To build a strong network and defend it, you need to understand the devices that comprise it.

What are network devices?

Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network.

Types of network devices

Here is the common network device list:

- Hub
- Switch
- Router
- Bridge
- Gateway
- Modem
- Repeater
- Access Point

> Handpicked related content:
>
> [Free Download] Network Security Best Practices

Hub

Hubs connect multiple computer networking devices together. A hub also acts as a repeater in that it amplifies signals that deteriorate after traveling long distances over connecting cables. A hub is the simplest in the family of network connecting devices because it connects LAN components with identical protocols.

A hub can be used with both digital and analog data, provided its settings have been configured to prepare for the formatting of the incoming data. For example, if the incoming data is in digital format, the hub must pass it on as packets; however, if the incoming data is analog, then the hub passes it on in signal form.

Hubs do not perform packet filtering or addressing functions; they just send data packets to all connected devices. Hubs operate at the Physical layer of the Open Systems Interconnection (OSI) model. There are two types of hubs: simple and multiple port.

Switch

Switches generally have a more intelligent role than hubs. A switch is a multiport device that improves network efficiency. The switch maintains limited routing information about nodes in the internal network, and it allows connections to systems like hubs or routers. Strands of LANs are usually connected using switches. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination.

Using switches improves network efficiency over hubs or routers because of the virtual circuit capability. Switches also improve network security because the virtual circuits are more difficult to examine with network monitors. You can think of a switch as a device that has some of the best capabilities of routers and hubs combined. A switch can work at either the Data Link layer or the Network layer of the OSI model. A multilayer switch is one that can operate at both layers, which means that it can operate as both a switch and a router. A multilayer switch is a high-performance device that supports the same routing protocols as routers.

Switches can be subject to distributed denial of service (DDoS) attacks; flood guards are used to prevent malicious traffic from bringing the switch to a halt. Switch port security is important so be sure to secure switches: Disable all unused ports and use DHCP snooping, ARP inspection and MAC address filtering.

> Handpicked related content:
>
> Why Native Network Device Auditing Is Not Enough

Router

Routers help transmit packets to their destinations by charting a path through the sea of interconnected networking devices using different network topologies. Routers are intelligent devices, and they store information about the networks they're connected to. Most routers can be configured to operate as packet-filtering firewalls and use access control lists (ACLs). Routers, in conjunction with a channel service unit/data service unit (CSU/DSU), are also used to translate from LAN framing to WAN framing. This is needed because LANs and WANs use different network protocols. Such routers are known as border routers. They serve as the outside connection of a LAN to a WAN, and they operate at the border of your network.

Router are also used to divide internal networks into two or more subnetworks. Routers can also be connected internally to other routers, creating zones that operate independently. Routers establish communication by maintaining tables about destinations and local connections. A router contains information about the systems connected to it and where to send requests if the destination isn't known. Routers usually communicate routing and other information using one of three standard protocols: Routing Information Protocol (RIP), Border Gateway Protocol (BGP) or Open Shortest Path First (OSPF).

Routers are your first line of defense, and they must be configured to pass only traffic that is authorized by network administrators. The routes themselves can be configured as static or dynamic. If they are static, they can only be configured manually and stay that way until changed. If they are dynamic, they learn of other routers around them and use information about those routers to build their routing tables.

Routers are general-purpose devices that interconnect two or more heterogeneous networks. They are usually dedicated to special-purpose computers, with separate input and output network interfaces for each connected network. Because routers and gateways are the backbone of large computer networks like the internet, they have special features that give them the flexibility and the ability to cope with varying network addressing schemes and frame sizes through segmentation of big packets into smaller sizes that fit the new network components. Each router interface has its own Address Resolution Protocol (ARP) module, its own LAN address (network card address) and its own Internet Protocol (IP) address. The router, with the help of a routing table, has knowledge of routes a packet could take from its source to its destination. The routing table, like in the bridge and switch, grows dynamically. Upon receipt of a packet, the router removes the packet headers and trailers and analyzes the IP header by determining the source and destination addresses and data type, and noting the arrival time. It also updates the router table with new addresses not already in the table. The IP header and arrival time information is entered in the routing table. Routers normally work at the Network layer of the OSI model.

> Handpicked related content:
>
> Why Monitoring of Network Devices Is Critical for Network Security

Bridge

Bridges are used to connect two or more hosts or network segments together. The basic role of bridges in network architecture is storing and forwarding frames between the different segments that the bridge connects. They use hardware Media Access Control (MAC) addresses for transferring frames. By looking at the MAC address of the devices connected to each segment, bridges can forward the data or block it from crossing. Bridges can also be used to connect two physical LANs into a larger logical LAN.

Bridges work only at the Physical and Data Link layers of the OSI model. Bridges are used to divide larger networks into smaller sections by sitting between two physical network segments and managing the flow of data between the two.

Bridges are like hubs in many respects, including the fact that they connect LAN components with identical protocols. However, bridges filter incoming data packets, known as frames, for addresses before they are forwarded. As it filters the data packets, the bridge makes no modifications to the format or content of the incoming data. The bridge filters and forwards frames on the network with the help of a dynamic bridge table. The bridge table, which is initially empty, maintains the LAN addresses for each computer in the LAN and the addresses of each bridge interface that connects the LAN to other LANs. Bridges, like hubs, can be either simple or multiple port.

Bridges have mostly fallen out of favor in recent years and have been replaced by switches, which offer more functionality. In fact, switches are sometimes referred to as “multiport bridges” because of how they operate.

Gateway

Gateways normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous protocols and standards from different vendors; gateways are used to deal with them. Gateways provide translation between networking technologies such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). Because of this, gateways connect two or more autonomous networks, each with its own routing algorithms, protocols, topology, domain name service, and network administration procedures and policies.

Gateways perform all of the functions of routers and more. In fact, a router with added translation functionality is a gateway. The function that does the translation between different network technologies is called a protocol converter.

Modem

Modems (modulators-demodulators) are used to transmit digital signals over analog telephone lines. Thus, digital signals are converted by the modem into analog signals of different frequencies and transmitted to a modem at the receiving location. The receiving modem performs the reverse transformation and provides a digital output to a device connected to a modem, usually a computer. The digital data is usually transferred to or from the modem over a serial line through an industry standard interface, RS-232. Many telephone companies offer DSL services, and many cable operators use modems as end terminals for identification and recognition of home and personal users. Modems work on both the Physical and Data Link layers.

Repeater

A repeater is an electronic device that amplifies the signal it receives. You can think of repeater as a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances, more than 100 meters for standard LAN cables. Repeaters work on the Physical layer.

Access Point

While an access point (AP) can technically involve either a wired or wireless connection, it commonly means a wireless device. An AP works at the second OSI layer, the Data Link layer, and it can operate either as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another.

Wireless access points (WAPs) consist of a transmitter and receiver (transceiver) device used to create a wireless LAN (WLAN). Access points typically are separate network devices with a built-in antenna, transmitter and adapter. APs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired Ethernet LAN. They also have several ports, giving you a way to expand the network to support additional clients. Depending on the size of the network, one or more

APs might be required to provide full coverage. Additional APs are used to allow access to more wireless clients and to expand the range of the wireless network. Each AP is limited by its transmission range — the distance a client can be from an AP and still obtain a usable signal and data process speed. The actual distance depends on the wireless standard, the obstructions and environmental conditions between the client and the AP. Higher end APs have high-powered antennas, enabling them to extend how far the wireless signal can travel.

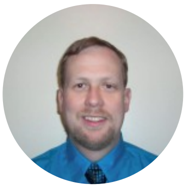
APs might also provide many ports that can be used to increase the network's size, firewall capabilities and Dynamic Host Configuration Protocol (DHCP) service. Therefore, we get APs that are a switch, DHCP server, router and firewall.

To connect to a wireless AP, you need a service set identifier (SSID) name. 802.11 wireless networks use the SSID to identify all systems belonging to the same network, and client stations must be configured with the SSID to be authenticated to the AP. The AP might broadcast the SSID, allowing all wireless clients in the area to see the AP's SSID. However, for security reasons, APs can be configured not to broadcast the SSID, which means that an administrator needs to give client systems the SSID instead of allowing it to be discovered automatically. Wireless devices ship with default SSIDs, security settings, channels, passwords and usernames. For security reasons, it is strongly recommended that you change these default settings as soon as possible because many internet sites list the default settings used by manufacturers.

Access points can be fat or thin. Fat APs, sometimes still referred to as autonomous APs, need to be manually configured with network and security settings; then they are essentially left alone to serve clients until they can no longer function. Thin APs allow remote configuration using a controller. Since thin clients do not need to be manually configured, they can be easily reconfigured and monitored. Access points can also be controller-based or stand-alone.

Conclusion

Having a solid understanding of the types of network devices available can help you design and built a network that is secure and serves your organization well. However, to ensure the ongoing security and availability of your network, you should carefully monitor your network devices and activity around them, so you can quickly spot hardware issues, configuration issues and attacks.



Jeff Melnick

Jeff is a former Director of Global Solutions Engineering at Netwrix. He is a long-time Netwrix blogger, speaker, and presenter. In the Netwrix blog, Jeff shares lifehacks, tips and tricks that can dramatically improve your system administration experience.

Network devices Network security