**What is a router?** **https://github.com/openjdk/jdk/blob/master/src/java.base/share/classes/java/util/ArrayList.java**private Object[] grow(int minCapacity) { int oldCapacity = elementData.length; if (oldCapacity > 0 || elementData != DEFAULTCAPACITY\_EMPTY\_ELEMENTDATA) { int newCapacity = ArraysSupport.newLength(oldCapacity, minCapacity - oldCapacity, oldCapacity >> 1); return elementData = Arrays.copyOf(elementData, newCapacity); } else { return elementData = new Object[Math.max(DEFAULT\_CAPACITY, minCapacity)]; } }

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding [data packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/) to their intended [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/), and allowing multiple devices to use the same Internet connection.

There are several types of routers, but most routers pass data between [LANs (local area networks)](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/) and [WANs (wide area networks)](https://www.cloudflare.com/learning/network-layer/what-is-a-wan/). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router.

A WAN, by contrast, is a large network spread out over a vast geographic area. Large organizations and companies that operate in multiple locations across the country, for instance, will need separate LANs for each location, which then connect to the other LANs to form a WAN. Because a WAN is distributed over a large area, it often necessitates multiple routers and switches\*.

\**A*[*network switch*](https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/)*forwards data packets between groups of devices in the same network, whereas a router forwards data between different networks.*

**How does a router work?**

Think of a router as an air traffic controller and data packets as aircraft headed to different airports (or networks). Just as each plane has a unique destination and follows a unique route, each packet needs to be guided to its destination as efficiently as possible. In the same way that an air traffic controller ensures that planes reach their destinations without getting lost or suffering a major disruption along the way, a router helps direct data packets to their destination IP address.

In order to direct packets effectively, a router uses an internal routing table — a list of paths to various network destinations. The router reads a packet's header to determine where it is going, then consults the routing table to figure out the most efficient path to that destination. It then forwards the packet to the next network in the path.

To learn more about [IP](https://www.cloudflare.com/learning/network-layer/internet-protocol/) routing and the protocols that are used during this process, read [What is routing?](https://www.cloudflare.com/learning/network-layer/what-is-routing/)

**What is the difference between a router and a modem?**

Although some Internet service providers (ISPs) may combine a router and a modem within a single device, they are not the same. Each plays a different but equally important role in connecting networks to each other and to the Internet.

A router forms networks and manages the flow of data within and between those networks, while a modem connects those networks to the Internet. Modems forge a connection to the Internet by converting signals from an ISP into a digital signal that can be interpreted by any connected device. A single device may plug into a modem in order to connect to the Internet; alternately, a router can help distribute this signal to multiple devices within an established network, allowing all of them to connect to the Internet simultaneously.

Think of it like this: If Bob has a router, but no modem, he will be able to create a LAN and send data between the devices on that network. However, he will not be able to connect that network to the Internet. Alice, on the other hand, has a modem, but no router. She will be able to connect a single device to the Internet (for example, her work laptop), but cannot distribute that Internet connection to multiple devices (say, her laptop and her smartphone). Carol, meanwhile, has a router and a modem. Using both devices, she can form a LAN with her desktop computer, tablet, and smartphone and connect them all to the Internet at the same time.

**What are the different types of routers?**

In order to connect a LAN to the Internet, a router first needs to communicate with a modem. There are two primary ways to do this:

* *Wireless router:* A wireless router uses an Ethernet cable to connect to a modem. It distributes data by converting packets from binary code into radio signals, then wirelessly broadcasts them using antennae. Wireless routers do not establish LANs; instead, they create WLANs (wireless local area networks), which connect multiple devices using wireless communication.
* *Wired router:* Like a wireless router, a wired router also uses an Ethernet cable to connect to a modem. It then uses separate cables to connect to one or more devices within the network, create a LAN, and link the devices within that network to the Internet.

In addition to wireless and wired routers for small LANs, there are many specialized types of routers that serve specific functions:

* *Core router:* Unlike the routers used within a home or small business LAN, a core router is used by large corporations and businesses that transmit a high volume of data packets within their network. Core routers operate at the "core" of a network and do not communicate with external networks.
* *Edge router:* While a core router exclusively manages data traffic within a large-scale network, an edge router communicates with both core routers and external networks. Edge routers live at the "edge" of a network and use the [BGP (Border Gateway Protocol)](https://www.cloudflare.com/learning/security/glossary/what-is-bgp/) to send and receive data from other LANs and WANs.
* *Virtual router:* A virtual router is a software application that performs the same function as a standard hardware router. It may use the Virtual Router Redundancy Protocol (VRRP) to establish primary and backup virtual routers, should one fail.

**What is an SSID?**

SSID stands for "service set identifier," and it is the technical term for the name of the network that WLAN routers broadcast. SSIDs enable users to find and connect to the wireless network broadcast by the router (a properly secured router should require password entry as well). Consumer routers for WiFi networks usually have their factory-default SSID printed on the side or bottom.

**What are some of the security challenges associated with routers?**

**Vulnerability exploits:** All hardware-based routers come with automatically installed software known as firmware that helps the router perform its functions. Like any other piece of software, router firmware often contains vulnerabilities that cyber attackers can exploit (one [example](https://threatpost.com/netgear-zero-day-takeover-routers/156744/)), and router vendors periodically issue updates to patch these vulnerabilities. For this reason, router firmware needs to be updated regularly. Unpatched routers can be compromised by attackers, enabling them to monitor traffic or use the router as part of a [botnet](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/).

**DDoS attacks:** Small and large organizations often are the targets of distributed denial-of-service (DDoS) attacks directed at their network infrastructure. Unmitigated [network layer DDoS attacks](https://www.cloudflare.com/learning/ddos/layer-3-ddos-attacks/) can overwhelm routers or cause them to crash, resulting in network downtime. [Cloudflare Magic Transit](https://www.cloudflare.com/magic-transit/) is one solution for protecting routers and networks from these kinds of DDoS attacks.

**Administrative credentials**: All routers come with a set of admin credentials for performing administrative functions. These credentials are set to default values, such as "admin" as the username and "admin" as the password. The username and password should be reset to something more secure as soon as possible: attackers are aware of the common default values for these credentials and can use them to gain control of the router remotely if they are not reset.

<https://www.cloudflare.com/en-gb/learning/network-layer/what-is-a-packet/>

**DATA PACKETS**

**What is a packet?**

In [networking](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/), a packet is a small segment of a larger message. Data sent over computer networks\*, such as the [Internet](https://www.cloudflare.com/learning/network-layer/how-does-the-internet-work/), is divided into packets. These packets are then recombined by the computer or device that receives them.

Suppose Alice is writing a letter to Bob, but Bob's mail slot is only wide enough to accept envelopes the size of a small index card. Instead of writing her letter on normal paper and then trying to stuff it through the mail slot, Alice divides her letter into much shorter sections, each a few words long, and writes these sections out on index cards. She delivers the group of cards to Bob, who puts them in order to read the whole message.

This is similar to how packets work on the Internet. Suppose a user needs to load an image. The image file does not go from a [web server](https://www.cloudflare.com/learning/cdn/glossary/origin-server/) to the user's computer in one piece. Instead, it is broken down into packets of data, sent over the wires, cables, and radio waves of the Internet, and then reassembled by the user's computer into the original photo.

*\*A network is a group of two or more connected computers. The Internet is a network of networks — multiple networks around the world that are all interconnected with each other.*

**Why use packets?**

Theoretically, it could be possible to send files and data over the Internet without chopping them down into small packets of information. One computer could send data to another computer in the form of a long unbroken line of bits (small units of information, communicated as pulses of electricity that computers can interpret).

However, such an approach quickly becomes impractical when more than two computers are involved. While the long line of bits passed over the wires between the two computers, no third computer could use those same wires to send information — it would have to wait its turn.

In contrast to this approach, the Internet is a "packet switching" network. Packet switching refers to the ability of networking equipment to process packets independently from each other. It also means that packets can take different network paths to the same destination, so long as they all arrive at the destination. (In certain protocols, packets do need to arrive at their final destinations in the correct order, even if each packet took a different route to get there.)

Because of packet switching, packets from multiple computers can travel over the same wires in basically any order. This enables multiple connections to take place over the same networking equipment at the same time. As a result, billions of devices can exchange data on the Internet at the same time, instead of just a handful.

**What is a packet header?**

A packet header is a "label" of sorts, which provides information about the packet’s contents, origin, and destination.

When Alice sends her series of index cards to Bob, the words on those cards alone will not give Bob enough context to read the letter correctly. Alice needs to indicate the order that the index cards go in so that Bob does not read them out of order. She also should indicate that each one is from her, in case Bob receives messages from other people while she is delivering hers. So Alice adds this information to the top of each index card, above the actual words of her message. On the first card she writes "Letter from Alice, 1 of 20," on the second she writes "Letter from Alice, 2 of 20," and so on.

Alice has created a miniature header for her cards so that Bob does not lose them or mix them up. Similarly, all network packets include a header so that the device that receives them knows where the packets come from, what they are for, and how to process them.

Packets consist of two portions: the header and the payload. The header contains information about the packet, such as its origin and destination [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/) (an IP address is like a computer's mailing address). The payload is the actual data. Referring back to the photo example, the thousands of packets that make up the image each have a payload, and the payload carries a little piece of the image.

**Where do packet headers come from?**

In practice, packets actually have more than one header, and each header is used by a different part of the networking process. Packet headers are attached by certain types of networking protocols.

A protocol is a standardized way of formatting data so that any computer can interpret the data. Many different protocols make the Internet work. Some of these protocols add headers to packets with information associated with that protocol. At minimum, most packets that traverse the Internet will include a [Transmission Control Protocol (TCP)](https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/) header and an [Internet Protocol (IP)](https://www.cloudflare.com/learning/network-layer/internet-protocol/) header.

**What are packet trailers and footers?**

Packet headers go at the front of each packet. Routers, [switches](https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/), computers, and anything else that processes or receives a packet will see the header first. A packet can also have trailers and footers attached at the end. Like headers, these contain additional information about the packet.

Only certain network protocols attach trailers or footers to packets; most only attach headers. ESP (part of the [IPsec](https://www.cloudflare.com/learning/network-layer/what-is-ipsec/) suite) is one example of a network layer protocol that attaches trailers to packets.

**What is an IP packet?**

IP (Internet Protocol) is a network layer protocol that has to do with routing. It is used to make sure packets arrive at the correct destination.

Packets are sometimes defined by the protocol they are using. A packet with an IP header can be referred to as an "IP packet." An IP header contains important information about where a packet is from (its source IP address), where it is going (destination IP address), how large the packet is, and how long network routers should continue to forward the packet before dropping it. It may also indicate whether or not the packet can be fragmented, and include information about reassembling fragmented packets.

**Packets vs. datagrams**

"Datagram" is a segment of data sent over a packet-switched network. A datagram contains enough information to be routed from its source to its destination. By this definition, an IP packet is one example of a datagram. Essentially, datagram is an alternative term for "packet."

**What is network traffic? What is malicious network traffic?**

Network traffic is a term that refers to the packets that pass through a network, in the same way that automobile traffic refers to the cars and trucks that travel on roads.

However, not all packets are good or useful, and not all network traffic is safe. Attackers can generate malicious network traffic — data packets designed to compromise or overwhelm a network. This can take the form of a [distributed denial-of-service (DDoS) attack](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/), a [vulnerability exploitation](https://www.cloudflare.com/learning/security/what-is-web-application-security/), or several other forms of cyber attack.

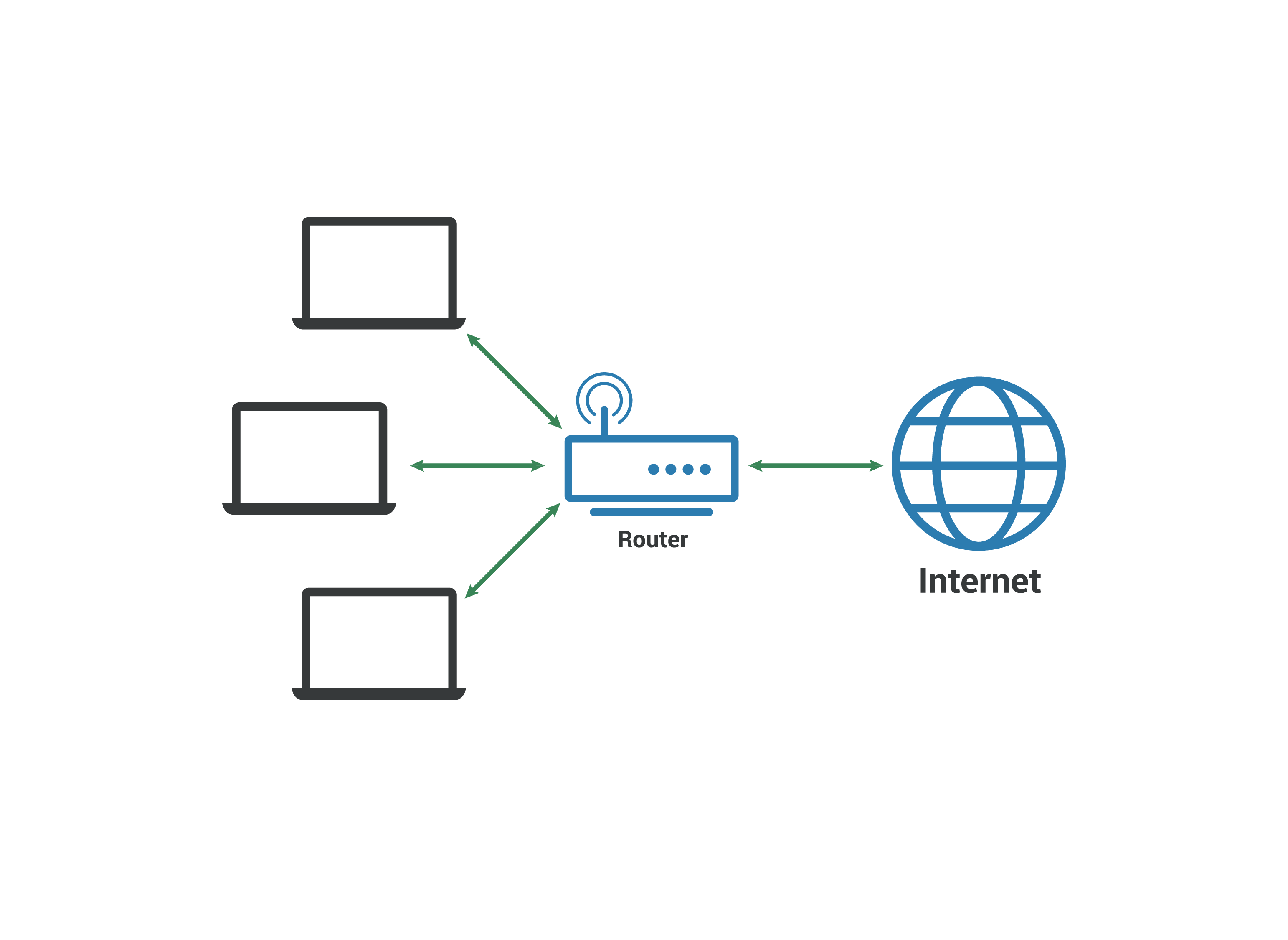
Cloudflare offers several products that protect against malicious network traffic. [Cloudflare Magic Transit](https://www.cloudflare.com/magic-transit/), for instance, protects company networks from [DDoS attacks at the network layer](https://www.cloudflare.com/learning/ddos/layer-3-ddos-attacks/) by extending the power of the Cloudflare global cloud network to on-premise, [hybrid](https://www.cloudflare.com/learning/cloud/what-is-hybrid-cloud/), and [cloud](https://www.cloudflare.com/learning/cloud/what-is-the-cloud/) infrastructure.

LAN

## What is a LAN (local area network)?

A local area network (LAN) is a network contained within a small geographic area, usually within the same building. Home WiFi networks and small business networks are common examples of LANs.

LANs can also be fairly large, although if they take up multiple buildings, it is usually more accurate to classify them as [wide area networks (WAN)](https://www.cloudflare.com/learning/network-layer/what-is-a-wan/) or [metropolitan area networks (MAN)](https://www.cloudflare.com/learning/network-layer/what-is-a-metropolitan-area-network/).



## How do LANs work?

Most LANs connect to the [Internet](https://www.cloudflare.com/learning/network-layer/how-does-the-internet-work/) at a central point: a [router](https://www.cloudflare.com/learning/network-layer/what-is-a-router/). Home LANs often use a single router, while LANs in larger spaces may additionally use [network switches](https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/) for more efficient packet delivery.

LANs almost always use Ethernet, WiFi, or both in order to connect devices within the network. Ethernet is a protocol for physical network connections that requires the use of Ethernet cables. WiFi is a protocol for connecting to a network via radio waves.

A variety of devices can connect to LANs, including servers, desktop computers, laptops, printers, IoT devices, and even game consoles. In offices, LANs are often used to provide shared access to internal employees to connected printers or servers.

## What equipment is needed to set up a LAN?

The simplest Internet-connected LANs require only a router and a way for computing devices to connect to the router, such as via Ethernet cables or a WiFi hotspot. LANs without an Internet connection need a switch for exchanging data. Large LANs, such as those in a large office building, may need additional routers or switches to more efficiently forward data to the right devices.

Not all LANs connect to the Internet. In fact, LANs predate the Internet: the first LANs were used in businesses in the late 1970s. (These old LANs used network protocols that are no longer in use today.) The only requirement for setting up a LAN is that the connected devices are able to exchange data. This usually requires a piece of networking equipment for packet switching, such as a network switch. Today, even non-Internet-connected LANs use the same networking protocols that are used on the Internet (such as [IP](https://www.cloudflare.com/learning/ddos/glossary/internet-protocol/)).

## What is a virtual LAN?

Virtual LANs, or VLANs, are a way of splitting up traffic on the same physical network into two networks. Imagine setting up two separate LANs, each with their own router and Internet connection, in the same room. VLANs are like that, but they are divided virtually using software instead of physically using hardware — only one router with one Internet connection is necessary.

VLANs help with network management, especially with very large LANs. By subdividing the network, administrators can manage the network much more easily. (VLANs are very different from [subnets](https://www.cloudflare.com/learning/network-layer/what-is-a-subnet/), which are another way of subdividing networks for greater efficiency.)

## What is the difference between a LAN and a WAN?

A WAN, or wide area network, is a collection of connected LANs. It is a widespread network of local networks. A WAN can be any size, even thousands of miles wide; it is not restricted to a given area.

## How do LANs relate to the rest of the Internet?

The Internet is a network of networks. LANs usually connect to a much larger network, an [autonomous system (AS)](https://www.cloudflare.com/learning/network-layer/what-is-an-autonomous-system/). ASes are very large networks with their own [routing](https://www.cloudflare.com/learning/network-layer/what-is-routing/) policies and with control over certain IP addresses. An Internet service provider (ISP) is one example of an AS.

Picture a LAN as a small network, that connects to a much larger network, that connects to other very large networks, all of which contain LANs. This is the Internet, and two computers connected to two different LANs thousands of miles apart can talk to each other by sending data over these connections between networks.

## How does Cloudflare protect LANs?

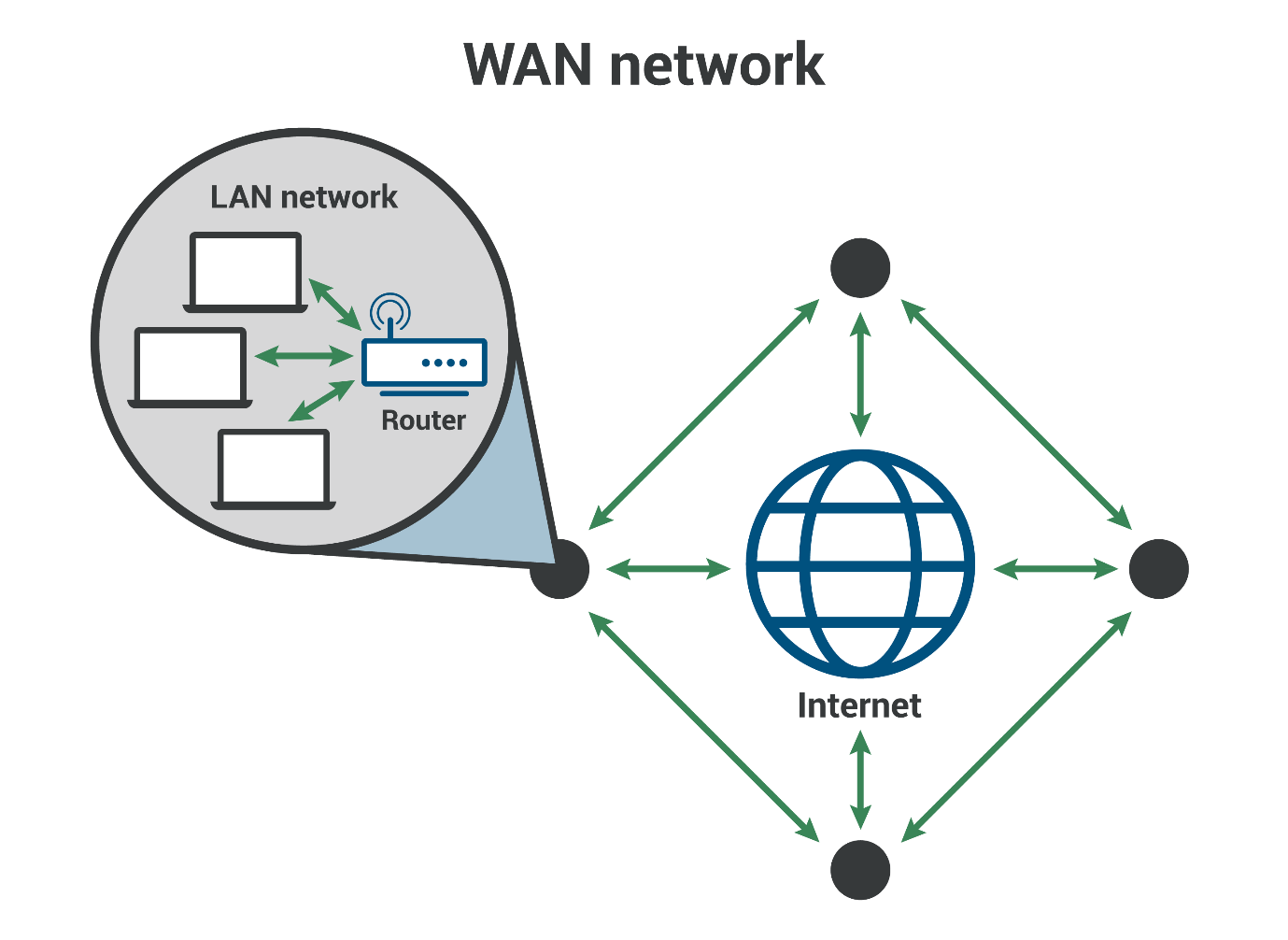
On-premise business infrastructure, such as LANs and their accompanying routers, switches, and servers, often face malicious attacks, including [DDoS](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/) attacks. [Cloudflare Magic Transit](https://www.cloudflare.com/magic-transit/) protects on-premise networks and infrastructure from malicious attacks, in addition to accelerating legitimate network traffic. Cloudflare Magic Transit also protects [cloud-hosted](https://www.cloudflare.com/learning/cloud/what-is-the-cloud/) and [hybrid](https://www.cloudflare.com/learning/cloud/what-is-hybrid-cloud/) networks.

WAN

**What is a wide area network (WAN)?**

A wide area network (WAN) is a large computer [network](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/) that connects groups of computers over large distances. WANs are often used by large businesses to connect their office networks; each office typically has its own local area network, or [LAN](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/), and these LANs connect via a WAN. These long connections may be formed in several different ways, including leased lines, [VPNs](https://www.cloudflare.com/learning/access-management/what-is-a-vpn/), or IP tunnels (see below).

The definition of what constitutes a WAN is fairly broad. Technically, any large network that spreads out over a wide geographic area is a WAN. The [Internet](https://www.cloudflare.com/learning/network-layer/how-does-the-internet-work/) itself is considered a WAN.



**What is a LAN?**

A local area network (LAN) is a network confined to a small, localized area. Home WiFi networks and small business networks are common examples of LANs. Typically, whoever manages the LAN also manages the networking equipment it uses. A small business, for instance, will manage the [routers](https://www.cloudflare.com/learning/network-layer/what-is-routing/) and [switches](https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/) involved in setting up the LAN.

**WAN vs. LAN**

LANs typically exist in a contained area and usually share a single central point of Internet connection. WANs are designed to provide network connectivity over long distances. They are usually made up of several connected LANs. An organization that sets up its own WAN will almost always rely on network infrastructure that is outside their control: for example, a company with an office in Paris and an office in New York will have to send data between these offices over undersea cables that cross the Atlantic Ocean.

Usually a WAN will include multiple routers and switches. A LAN only needs one router for connecting to the Internet or other LANs, although it may use switches as well.

**What is a leased line?**

One of the ways that organizations connect their LANs to form a WAN is by using something called a leased line. A leased line is a direct network connection rented from a large network provider such as an ISP. Building their own physical network infrastructure — including cables, routers, and Internet exchange points across hundreds or thousands of miles — would be an almost impossible task for most organizations. So instead, they lease a direct, dedicated connection from a company that already has this infrastructure.

**What is tunneling? What is a VPN?**

If a company does not want to pay for a leased line, they can connect their LANs using [tunneling](https://www.cloudflare.com/learning/network-layer/what-is-gre-tunneling/). In networking, tunneling is a method for encapsulating [data packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/)\* within other data packets so that they go somewhere that they would not go otherwise. Imagine mailing an envelope inside another envelope, with both envelopes having a different address, so that the internal envelope gets mailed from the external envelope's destination address. That is the general idea of tunneling, except data is contained within packets instead of envelopes.

Some network tunnels are [encrypted](https://www.cloudflare.com/learning/ssl/what-is-encryption/) in order to protect the packets' contents from anyone who might intercept them en route. Encrypted tunnels are called VPNs, or virtual private networks. VPN connections between WANs are more secure than unencrypted tunneling connections. [IPsec](https://www.cloudflare.com/learning/network-layer/what-is-ipsec/) is one common VPN encryption protocol.

The main drawback of using tunneling to connect LANs is that tunneling increases overhead; it takes more computing power, and thus more time, to send packets in this way. Encapsulating and encrypting each packet slows down communications, just as stuffing an envelope twice instead of once slows down how quickly it can be placed in the mail. Additionally, encapsulated packets may end up larger than some routers on the network can handle, resulting in [fragmentation](https://www.cloudflare.com/learning/network-layer/what-is-mtu/) and adding more delays.

*\*All data sent over a network is broken up into packets, which are smaller chunks of data. Each packet includes information about the packet's origin, destination, and position in the series of packets.*

**What is a software-defined WAN (SD-WAN)?**

A software-defined WAN, or [SD-WAN](https://www.cloudflare.com/learning/network-layer/what-is-an-sd-wan/), is a more flexible WAN architecture that can take advantage of multiple hardware platforms and connectivity options. The controlling software works with any networking hardware.

SD-WANs are one form of software-defined networking (SDN), which is a category of technologies that make it possible to manage networks with software. They are also a key component of [secure access service edge (SASE)](https://www.cloudflare.com/learning/access-management/what-is-sase/) solutions, which combine networking and network security functions into a single, cloud-based service.

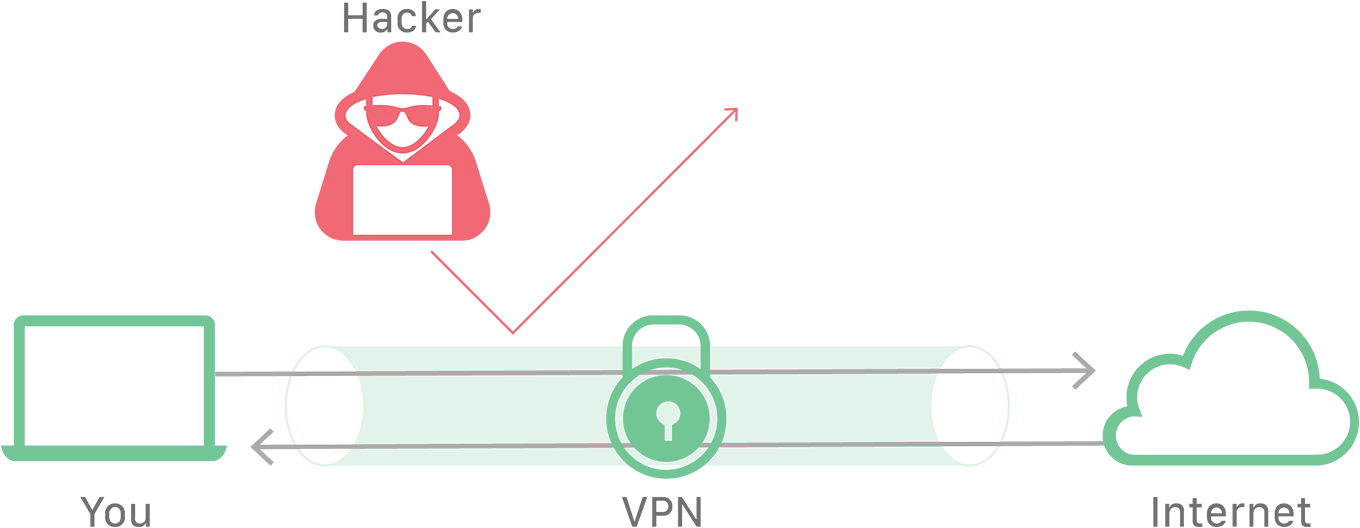
**What is WAN-as-a-service?**

WAN-as-a-service is a [cloud-based](https://www.cloudflare.com/learning/cloud/what-is-the-cloud/) WAN model. WAN-as-a-service offerings are designed to replace legacy WAN configurations that rely on hardware, use connectivity protocols like multiprotocol label switching ([MPLS](https://www.cloudflare.com/learning/network-layer/what-is-mpls/)), and are difficult to scale up. As WAN-as-a-service is offered via the cloud, customers only need Internet connectivity and can configure their WAN using software, instead of using hardware appliances. Learn about Cloudflare [Magic WAN](https://www.cloudflare.com/magic-wan); also see [What is network-as-a-service (NaaS)?](https://www.cloudflare.com/learning/network-layer/network-as-a-service-naas/)

**VPN**

**What is a VPN?**

A virtual private network (VPN) is an Internet security service that allows users to access the Internet as though they were connected to a private network. This encrypts Internet communications as well as providing a strong degree of anonymity. Some of the most common reasons people use VPNs are to protect against snooping on public WiFi, to circumvent Internet censorship, or to connect to a business’s internal network for the purpose of [remote work](https://www.cloudflare.com/learning/access-management/remote-workforce-security/).



**How does a VPN work?**

Ordinarily, most Internet traffic is unencrypted and very public. When a user creates an Internet connection, such as visiting a website in a browser, the user’s device will connect to their Internet Service Provider (ISP), and then the ISP will connect to the Internet to find the appropriate web server to communicate with to fetch the request website.

Information about the user is exposed in every step of the website request. Since the user’s [IP address](https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/) is exposed throughout the process, the ISP and any other intermediary can keep logs of the user’s browsing habits. Additionally, the data flowing between the user’s device and the web server is unencrypted; this creates opportunities for malicious actors to spy on the data or perpetrate attacks on the user, such as a [on-path attack](https://www.cloudflare.com/learning/security/threats/on-path-attack/).

Conversely, a user connecting to the Internet using a VPN service has a higher level of security and [privacy](https://www.cloudflare.com/learning/privacy/what-is-data-privacy/). A VPN connection involves the following 4 steps:

1. The VPN client\* connects to the ISP using an encrypted connection.
2. The ISP connects the VPN client to the VPN server, maintaining the encrypted connection.
3. The VPN server decrypts the data from the user’s device and then connects to the Internet to access the web server in an unencrypted communication.
4. The VPN server creates an encrypted connection with the client, known as a ‘VPN tunnel’.

The VPN tunnel between the VPN client and VPN server passes through the ISP, but since all the data is encrypted, the ISP cannot see the user’s activity. The VPN server’s communications with the Internet are unencrypted, but the web servers will only log the IP address of the VPN server, which gives them no information about the user.

\*The VPN client is the VPN software installed on the user’s device.

**Is a VPN only for people with something to hide?**

As with other Internet privacy services, VPNs are sometimes categorized as tools for illegal or subversive activity. The truth is that there are a number of valid and legitimate reasons to use a VPN. Here are a few of the most common:

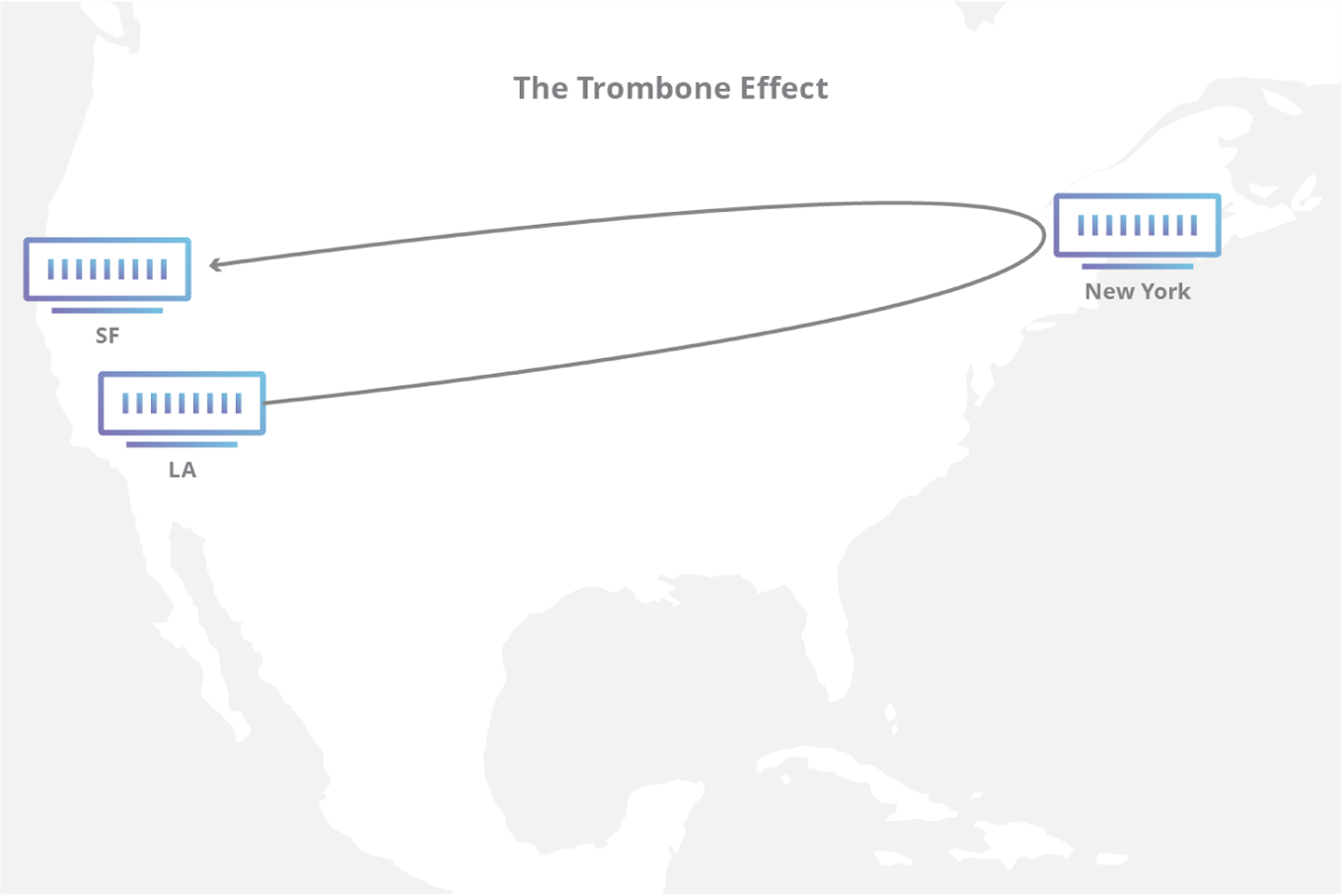
* **Protection over public WiFi** - Users who go on public WiFi networks without a VPN are putting themselves at risk. Their Internet traffic is unencrypted, and other users on the same network can monitor their activity using easily accessible tools. This is a common way for attackers to steal login credentials and other sensitive information. If a user is connected through a VPN, a snooping attacker will only be able to see encrypted data, which won’t reveal any sensitive information.
* **Remote work** - Many businesses allow their employees to work remotely using a VPN. This can allow the remote employee to have [access](https://www.cloudflare.com/learning/access-management/what-is-access-control/) to the company’s internal network, as well as provide encryption to protect the business from attackers or spying.
* **Freedom from censorship in oppressive states** - In some parts of the world, expressing or even reading views that are critical of the government is forbidden. Many of these states also provide their citizens with a suppressed version of the Internet that blocks significant amounts of domains. People accessing the Internet in these states can use a VPN to access content that their state wants blocked, as well as speak freely online, since VPN encryption protects their activity from state surveillance.
* **Location anonymity** - Some web services will restrict or filter content based on the location of the user. A VPN can be used to anonymize a user’s location and get around these restrictions.
* **The right to online privacy** - ISPs have been known to sell the private data of their uses. Similarly, some websites will sell information about their visitors. The privacy offered by VPN services enable consumers to opt out of having their data harvested.

**What are the downsides of a VPN?**

A VPN service does not guarantee an increased level of security; users can only feel secure with a VPN if they trust the VPN provider. A dishonest VPN provider could sell their users’ information or leave them open to attacks. It is also worth noting that most VPN services come at a recurring monthly cost. Some VPN users may also experience issues with performance.

**How does a VPN affect performance?**

Some users will experience performance degradation from a VPN, and this depends largely on which VPN service they are using. Not all VPNs are created equal, and if a VPN service does not have the server capacity to handle the load created by their users, those users will experience a slowdown in their Internet connection. Additionally, if a VPN is located a great distance from both the user and the web server they are trying to access, the resulting travel time can create latency. For example, if a user in San Francisco is accessing a web site whose servers are also in San Francisco, but that user’s VPN service is located in Tokyo, the user’s request will have to travel halfway around the world and back before connecting to a server just a few miles away. This is sometimes called the trombone effect.



## What is a network switch?

A network switch connects devices within a network (often a [local area network, or LAN](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/)\*) and forwards [data packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/) to and from those devices. Unlike a [router](https://www.cloudflare.com/learning/network-layer/what-is-a-router/), a switch only sends data to the single device it is intended for (which may be another switch, a router, or a user's computer), not to networks of multiple devices.

*\*A local area network (LAN) is a group of connected devices within close physical proximity. Home WiFi networks are one common example of a LAN.*

## What is the difference between a switch and a router?

Routers select paths for data packets to cross networks and reach their destinations. Routers do this by connecting with different networks and forwarding data from network to network — including LANs, [wide area networks (WANs)](https://www.cloudflare.com/learning/network-layer/what-is-a-wan/), or [autonomous systems](https://www.cloudflare.com/learning/network-layer/what-is-an-autonomous-system/), which are the large networks that make up the Internet.

In practice, what this means is that routers are necessary for an Internet connection, while switches are only used for interconnecting devices. Homes and small offices need routers for Internet access, but most do not need a network switch, unless they require a large amount of Ethernet\* ports. However, large offices, networks, and data centers with dozens or hundreds of computers usually do require switches.

*\*Ethernet is a layer 2*[*protocol*](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/)*for sending data between devices. Unlike WiFi, Ethernet requires a physical connection via an Ethernet cable.*

## What is a layer 2 switch? What is a layer 3 switch?

Network switches can operate at either [OSI](https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/) layer 2 (the data link layer) or [layer 3](https://www.cloudflare.com/learning/ddos/layer-3-ddos-attacks/) (the [network layer](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/)). Layer 2 switches forward data based on the destination MAC address (see below for definition), while layer 3 switches forward data based on the destination [IP address](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/). Some switches can do both.

Most switches, however, are layer 2 switches. Layer 2 switches most often connect to the devices in their networks using Ethernet cables. Ethernet cables are physical cables that plug into devices via Ethernet ports.

## What is an unmanaged switch? What is a managed switch?

An unmanaged switch simply creates more Ethernet ports on a LAN, so that more local devices can access the Internet. Unmanaged switches pass data back and forth based on device MAC addresses.

A managed switch fulfills the same function for much larger networks, and offers network administrators much more control over how traffic is prioritized. They also enable administrators to set up Virtual LANs (VLANs) to further subdivide a local network into smaller chunks.

## What is the difference between a MAC address and an IP address?

Network switches refer to MAC addresses in order to send Internet traffic to the right devices, not IP addresses.

Every device that connects to the Internet has an IP address. An IP address is a series of alphanumeric characters, like 192.0.2.255 or 2001:0db8:85a3:0000:0000:8a2e:0370:7334. IP addresses act like a mailing address, enabling Internet communications directed at that address to reach that device. IP addresses often change: because there is a limited number of IPv4 addresses, user devices are typically assigned new ones when they form a new connection with a network.

IP addresses are used at layer 3, which means computers and devices all over the Internet use IP addresses for sending and receiving data, no matter which network they are connected to. All IP packets include their source and destination IP addresses in their headers, just as a piece of mail has a destination address and a return address.

In contrast, a MAC address is a permanent identifier for each piece of hardware, somewhat like a serial number. Unlike IP addresses, MAC addresses do not change. MAC addresses are used at layer 2, not layer 3 — which means they are not included in IP packet headers. In other words, MAC addresses are not part of Internet traffic. They are only used inside a given network.

## How do network switches know the MAC addresses of the devices in their network?

Layer 2 network switches maintain a table in memory that matches MAC addresses to the switch's Ethernet ports. This table is called a Content Addressable Memory (CAM) table.

Suppose Computer A is connected to an Ethernet cable that plugs into the switch's Port 1, Computer B is connected to Port 2, and Computer C to Port 3. When data arrives for Computer A, the switch consults its CAM table, sees where Computer A is connected, and knows to forward Computer A-bound traffic at Port 1, not Ports 2 or 3.

The switch's CAM table would look something like this:

|  |  |
| --- | --- |
| **MAC address** | **Port** |
| Computer A's MAC address | 1 |
| Computer B's MAC address | 2 |
| Computer C's MAC address | 3 |

The switch's CAM table is stored in memory. If the switch is turned off, the table will disappear and the switch has to relearn the table when it is rebooted.

Now, suppose the switch was just turned on and has not yet created its CAM table. It does not know which ports Computers A, B, and C are connected to. It also does not know their MAC addresses.

|  |  |
| --- | --- |
| **MAC address** | **Port** |
| ? | ? |
| ? | ? |
| ? | ? |

Suppose Computer A sends a message to Computer B. The switch takes the following steps to get the message to Computer B and start filling out its CAM table:

* It records Computer A's MAC address and the port its message came in on
* It forwards Computer A's message to all other computers on the network (except Computer A); this is known as "flooding"
* When Computer B replies, it records Computer B's MAC address and port as well

|  |  |
| --- | --- |
| **MAC address** | **Port** |
| Computer A's MAC address | 1 |
| Computer B's MAC address | 2 |
| ? | ? |

Now, the switch's CAM table knows where Computer A and Computer B are. It also knows their MAC addresses.

## How does Cloudflare protect network switches?

Cloudflare Magic Transit protects network infrastructure devices such as switches and routers from [DDoS](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/) attack traffic that can knock them offline or compromise them. Magic Transit protects on-premise, [cloud](https://www.cloudflare.com/learning/cloud/what-is-the-cloud/), and [hybrid](https://www.cloudflare.com/learning/cloud/what-is-hybrid-cloud/) networks. Learn more about [Magic Transit](https://www.cloudflare.com/magic-transit/) or about [layer 3 attacks](https://www.cloudflare.com/learning/ddos/layer-3-ddos-attacks/).

**What is the Internet Protocol (IP)?**

The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called [packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/). IP information is attached to each packet, and this information helps [routers](https://www.cloudflare.com/learning/network-layer/what-is-a-router/) to send packets to the right place. Every device or [domain](https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/) that connects to the Internet is assigned an [IP address](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/), and as packets are directed to the IP address attached to them, data arrives where it is needed.

Once the packets arrive at their destination, they are handled differently depending on which transport protocol is used in combination with IP. The most common transport protocols are TCP and UDP.

**What is a network protocol?**

In networking, a [protocol](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/) is a standardized way of doing certain actions and formatting data so that two or more devices are able to communicate with and understand each other.

To understand why protocols are necessary, consider the process of mailing a letter. On the envelope, addresses are written in the following order: name, street address, city, state, and zip code. If an envelope is dropped into a mailbox with the zip code written first, followed by the street address, followed by the state, and so on, the post office won't deliver it. There is an agreed-upon protocol for writing addresses in order for the postal system to work. In the same way, all IP data packets must present certain information in a certain order, and all IP addresses follow a standardized format.

**What is an IP address? How does IP addressing work?**

An IP address is a unique identifier assigned to a device or domain that connects to the Internet. Each IP address is a series of characters, such as '192.168.1.1'. Via [DNS](https://www.cloudflare.com/learning/dns/what-is-dns/) resolvers, which translate human-readable domain names into IP addresses, users are able to access websites without memorizing this complex series of characters. Each IP packet will contain both the IP address of the device or domain sending the packet and the IP address of the intended recipient, much like how both the destination address and the return address are included on a piece of mail.

**IPv4 vs. IPv6**

The fourth version of IP (IPv4 for short) was introduced in 1983. However, just as there are only so many possible permutations for automobile license plate numbers and they have to be reformatted periodically, the supply of available IPv4 addresses has become depleted. IPv6 addresses have many more characters and thus more permutations; however, IPv6 is not yet completely adopted, and most domains and devices still have IPv4 addresses. For more on IPv4 and IPv6, see [What is my IP address?](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/)

**What is an IP packet?**

IP packets are created by adding an IP header to each packet of data before it is sent on its way. An IP header is just a series of bits (ones and zeros), and it records several pieces of information about the packet, including the sending and receiving IP address. IP headers also report:

* Header length
* Packet length
* [Time to live (TTL)](https://www.cloudflare.com/learning/cdn/glossary/time-to-live-ttl/), or the number of network hops a packet can make before it is discarded
* Which transport protocol is being used (TCP, UDP, etc.)

In total there are 14 fields for information in IPv4 headers, although one of them is optional.

**How does IP routing work?**

The Internet is made up of interconnected large networks that are each responsible for certain blocks of IP addresses; these large networks are known as [autonomous systems (AS)](https://www.cloudflare.com/learning/network-layer/what-is-an-autonomous-system/). A variety of routing protocols, including [BGP](https://www.cloudflare.com/learning/security/glossary/what-is-bgp/), help route packets across ASes based on their destination IP addresses. Routers have routing tables that indicate which ASes the packets should travel through in order to reach the desired destination as quickly as possible. Packets travel from AS to AS until they reach one that claims responsibility for the targeted IP address. That AS then internally routes the packets to the destination.

Protocols attach packet headers at different layers of the OSI model:

Packets can take different routes to the same place if necessary, just as a group of people driving to an agreed-upon destination can take different roads to get there.

**What is TCP/IP?**

The Transmission Control Protocol (TCP) is a transport protocol, meaning it dictates the way data is sent and received. A TCP header is included in the data portion of each packet that uses [TCP/IP](https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/). Before transmitting data, TCP opens a connection with the recipient. TCP ensures that all packets arrive in order once transmission begins. Via TCP, the recipient will acknowledge receiving each packet that arrives. Missing packets will be sent again if receipt is not acknowledged.

TCP is designed for reliability, not speed. Because TCP has to make sure all packets arrive in order, loading data via TCP/IP can take longer if some packets are missing.

TCP and IP were originally designed to be used together, and these are often referred to as the TCP/IP suite. However, other transport protocols can be used with IP.

**What is UDP/IP?**

The User Datagram Protocol, or [UDP](https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/), is another widely used transport protocol. It is faster than TCP, but it is also less reliable. UDP does not make sure all packets are delivered and in order, and it does not establish a connection before beginning or receiving transmissions.

**Do network switches refer to IP addresses?**

A network switch is an appliance that forwards data packets within a [local area network (LAN)](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/). Most network switches operate at layer 2, the data link layer, not layer 3, the network layer, and therefore use MAC addresses to forward packets, not IP addresses. To learn more, see [What is a network switch?](https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/)

**What is an IP address and why does it matter?**

‘IP’ stands for [Internet Protocol](https://www.cloudflare.com/learning/network-layer/internet-protocol/), which is the set of rules that makes it possible for devices to communicate over the [Internet](https://www.cloudflare.com/learning/network-layer/how-does-the-internet-work/). With billions of people accessing the Internet every day, unique identifiers are necessary to keep track of who is doing what. The Internet Protocol solves this by assigning IP numbers to every device accessing the Internet.

A computer’s IP address is like the physical address of a house. If someone calls a pizzeria to order a delivery, they need to provide their physical address. Without that address, the pizza delivery person will have no idea which house to deliver the pizza to.

For example, when a user types a [domain name](https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/), like google.com, into a web browser, this will initiate a request to Google’s web server asking for content (the Google homepage). Once Google receives the request, it needs to know where to send the website content. For this reason, the request will contain the asker’s IP address. Using the provided IP address, Google can send a response back to the user’s device, which will then display that content in the user’s web browser.

The system that orchestrates all this is called [DNS](https://www.cloudflare.com/learning/dns/what-is-dns/). It works like a phone book for IP addresses so that users can access web services using human-friendly domain names. When a user types a domain name like ‘facebook.com’ into their browser window, this begins a DNS query which ultimately leads to a [DNS server](https://www.cloudflare.com/learning/dns/dns-server-types/) translating the domain name into an IP address.

What do IP addresses look like? These addresses have a different format based on whether they are IPv4 or IPv6.

**What is the difference between IPv4 and IPv6?**

IPv4 and IPv6 are different versions of the Internet Protocol. IPv4 was implemented in 1983 and is still in use today. The format for IPv4 addresses is four sets of numbers separated by dots, for example: ‘192.0.2.1’. This is a 32-bit format, which means that it allows for 232, or about 4.3 billion, unique IP addresses, which it turns out is not enough for the amount of devices that are now on the Internet. The need for more IP addresses led to the implementation of IPv6.\* IPv6 addresses use a more complex format that utilizes sets of numbers and letters separated by single or double colons, for example: ‘2001:0db8:85a3:0000:0000:8a2e:0370:7334’. This 128-bit format can support 2128 unique addresses. (That computes to a 39-digit number!)

IPv6 provides some other updates to IPv4, including security and [privacy](https://www.cloudflare.com/learning/privacy/what-is-data-privacy/) improvements. Despite their differences, both IPv4 and IPv6 have been used concurrently on the web for over a decade. The two versions can run in parallel, but special measures had to be implemented to facilitate communications between IPv4 and IPv6 devices. This compromise had to be made because so much of the web is still running on IPv4 addresses.

*\*What happened to IPv5? IPv5 was an experimental streaming data protocol that was never implemented. It used the same 32-bit formatting as IPv4, so it did not adequately solve the problem of not having enough unique IP addresses. For this reason, IPv6 became the successor to IPv4.*

**What is the difference between static IPs and dynamic IPs?**

The limited supply of IPv4 addresses led to the introduction of dynamically assigning IP addresses, which is still a very common practice. Most devices connected to the Internet are assigned temporary IP addresses.

For example, when a home user connects to the Internet on their laptop, that user’s ISP assigns them a temporary IP address from a pool of shared IP addresses. This is known as a dynamic IP address. This is more cost-effective for the ISP than assigning each user a permanent, or static, IP address.

Some ISP customers, such as large enterprises, will pay to maintain a static IP address (for example, Cloudflare’s [1.1.1.1](https://www.cloudflare.com/learning/dns/what-is-1.1.1.1/)). However, for most users, having a dynamic IP address is sufficient. When hosting a web server, such as a self-hosted website, [API](https://www.cloudflare.com/learning/security/api/what-is-an-api/), or gaming server, a dynamic IP address can create problems. A change in IP address can cause their DNS queries to fail, effectively taking the resource offline. Luckily, this issue can easily be corrected with Cloudflare’s [dynamic DNS](https://www.cloudflare.com/learning/dns/glossary/dynamic-dns/).

## What is DNS?

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through [domain names](https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/), like nytimes.com or espn.com. Web browsers interact through [Internet Protocol (IP)](https://www.cloudflare.com/learning/network-layer/internet-protocol/) addresses. DNS translates domain names to [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/) so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).



## How does DNS work?

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.

In order to understand the process behind the DNS resolution, it’s important to learn about the different hardware components a DNS query must pass between. For the web browser, the DNS lookup occurs "behind the scenes" and requires no interaction from the user’s computer apart from the initial request.

## There are 4 DNS servers involved in loading a webpage:

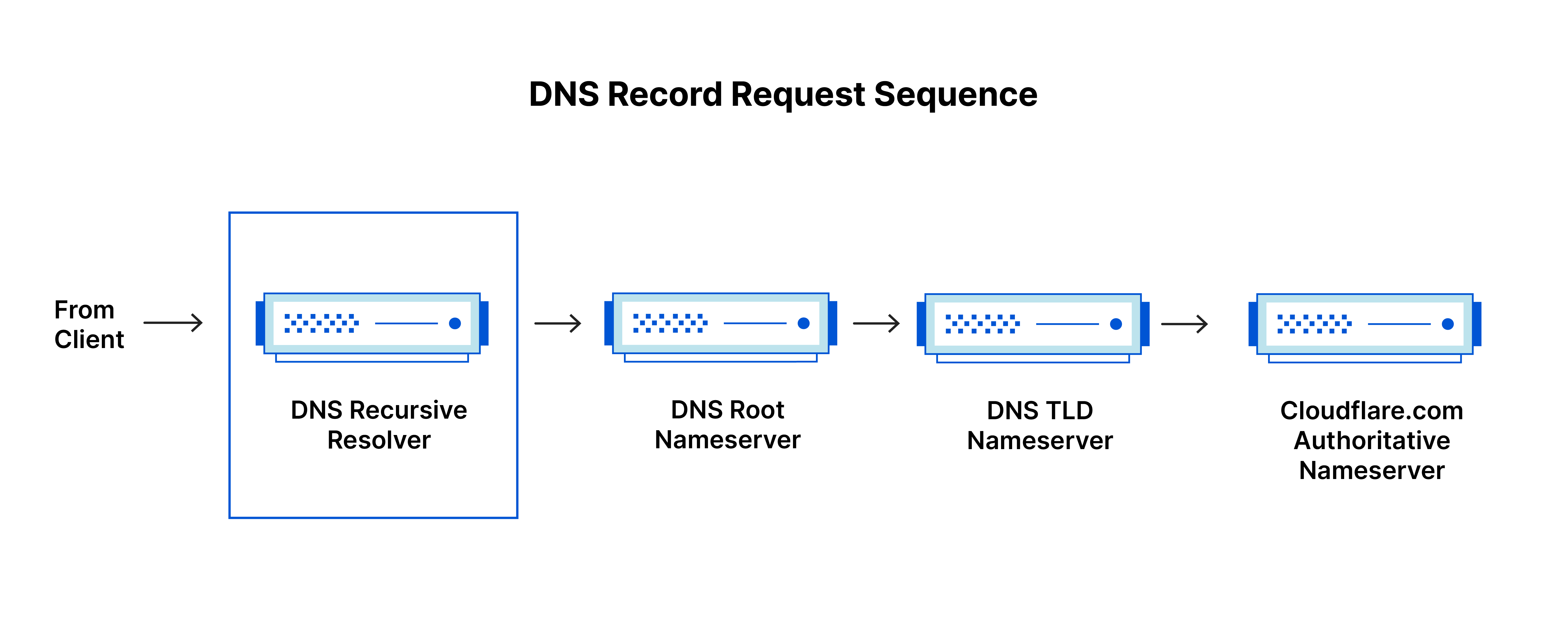
* [DNS recursor](https://www.cloudflare.com/learning/dns/dns-server-types/) - The recursor can be thought of as a librarian who is asked to go find a particular book somewhere in a library. The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers. Typically the recursor is then responsible for making additional requests in order to satisfy the client’s DNS query.
* **Root nameserver** - The [root server](https://www.cloudflare.com/learning/dns/glossary/dns-root-server/) is the first step in translating (resolving) human readable host names into IP addresses. It can be thought of like an index in a library that points to different racks of books - typically it serves as a reference to other more specific locations.
* [TLD nameserver](https://www.cloudflare.com/learning/dns/dns-server-types/) - The top level domain server ([TLD](https://www.cloudflare.com/learning/dns/top-level-domain/)) can be thought of as a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is “com”).
* [Authoritative nameserver](https://www.cloudflare.com/learning/dns/dns-server-types/) - This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be translated into its definition. The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor (the librarian) that made the initial request.

## What's the difference between an authoritative DNS server and a recursive DNS resolver?

Both concepts refer to servers (groups of servers) that are integral to the DNS infrastructure, but each performs a different role and lives in different locations inside the pipeline of a DNS query. One way to think about the difference is the [recursive](https://www.cloudflare.com/learning/dns/what-is-recursive-dns/) resolver is at the beginning of the DNS query and the authoritative nameserver is at the end.

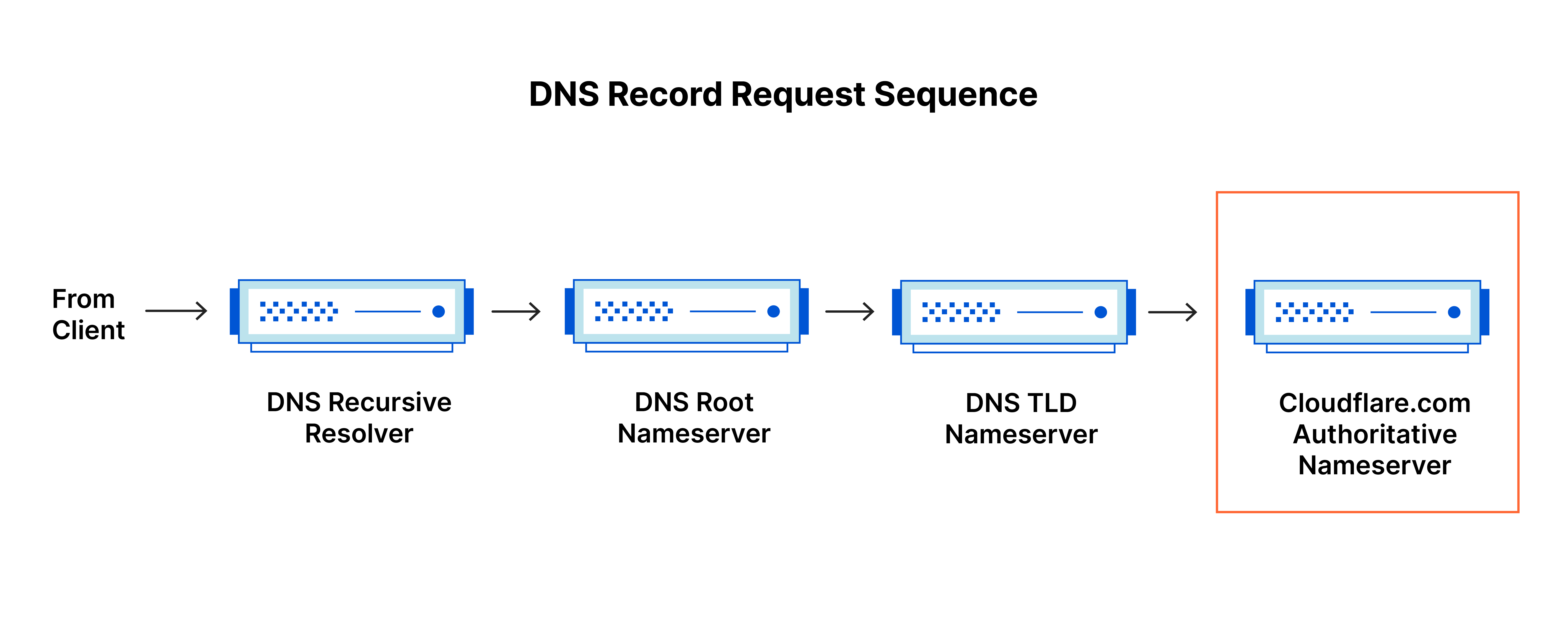
#### Recursive DNS resolver

The recursive resolver is the computer that responds to a recursive request from a client and takes the time to track down the [DNS record](https://www.cloudflare.com/learning/dns/dns-records/). It does this by making a series of requests until it reaches the authoritative DNS nameserver for the requested record (or times out or returns an error if no record is found). Luckily, recursive DNS resolvers do not always need to make multiple requests in order to track down the records needed to respond to a client; [caching](https://www.cloudflare.com/learning/cdn/what-is-caching/) is a data persistence process that helps short-circuit the necessary requests by serving the requested resource record earlier in the DNS lookup.

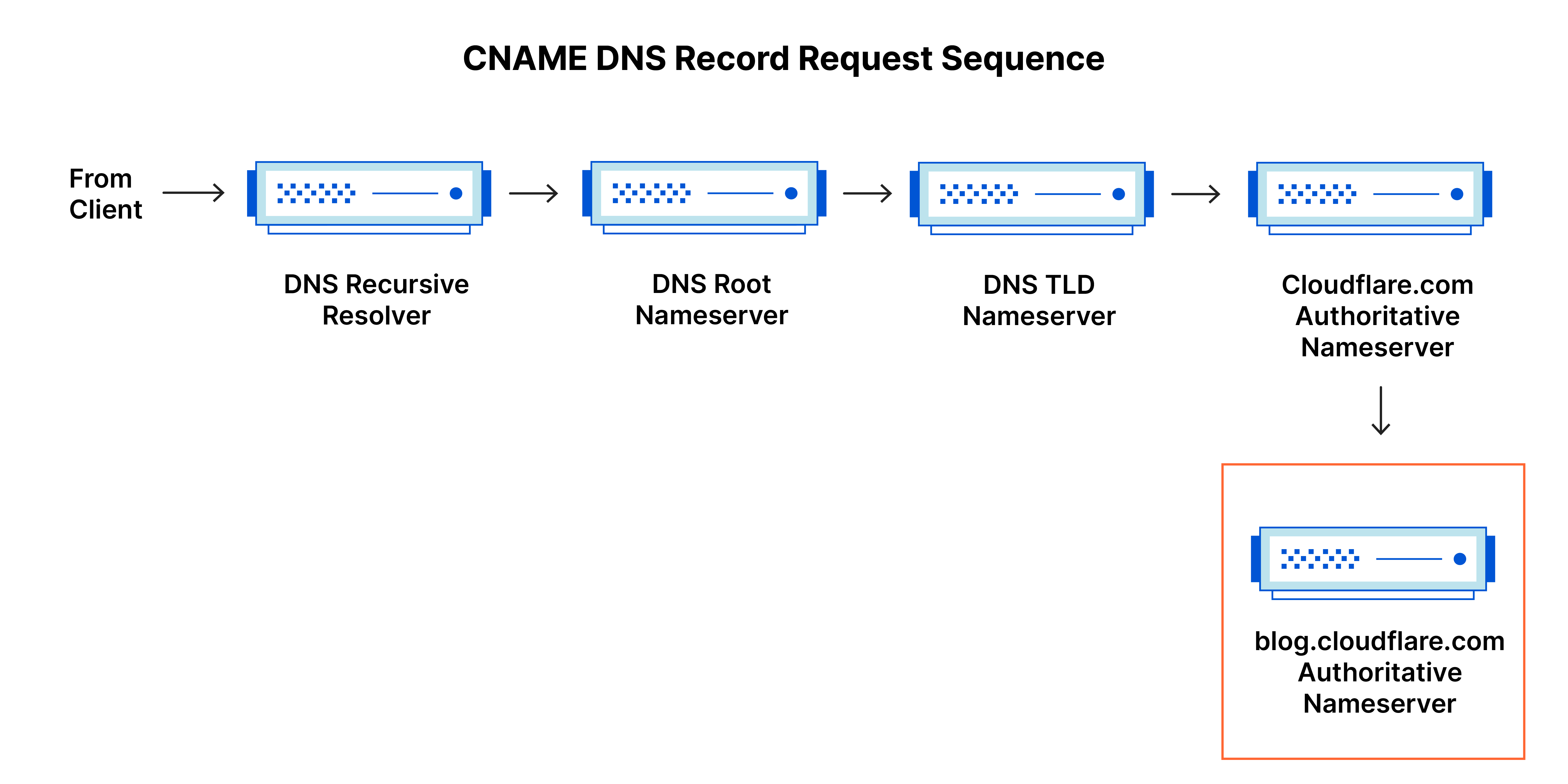


#### Authoritative DNS server

Put simply, an authoritative DNS server is a server that actually holds, and is responsible for, DNS resource records. This is the server at the bottom of the DNS lookup chain that will respond with the queried resource record, ultimately allowing the web browser making the request to reach the IP address needed to access a website or other web resources. An authoritative nameserver can satisfy queries from its own data without needing to query another source, as it is the final source of truth for certain DNS records.



It’s worth mentioning that in instances where the query is for a subdomain such as foo.example.com or [blog.cloudflare.com](https://blog.cloudflare.com/), an additional nameserver will be added to the sequence after the authoritative nameserver, which is responsible for storing the subdomain’s [CNAME record](https://www.cloudflare.com/learning/dns/dns-records/dns-cname-record/).



There is a key difference between many DNS services and the one that Cloudflare provides. Different DNS recursive resolvers such as Google DNS, OpenDNS, and providers like Comcast all maintain data center installations of DNS recursive resolvers. These resolvers allow for quick and easy queries through optimized clusters of DNS-optimized computer systems, but they are fundamentally different than the nameservers hosted by Cloudflare.

Cloudflare maintains infrastructure-level nameservers that are integral to the functioning of the Internet. One key example is the [f-root server network](https://blog.cloudflare.com/f-root/) which Cloudflare is partially responsible for hosting. The F-root is one of the root level DNS nameserver infrastructure components responsible for the billions of Internet requests per day. Our [Anycast network](https://www.cloudflare.com/learning/cdn/glossary/anycast-network/) puts us in a unique position to handle large volumes of DNS traffic without service interruption.

## What are the steps in a DNS lookup?

For most situations, DNS is concerned with a domain name being translated into the appropriate IP address. To learn how this process works, it helps to follow the path of a DNS lookup as it travels from a web browser, through the DNS lookup process, and back again. Let's take a look at the steps.

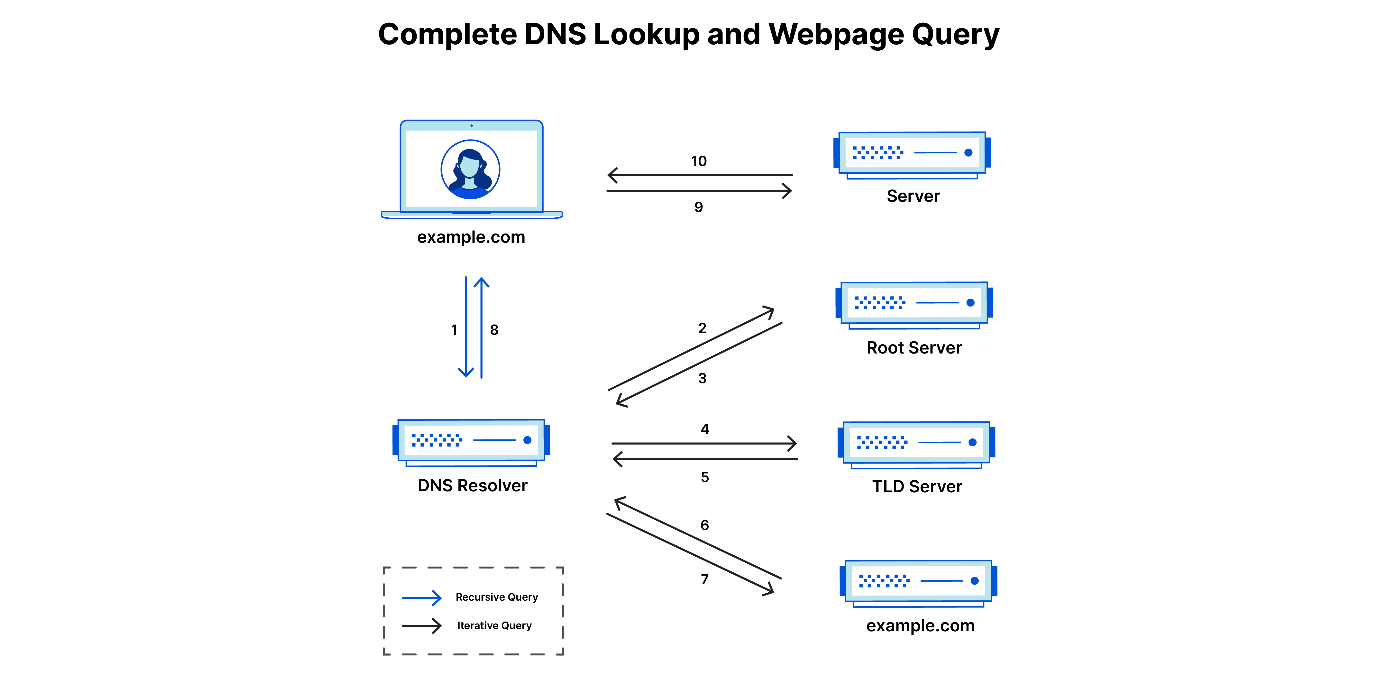
Note: Often DNS lookup information will be cached either locally inside the querying computer or remotely in the DNS infrastructure. There are typically 8 steps in a DNS lookup. When DNS information is cached, steps are skipped from the DNS lookup process which makes it quicker. The example below outlines all 8 steps when nothing is cached.

#### The 8 steps in a DNS lookup:

1. A user types ‘example.com’ into a web browser and the query travels into the Internet and is received by a DNS recursive resolver.
2. The resolver then queries a DNS root nameserver (.).
3. The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD.
4. The resolver then makes a request to the .com TLD.
5. The TLD server then responds with the IP address of the domain’s nameserver, example.com.
6. Lastly, the recursive resolver sends a query to the domain’s nameserver.
7. The IP address for example.com is then returned to the resolver from the nameserver.
8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially.

Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser is able to make the request for the web page:

1. The browser makes a [HTTP](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/) request to the IP address.
2. The server at that IP returns the webpage to be rendered in the browser (step 10).

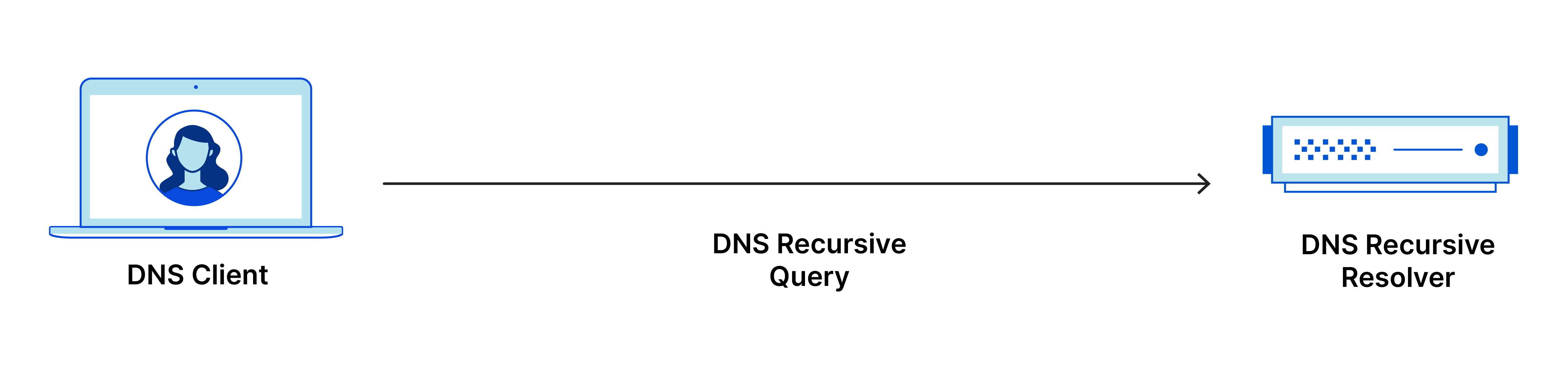


## What is a DNS resolver?

The DNS resolver is the first stop in the DNS lookup, and it is responsible for dealing with the client that made the initial request. The resolver starts the sequence of queries that ultimately leads to a URL being translated into the necessary IP address.

Note: A typical uncached DNS lookup will involve both recursive and iterative queries.

It's important to differentiate between a [recursive DNS](https://www.cloudflare.com/learning/dns/what-is-recursive-dns/) query and a recursive DNS resolver. The query refers to the request made to a DNS resolver requiring the resolution of the query. A DNS recursive resolver is the computer that accepts a recursive query and processes the response by making the necessary requests.



## What are the types of DNS queries?

In a typical DNS lookup three types of queries occur. By using a combination of these queries, an optimized process for DNS resolution can result in a reduction of distance traveled. In an ideal situation cached record data will be available, allowing a DNS name server to return a non-recursive query.

#### 3 types of DNS queries:

1. **Recursive query** - In a recursive query, a DNS client requires that a DNS server (typically a DNS recursive resolver) will respond to the client with either the requested resource record or an error message if the resolver can't find the record.
2. **Iterative query** - in this situation the DNS client will allow a DNS server to return the best answer it can. If the queried DNS server does not have a match for the query name, it will return a referral to a DNS server authoritative for a lower level of the domain namespace. The DNS client will then make a query to the referral address. This process continues with additional DNS servers down the query chain until either an error or timeout occurs.
3. **Non-recursive query** - typically this will occur when a DNS resolver client queries a DNS server for a record that it has access to either because it's authoritative for the record or the record exists inside of its cache. Typically, a DNS server will cache DNS records to prevent additional bandwidth consumption and load on upstream servers.

## What is DNS caching? Where does DNS caching occur?

The purpose of caching is to temporarily stored data in a location that results in improvements in performance and reliability for data requests. DNS caching involves storing data closer to the requesting client so that the DNS query can be resolved earlier and additional queries further down the DNS lookup chain can be avoided, thereby improving load times and reducing bandwidth/CPU consumption. DNS data can be cached in a variety of locations, each of which will store DNS records for a set amount of time determined by a [time-to-live (TTL)](https://www.cloudflare.com/learning/cdn/glossary/time-to-live-ttl/).

#### Browser DNS caching

Modern web browsers are designed by default to cache DNS records for a set amount of time. The purpose here is obvious; the closer the DNS caching occurs to the web browser, the fewer processing steps must be taken in order to check the cache and make the correct requests to an IP address. When a request is made for a DNS record, the browser cache is the first location checked for the requested record.

In Chrome, you can see the status of your DNS cache by going to chrome://net-internals/#dns.

#### Operating system (OS) level DNS caching

The operating system level DNS resolver is the second and last local stop before a DNS query leaves your machine. The process inside your operating system that is designed to handle this query is commonly called a “stub resolver” or DNS client. When a stub resolver gets a request from an application, it first checks its own cache to see if it has the record. If it does not, it then sends a DNS query (with a recursive flag set), outside the local network to a DNS recursive resolver inside the Internet service provider (ISP).

When the recursive resolver inside the ISP receives a DNS query, like all previous steps, it will also check to see if the requested host-to-IP-address translation is already stored inside its local persistence layer.

The recursive resolver also has additional functionality depending on the types of records it has in its cache:

1. If the resolver does not have the [A records](https://www.cloudflare.com/learning/dns/dns-records/dns-a-record/), but does have the [NS records](https://www.cloudflare.com/learning/dns/dns-records/dns-ns-record/) for the authoritative nameservers, it will query those name servers directly, bypassing several steps in the DNS query. This shortcut prevents lookups from the root and .com nameservers (in our search for example.com) and helps the resolution of the DNS query occur more quickly.
2. If the resolver does not have the NS records, it will send a query to the TLD servers (.com in our case), skipping the root server.
3. In the unlikely event that the resolver does not have records pointing to the TLD servers, it will then query the root servers. This event typically occurs after a DNS cache has been purged.

Learn about what differentiates [Cloudflare DNS](https://www.cloudflare.com/dns/) from other DNS providers.

<https://learn.microsoft.com/en-us/linkedin/consumer/integrations/self-serve/share-on-linkedin>