP routing. The security is also better, protecting all types of traffic that they handle.

Because of their advanced features, managed switches cost much more than unmanaged switches.

Smart or intelligent switches

Smart or intelligent switches are managed switches that have some features beyond what an unmanaged switch offers, but fewer than a managed switch. So they are more sophisticated than unmanaged switches, but they are also less expensive than a fully manageable switch. They generally lack support for telnet access and have Web GUIs rather than CLIs. Other options, such as VLANs, may not have as many features as those supported by fully managed switches. But because they are less expensive, they may be a good fit for smaller networks with fewer financial resources and those with fewer feature needs.

Management features

The full list of features and functionalities of a network switch will vary depending on the switch manufacturer and any additional software provided, but in general a switch will offer professionals the ability to:

- Enable and disable specific ports on the switch.
- Configure settings for duplex (half or full), as well as bandwidth.
- Set quality of service (QoS) levels for a specific port.
- Enable MAC filtering and other access control features.
- Set up SNMP monitoring of devices, including the health of the link.
- Configure port mirroring, for monitoring network traffic.

Other uses

In larger networks, switches are often used as a way to offload traffic for analytic purposes. This can be important to security, where a switch can be placed in front of a WAN router, before the traffic goes to the LAN. It can facilitate intrusion detection, performance analytics, and firewalling. In many cases, port mirroring is used to create a mirror image of the data flowing through the switch before it is sent to an intrusion detection system or packet sniffer, for example.

At its most basic, however, it is the simple task for a network switch to quickly and efficiently deliver packets from computer A to computer B, whether the computers are located across the hallway or halfway around the world. Several other devices contribute to this delivery along the way, but the switch is an essential part of the networking architecture.

Join the Network World communities on Facebook and LinkedIn to comment on topics that are top of mind.

Keith Shaw is a freelance digital journalist who has written about the IT world for more than 20 years.

Follow