What Is a Network Switch? Meaning, Working, Types, and Uses

Network switches are multiport networking devices that receive data and relay it via MAC addresses. Here’s a detailed description of how it works, the various types of switches to choose from, and the top five uses of a network switch.

Technical Writer

Last Updated: July 28, 2022

A network switch is defined as a hardware component responsible for relaying data from a computer network to the destination endpoint through packet switching, MAC address identification, and a multiport bridge system. This article explains how a network switch works, its types, and its uses.

Table of Contents

What Is a Network Switch?

How Does a Network Switch Work?

Types of Network Switches

Top 5 Uses of a Network Switch

What Is a Network Switch?

A network switch is a hardware component responsible for relaying data from networks to the destination endpoint through packet switching, MAC address identification, and a multiport bridge system.

Cisco’s Industry-Standard Network Switch

Cisco’s Industry-Standard Network Switch | SourceOpens a new window

A network switch connects and transmits data packets to and from devices on a local area network (LAN). Far from a router, a switch only distributes information to the one device for which it was designed, including some other switch, a router, or a user’s computer, rather than to several devices in a network.

Nowadays, networks are critical for supporting companies, offering connected services, and enabling collaboration, among other things. As they link devices that share resources, network switches are a vital component of all networks.

A network switch works at the data link Layer 2 of the architecture of Open Systems Interconnection (OSI). It accepts packets from access points linked to physical ports and then sends them only via the ports going to a destination device.

These could also function where routing occurs at the network Layer 3. Switches are standard components in ethernet, fiber channels, InfiniBand, and asynchronous transfer mode (ATM) networks, to name a few. The majority of switches nowadays, however, utilize ethernet.

A network switch connects network devices (printers, computers, and wireless devices/access points, and enables users to exchange data packets. Switches may be both hardware and software-based virtual devices that govern physical systems. In today’s network systems, switches make up the vast bulk of network equipment.

They connect desktop PCs, industrial machinery, wireless access points, and specific internet of things (IoT) devices, including card entry systems for the internet.

They connect the machines in data centers that operate virtual machines (VMs) and most of the servers and storage devices. In telecommunications provider networks, they transport massive volumes of data.

See More:Opens a new window What Is Network Hardware? Definition, Architecture, Challenges, and Best Practices

How Does a Network Switch Work?

A network switch can work in three ways:

Edge switches, also known as access switches: They handle traffic entering and departing the network. Edge switches link various devices, including personal computers and access points.

Aggregation switches: Switches for aggregation or dissemination are located within an optional intermediary layer. These connect to edge switches, which may transmit traffic from one switch to another or up to the core switches.

Core switches: The network’s backbone is made up of these switches. Core switches link edge or aggregation switches, device or consumer edge networks to networks at data centers, and routers to organizational LANs.

As illustrated below, a network switch is a multiport bridge for networks operating at the OSI model’s data connection layer 2. It is responsible for data transmission using media access control address (MAC) addresses. Certain switches can forward data to the network layer (i.e., layer 3) because they are equipped with routing functionality. Layer 3 switches, often known as multilayer switches, are examples of such switches.

Network Switch is Part of Layer 2 in the OSI Model

Network Switch is Part of Layer 2 in the OSI Model

When frames are sent to a MAC address not recognized by the switch infrastructure, they are flooded to all the switching domain’s ports to be delivered to their intended recipient. Saturation also occurs in the frames used for broadcasting and multicasting. As part of the OSI design, the BUM flooding function transforms a switch into a data-link layer or Layer 2 device. BUM flooding refers to the flooding of unknown unicast, broadcast, and multicast traffic.

Switches are essential components of every network. They link several devices on the same network within a premises, such as PCs, printers, wireless access points, and servers.

A switch allows linked devices to transfer data and communicate with one another. When devices are connected to switches, they note the device’s media access control (MAC) information. This address is a code stored In the device’s network interface card (NIC), which is the part of the device that connects to the switch through an ethernet cable.

The MAC address determines which associated device sends outgoing packets and addresses where incoming packets should be delivered. Unlike the IP address of the network Layer 3, which may be assigned to a device on a sporadic basis and change with time, the MAC address is used to identify the physical endpoint device persistently. When a device transmits a packet to the other device, it reaches the switch, which scans the packet’s header to figure out what to do next.

It checks the address of the destination and transmits the packet to devices through the proper ports. Many switches are equipped with full-duplex capabilities to minimize the possibility of collisions in network traffic. This gives packets the entire bandwidth of the connection between the device and the switch.

Even though switches typically perform functions at Layer 2, they can perform at Layer 3. This is necessary to allow virtual local area networks (VLANs) — i.e., logical network segments that extend beyond subnets. Traffic must pass between switches to move from one subnet to another, which is made easier by their built-in routing capabilities.

See More: What Is Network Management? Definition, Key Components, and Best Practices

Types of Network Switches

Network switches are available in various types and categories to address different use cases. These are:

Types of Network Switches

Types of Network Switches

1. Managed switches

Managed switches, most commonly seen in commercial and enterprise settings, provide greater capacity and capabilities for IT experts. To configure managed switches, command-line interfaces are utilized. They enable simple network management protocol agents, which offer information for troubleshooting network issues.

Administrators can also use them to create virtual LANs to split a local network into smaller parts. Managed switches are substantially more expensive than unmanaged switches due to their additional functionality.

1. Unmanaged switches

The most basic switches are unmanaged switches, which have a set configuration. An unmanaged switch merely expands a LAN’s Ethernet connections, allowing additional internet connections to local devices. Unmanaged switches use device MAC addresses to transmit data back and forth. They are usually plug-and-play, meaning the user has few alternatives to pick from.

These switches could have default configurations for aspects like quality of service, but one cannot modify them. Unmanaged switches are relatively cheap, but poor capability renders them unsuitable for many corporate applications.

1. Power over ethernet (POE) switches

PoE capabilities are now available on some network switches, making installing IoT devices and other gear faster, simpler, and safer. PoE is a method of supplying DC power to low-power devices across a LAN wire. Low-power devices connected to a PoE-capable network switch will no longer require a power supply. When concealing connections isn’t possible, this avoids the need for additional power outlets and makes the installation seem efficient. A PoE-capable switch is also safer because the power output is low and intelligently managed.

1. Local area network (LAN) switches

LAN switches, or local area network switches, are typically used to link locations on a company’s internal LAN. It also is referred to as an Ethernet switch or a data switch. Allocating bandwidth efficiently prevents data packets from overlapping as they travel via a network. Before directing the delivered data packet to its intended destination, the LAN switch delivers it. These switches alleviate network congestion or bottlenecks by sending a packet of data solely to its intended receiver.

1. Smart switches

Managed switches are called smart or intelligent switches when they have characteristics that go beyond an unmanaged switch but are less than a conventional managed switch. They are therefore more advanced than unmanaged switches but less expensive than fully controllable ones.

Other alternatives, such as VLANs, may not offer as many functions as fully controlled switches. However, because they are less costly, they may be suitable for smaller networks with limited budgets and fewer feature requirements.

1. Modular switches

Modular switches allow you to add extension modules as needed, providing greater flexibility as the network grows. Expansion modules for wireless connection, firewalls, and network analysis are some examples of app-specific expansion options.

Additional connections, power sources, and cooling fans may be possible. However, these switches are significantly more expensive than fixed ones and often employed in massive networks. In most cases, they also include Layer 3 capabilities (in addition to Layer 2), allowing them to operate as network routers.

See More: What Is a Mesh Network? Meaning, Types Working, and Applications in 2022

1. Fixed-configuration switches

Fixed-configuration switches feature a fixed number of ports and are often not expandable, making them affordable over time. The most common switches on the market are these. They have a predetermined number of Ethernet ports, for example, 8 Gigabit Ports, 16 ports, 24 ports, and 48 ports, among others. They can have a variety of ports (in terms of speed and connection). However, port speeds are typically 1 Gbps (at the very least), and connectivity choices are either wired electrical ports (RJ45) or optical fiber ports.

1. Stackable switches

Stackable switches allow you to optimize your network while also increasing its reliability. With an actual stackable switch, these clusters of switches function as a single switch powered by a single SNMP/RMON agent, one domain, just one command line interface (CLI), or a Web interface.

The ability to create link aggregation groupings covering several units in the stack, transfer mirror traffic from one component to another in the stack, and configure Quality of Service (QoS) encompassing all units are all advantages of using these types of switches for connection.

1. Layer three switches

Switches are part of the OSI model’s Layer 2 layer. They function at the data network layer, and their main job is to forward ethernet frames as quickly as possible from one port to another. Because they operate at the Network Layer of the OSI model, these switches are referred to as Layer 3 switches. A Layer 3 switch is a hybrid of Layer 2 and 3 devices. Their software is more complex than traditional Layer 2 switches, and they can run dynamic routing protocols.

1. Data center switches

Data centers have exploded in popularity in recent years. Almost all major organizations consolidate their IT assets and networks into a few large data centers for easier administration, management, and other reasons. As a result, data center switches must-have features like high-speed performance, huge port capacity, low latency, virtualization support, security, and QoS, among others.

The Cisco Nexus range of devices is an excellent example of Data Center switches. These switches are ideal for implementing the software-defined network (SDN) concept and providing virtualization and programmability.

1. Switches with optical fiber ports

The RJ45 connector connects to a standard ethernet cable and is the most common switch interface. In many circumstances, you’ll need to employ a fiber-optic connection to extend connectivity beyond the 100-meter limit of standard ethernet cables. Switches with optical fiber ports often have RJ45 ports and additional fiber optic ports for connecting to fiber connections.

Small-form factor pluggable fiber optic ports are what they’re called. In most cases, optical fiber ports are utilized to connect to other remote switches, either inside the same building or across facilities located kilometers apart.

1. Keyboard, video, and mouse (KVM) switch

This switch connects numerous computers to a keyboard, mouse, or monitor. These switches are frequently used to control groups of servers while removing cords from the desktop. A KVM switch is an excellent interface for a user who wants to handle many machines from a single console. Keyboard hotkeys may typically be configured into these devices, allowing you to switch between PCs quickly. A KVM extender may bolster the switch’s reach by several hundred feet to transmit DVI, VGA, or HDMI video transmissions.

See More: How To Make Networks Ready for Cloud-First Era With SD-WAN

Top 5 Uses of a Network Switch

When deploying network switches, IT managers should remember the following use cases and applications:

Uses of a Network Switch

Uses of a Network Switch

1. Make a connection with several different hosts

A network switch may have endless ports for connecting cables, which is helpful in a star topology. In addition, switches connect many computers to the network system. Whether the computers are located across the room or halfway across the world, the primary function of a network switch is to move data packets from one computer to another efficiently. This is true regardless of the physical distance between the devices. A few other devices aid in transporting data along the route, but the switch is a critical component of the networking design.

Every port on a network switch has the same forwarding or filtering mechanism. Users can have several ports linking each switch by cascading multiple switches together, all of which can be set and operated individually in the group.

1. Offload network traffic

The usage of switches to offload traffic for analytical reasons is common. Switches in a network may help regulate different types of network traffic, such as traffic entering and leaving the network and connecting many network devices, such as personal computers and wireless access points. A key concept in this regard is “forwarding.”

Forwarding is the process of routing network traffic from one device connected to one port of a network switch to another device connected to another port of the switch. This process begins when one device is connected to one port and ends when another device is connected to a different switch port.

This is useful for network security since it allows a switch to be positioned in front of a wide area network (WAN) router before traffic is sent to the LAN. It is also like that using network switches will make intrusion detection, performance analysis, and setting up firewalls simpler. Before the data is sent to a packet sniffer or an intrusion detection system, for example, port mirroring can help make a mirror copy of the information traveling through the switch. This occurs before the information is sent to the destination. This aids in future analysis.

1. Optimize LAN bandwidth

Network switches divide the LAN network into many collision domains, each with its broadband connection, resulting in an increased LAN frequency band. While transferring frames, network switches can generate an unaltered square electrical signal.

Switches are devices that function at several OSI model levels at the same time, such as data links, networks, or transport layers. Multilayer switches are devices that operate at many layers at the same time. Effective switching is required to handle the increased network traffic from video and other bandwidth-intensive apps, more user devices, and more packets destined for servers and cloud storage. Any small or mid-sized firm may use LAN switching to maintain the speeds and reliability that users need.

1. Populate the MAC address table

As a Layer 2 device, a switch will base all of its decisions on the data contained in the L2 Header. Depending on the MAC address sources and destinations, switches will determine the forwarding path. Establishing a MAC address database that matches each of the Switch’s switch ports to the MAC locations of the devices connected is one of the jobs of the switch.

The MAC address database is empty at the outset, and when a switch receives data, it checks the originating MAC address field of the incoming frame. It populates the MAC address database with the source MAC addresses and the switch port collecting the packet. The switch will eventually have a wholly populated MAC address table as each connected device delivers something. One may then utilize this table to advance frames to their desired location intelligently.

1. Enable MAC filtering and other access control features

Finally, let us discuss the filtering use case of network switches. This function specifies that a Switch would never forward a frame back out of the same port that it was received at. One may use the MAC address filter to prevent specific nodes from connecting. You may achieve this by filtering source and destination MAC-layer ethernet addresses at a switch’s source (incoming) port.

Depending on your network access control needs, the filtering MAC address might be unicast, multicast, or broadcast. When a switch needs to flood a frame, the frame is copied and sent out to all switch ports save the one that got it. A host seldom sends a frame with the destination as its own MAC address. This is frequently due to a host having an incorrect situation or being malicious. When this occurs, the switch merely discards the frame in any case.

See More: How Does an Edge Network Work and What Does Its Future Hold? AT&T’s Theresa Lanowitz Answers

Takeaway

The global demand for network switches is constantly increasing to support an era of remote connectivity and the rise of IoT. IDC’s worldwide trackers found that the global switch market increased by 7.5% in Q3 of 2021. This is also due to the increase in the adoption of cloud computing, as network switches help to orchestrate, maintain, and stabilize resource distribution across large-scale cloud computing environments. In the next few years, this demand will grow further, making it essential to know about the operations of network switches.

Did this article help you understand network switches and how they work? Tell us on FacebookOpens a new window , TwitterOpens a new window , and LinkedInOpens a new window . We’d love to hear from you!

MORE ON NETWORKING

What Is a Computer Network? Definition, Objectives, Components, Types, and Best Practices

Top 10 Best Practices for Network Monitoring in 2022

Top 10 Enterprise Networking Hardware Companies in 2022

What Is Network Topology? Definition, Types With Diagrams, and Selection Best Practices for 2022

Wide Area Network (WAN) vs. Local Area Network (LAN): Key Differences and Similarities

Share This Article:

Chiradeep BasuMallick

Chiradeep BasuMallick

Technical Writer

Opens a new window

Chiradeep is a content marketing professional, a startup incubator, and a tech journalism speciali