Networking Concepts

Refer Links:

https://www.geeksforgeeks.org/computer-network-tutorials/?ref=lbp

or https://www.geeksforgeeks.org/

*__Networking__: Networking is defined as the act of making contact and exchanging information with other people, groups and institutions to develop mutually beneficial relationships, or to access and share information between computers.

What are the 7 types of network?

***7 Types of Computer Networks Explained**

PERSONAL AREA NETWORK (PAN)

LOCAL AREA NETWORK (LAN)

WIRELESS LOCAL AREA NETWORK (WLAN)

METROPOLITAN AREA NETWORK (MAN)

WIDE AREA NETWORK (WAN)

STORAGE AREA NETWORK (SAN)

VIRTUAL PRIVATE NETWORK (VPN)

***What are the three main purposes of networking?**

The main purpose of computer networking is sharing. It allows us to share mainly three things; **data,** resources**, and applications**

***What is an IP Address – Definition and Explanation**

IP address definition

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

What do you mean by Internet? The Internet is a vast network that connects computers all over the world. Through the Internet, people can share information and communicate from anywhere with an Internet connection. What is the full name of Internet? Its **Interconnected Network**

***What is an IP?**

An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.

IP addresses are not random. They are mathematically produced and allocated by the Internet Assigned Numbers Authority (IANA), a division of the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a non-profit organization that was established in the United States in 1998 to help maintain the security of the internet and allow it to be usable by all. Each time anyone registers a domain on the internet, they go through a domain name registrar, who pays a small fee to ICANN to register the domain.

How do IP addresses work

If you want to understand why a particular device is not connecting in the way you would expect or you want to troubleshoot why your network may not be working, it helps understand how IP addresses work.

Internet Protocol works the same way as any other language, by communicating using set guidelines to pass information. All devices find, send, and exchange information with other connected devices using this protocol. By speaking the same language, any computer in any location can talk to one another.

The use of IP addresses typically happens behind the scenes. The process works like this:

Your device indirectly connects to the internet by connecting at first to a network connected to the internet, which then grants your device access to the internet.

When you are at home, that network will probably be your Internet Service Provider (ISP). At work, it will be your company network.

Your IP address is assigned to your device by your ISP.

Your internet activity goes through the ISP, and they route it back to you, using your IP address. Since they are giving you access to the internet, it is their role to assign an IP address to your device.

However, your IP address can change. For example, turning your modem or router on or off can change it. Or you can contact your ISP, and they can change it for you.

When you are out and about – for example, traveling – and you take your device with you, your home IP address does not come with you. This is because you will be using another network (Wi-Fi at a hotel, airport, or coffee shop, etc.) to access the internet and will be using a different (and temporary) IP address, assigned to you by the ISP of the hotel, airport or coffee shop.

As the process implies, there are different types of IP addresses, which we explore below.

Types of IP addresses

There are different categories of IP addresses, and within each category, different types.

Consumer IP addresses

Every individual or business with an internet service plan will have two types of IP addresses: their private IP addresses and their public IP address. The terms public and private relate to the network location — that is, a private IP address is used inside a network, while a public one is used outside a network.

Private IP addresses

Every device that connects to your internet network has a private IP address. This includes computers, smartphones, and tablets but also any Bluetooth-enabled devices like speakers, printers, or smart TVs. With the growing internet of things, the number of private IP addresses you have at home is probably growing. Your router needs a way to identify these items separately, and many items need a way to recognize each other. Therefore, your router generates private IP addresses that are unique identifiers for each device that differentiate them on the network.

Public IP addresses

A public IP address is the primary address associated with your whole network. While each connected device has its own IP address, they are also included within the main IP address for your network. As described above, your public IP address is provided to your router by your ISP. Typically, ISPs have a large pool of IP addresses that they distribute to their customers. Your public IP address is the address that all the devices outside your internet network will use to recognize your network.

Public IP addresses

Public IP addresses come in two forms – dynamic and static.

Dynamic IP addresses

Dynamic IP addresses change automatically and regularly. ISPs buy a large pool of IP addresses and assign them automatically to their customers. Periodically, they re-assign them and put the older IP addresses back into the pool to be used for other customers. The rationale for this approach is to generate cost savings for the ISP. Automating the regular movement of IP addresses means they don’t have to carry out specific actions to re-establish a customer's IP address if they move home, for example. There are security benefits, too, because a changing IP address makes it harder for criminals to hack into your network interface.

Static IP addresses

In contrast to dynamic IP addresses, static addresses remain consistent. Once the network assigns an IP address, it remains the same. Most individuals and businesses do not need a static IP address, but for businesses that plan to host their own server, it is crucial to have one. This is because a static IP address ensures that websites and email addresses tied to it will have a consistent IP address — vital if you want other devices to be able to find them consistently on the web.

This leads to the next point – which is the two types of website IP addresses.

There are two types of website IP addresses: For website owners who don't host their own server, and instead rely on a web hosting package – which is the case for most websites – there are two types of website IP addresses. These are shared and dedicated.

Shared IP addresses

Websites that rely on shared hosting plans from web hosting providers will typically be one of many websites hosted on the same server. This tends to be the case for individual websites or SME websites, where traffic volumes are manageable, and the sites themselves are limited in terms of the number of pages, etc. Websites hosted in this way will have shared IP addresses.

Dedicated IP addresses

Some web hosting plans have the option to purchase a dedicated IP address (or addresses). This can make obtaining an SSL certificate easier and allows you to run your own File Transfer Protocol (FTP) server. This makes it easier to share and transfer files with multiple people within an organization and allow anonymous FTP sharing options. A dedicated IP address also allows you to access your website using the IP address alone rather than the domain name — useful if you want to build and test it before registering your domain.

How to look up IP addresses

The simplest way to check your router's public IP address is to search "What is my IP address?" on Google. Google will show you the answer at the top of the page.

Other websites will show you the same information: they can see your public IP address because, by visiting the site, your router has made a request and therefore revealed the information. The site IPLocation goes further by showing the name of your ISP and your city.

Generally, you will only receive an approximation of location using this technique — where the provider is, but not the actual device location. If you are doing this, remember to log out of your VPN too. Obtaining the actual physical location address for the public IP address usually requires a search warrant to be submitted to the ISP.

Finding your private IP address varies by platform:

In Windows:

Use the command prompt.

Search for "cmd" (without the quotes) using Windows search

In the resulting pop-up box, type "ipconfig" (no quote marks) to find the information.

On a Mac:

Go to System Preferences

Select network – and the information should be visible.

On an iPhone:

Go to Settings

Select Wi-Fi and click the "i" in a circle () next to the network you are on – the IP address should be visible under the DHCP tab.

If you need to check the IP addresses of other devices on your network, go into the router. How you access the router depends on the brand and the software it uses. Generally, you should be able to type the router's gateway IP address into a web browser on the same network to access it. From there, you will need to navigate to something like "attached devices," which should display a list of all the devices currently or recently attached to the network — including their IP addresses.

IP address security threats

Cybercriminals can use various techniques to obtain your IP address. Two of the most common are social engineering and online stalking.

Attackers can use social engineering to deceive you into revealing your IP address. For example, they can find you through Skype or a similar instant messaging application, which uses IP addresses to communicate. If you chat with strangers using these apps, it is important to note that they can see your IP address. Attackers can use a Skype Resolver tool, where they can find your IP address from your username.

Online stalking

Criminals can track down your IP address by merely stalking your online activity. Any number of online activities can reveal your IP address, from playing video games to commenting on websites and forums.

Once they have your IP address, attackers can go to an IP address tracking website, such as whatismyipaddress.com, type it in, and then get an idea of your location. They can then cross-reference other open-source data if they want to validate whether the IP address is associated with you specifically. They can then use LinkedIn, Facebook, or other social networks that show where you live, and then see if that matches the area given.

If a Facebook stalker uses a phishing attack against people with your name to install spying malware, the IP address associated with your system would likely confirm your identity to the stalker.

If cybercriminals know your IP address, they can launch attacks against you or even impersonate you. It is important to be aware of the risks and how to mitigate them. Risks include:

Downloading illegal content using your IP address

Hackers are known to use hacked IP addresses to download illegal content and anything else they do not want to be traced back to them. For example, using the identity of your IP address, criminals could download pirated movies, music, and video – which would breach your ISP's terms of use – and much more seriously, content related to terrorism or child pornography. This could mean that you – through no fault of your own – could attract the attention of law enforcement.

Tracking down your location

If they know your IP address, hackers can use geolocation technology to identify your region, city, and state. They only need to do a little more digging on social media to identify your home and potentially burgle it when they know you are away.

Directly attacking your network

Criminals can directly target your network and launch a variety of assaults. One of the most popular is a DDoS attack (distributed denial-of-service). This type of cyberattack occurs when hackers use previously infected machines to generate a high volume of requests to flood the targeted system or

server. This creates too much traffic for the server to handle, resulting in a disruption of services. Essentially, it shuts down your internet. While this attack is typically launched against businesses and video game services, it can occur against an individual, though this is much less common. Online gamers are at particularly high risk for this, as their screen is visible while streaming (on which an IP address can be discovered).

Hacking into your device

The internet uses ports as well as your IP address to connect. There are thousands of ports for every IP address, and a hacker who knows your IP can try those ports to attempt to force a connection. For example, they could take over your phone and steal your information. If a criminal does obtain access to your device, they could install malware on it.

How to protect and hide your IP address

Hiding your IP address is a way to protect your personal information and online identity. The two primary ways to hide your IP address are:

Using a proxy server

Using a virtual private network (VPN)

A proxy server is an intermediary server through which your traffic is routed:

The internet servers you visit see only the IP address of that proxy server and not your IP address.

When those servers send information back to you, it goes to the proxy server, which then routes it to you.

A drawback of proxy servers is that some of the services can spy on you — so you need to trust it. Depending on which one you use, they can also insert ads into your browser.

VPN offers a better solution:

When you connect your computer – or smartphone or tablet – to a VPN, the device acts as if it is on the same local network as the VPN.

All your network traffic is sent over a secure connection to the VPN.

Because your computer behaves as if it is on the network, you can securely access local network resources even when you are in another country.

You can also use the internet as if you were present at the VPN's location, which has benefits if you are using public Wi-Fi or want to access geo-blocked websites.

Kaspersky Secure Connection or any VPN is a VPN that protects you on public Wi-Fi, keeps your communications private, and ensures that you are not exposed to phishing, malware, viruses, and other cyber threats.

When should you use VPN

Using a VPN hides your IP address and redirects your traffic through a separate server, making it much safer for you online. Situations where you might use a VPN include:

When using public Wi-Fi

When using a public Wi-Fi network, even one that is password-protected, a VPN is advisable. If a hacker is on the same Wi-Fi network, it is easy for them to snoop on your data. The basic security that the average public Wi-Fi network employs does not provide robust protection from other users on the same network.

Using a VPN will add an extra layer of security to your data, ensuring you bypass the public Wi-Fi's ISP and encrypting all your communication.

When you are traveling

If you are traveling to a foreign country – for example, China, where sites like Facebook are blocked – a VPN can help you access services that may not be available in that country.

The VPN will often allow you to use streaming services that you paid for and have access to in your home country, but they are not available in another because of international rights issues. Using a VPN can enable you to use the service as if you were at home. Travelers may also be able to find cheaper airfare when using a VPN, as prices can vary from region to region.

When you are working remotely

This is especially relevant in the post-COVID world, where many people are working remotely. Often employers require the use of a VPN to access company services remotely for security reasons. A VPN that connects to your office's server can give you access to internal company networks and resources when you are not in the office. It can do the same for your home network while you are out and about.

When you just want some privacy

Even in the comfort of your own home, using the internet for everyday purposes, using a VPN can be a good idea. Whenever you access a website, the server you connect to logs your IP address and attaches it to all the other data the site can learn about you: your browsing habits, what you click on,

how long you spend looking at a particular page. They can sell this data to advertising companies who use it to tailor ads straight to you. This is why ads on the internet sometimes feel oddly personal: it's because they are. Your IP address can also be used to track your location, even when your location services are turned off. Using a VPN prevents you from leaving footprints on the web.

Don't forget your mobile devices, either. They have IP addresses too, and you probably use them in a wider variety of locations than your home computer, including public Wi-Fi hotspots. It is advisable to use a VPN on your mobile when connecting to a network you may not fully trust.

Other ways to protect your privacy

Change privacy settings on instant messaging applications

Apps installed on your device are a major source of IP address hacking. Instant messaging and other calling apps can be used as a tool by cybercriminals. Using IM apps only allows direct connections from contacts and doesn't accept calls or messages from people you don't know. Changing your privacy settings makes it harder to find your IP address because people who don't know you cannot connect with you.

Create unique passwords

Your device password is the only barrier that can restrict people from accessing your device. Some people prefer to stick to their devices' default passwords, which makes them vulnerable to attack. Like all your accounts, your device needs to have a unique and strong password that is not easy to decode. A strong password contains a mix of upper- and lower-case letters, numerals, and characters. This will help to safeguard your device against IP address hacking.

Stay alert to phishing emails and malicious content

A high proportion of malware and device tracking software is installed via phishing emails. When you connect with any site, this provides the site with access to your IP address and device location, making it vulnerable to hacking. Be vigilant when opening emails from unknown senders and avoid clicking on links that could send you to unauthorized sites. Pay close attention to the emails' content, even if they appear to come from well-known sites and legitimate businesses.

Use a good antivirus solution and keep it up to date

Install comprehensive antivirus software and keep it up to date. For example, Kaspersky's Anti-Virus protection guards you from viruses on your PC and Android devices, secures and stores your passwords and private documents, and encrypts the data you send and receive online with VPN.

Protecting your IP address is a crucial aspect of protecting your online identity. Securing it through these steps is a way to stay safe against the wide variety of cybercriminals' attacks.

***IPV4:** What is IPv4?

IPv4 stands for Internet Protocol version 4. It is the underlying technology that makes it possible for us to connect our devices to the web. Whenever a device accesses the Internet, it is assigned a unique, numerical IP address such as 99.48.227.227. To send data from one computer to another through the web, a data packet must be transferred across the network containing the IP addresses of both devices.

***What is IPv6?**

IPv6 is the next generation Internet Protocol (IP) address standard intended to supplement and eventually replace IPv4, the protocol many Internet services still use today. Every computer, mobile phone, home automation component, IoT sensor and any other device connected to the Internet needs a numerical IP address to communicate between other devices. The original IP address scheme, called IPv4, is running out of addresses due to its widespread usage from the proliferation of so many connected devices.

Why Support IPv6? What are the benefits of IPv6?

IPv6 (Internet Protocol version 6) is the sixth revision to the Internet Protocol and the successor to IPv4. It functions similarly to IPv4 in that it provides the unique IP addresses necessary for Internet-enabled devices to communicate. However, it does have one significant difference: it utilizes a 128-bit IP address.

Key benefits to IPv6 include:

No more NAT (Network Address Translation)

Auto-configuration

No more private address collisions

Better multicast routing

Simpler header format

Simplified, more efficient routing

True quality of service (QoS), also called "flow labeling"

Built-in authentication and privacy support

Flexible options and extensions

Easier administration (no more DHCP)

IPv4 uses a 32-bit address for its Internet addresses. That means it can provide support for 2^32 IP addresses in total â€” around 4.29 billion. That may seem like a lot, but all 4.29 billion IP addresses have now been assigned, leading to the address shortage issues we face today.

IPv6 utilizes 128-bit Internet addresses. Therefore, it can support 2^128 Internet addresses—340,282,366,920,938,463,463,374,607,431,768,211,456 of them to be exact. The number of IPv6 addresses is 1028 times larger than the number of IPv4 addresses. So there are more than enough IPv6 addresses to allow for Internet devices to expand for a very long time.

The text form of the IPv6 address is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where each x is a hexadecimal digit, representing 4 bits. Leading zeros can be omitted. The double colon (::) can be used once in the text form of an address, to designate any number of 0 bits.

With Dual-IP stacks, your computers, routers, switches, and other devices run both protocols, but IPv6 is the preferred protocol. A typical procedure for businesses is to start by enabling both TCP/IP

protocol stacks on the wide area network (WAN) core routers, then perimeter routers and firewalls, followed by data-center routers and finally the desktop access routers.

***What is a Domain Name and How Does DNS work?**

The Domain Name System (DNS) is the Internet's system for mapping alphabetic names to numeric Internet Protocol (IP) addresses like a phone book maps a person's name to a phone number. For example, when a Web address (URL) is typed into a browser, a DNS query is made to learn an IP address of a Web server associated with that name.

Using the www.example.com URL, example.com is the domain name, and www is the hostname. DNS resolution maps www.example.com into an IP address (such as 192.0.2.1). When a user needs to load a webpage, a conversion must occur between what a user types into their web browser (www.example.com) into an IP address required to locate the www.example.com site.

The DNS system is an open worldwide network of database name servers that include 13 authoritative name servers that serve the DNS root zone level, known as "root servers". A root server (also called a DNS root nameserver) receives a DNS query that includes a domain name (e.g. www.thousandeyes.com), and responds by directing that request to a top-level domain (TLD) nameserver, based on the TLD of that domain such as .com, .net, and .org. It directly responds to requests for DNS records in the root zone by returning an appropriate list of the authoritative TLD name servers for the appropriate TLD that can resolve the initial DNS lookup request for an IP address of that domain name.

***What is an ISP? Internet Service Provider**

An Internet Service Provider (ISP) is a company that provides transport of Internet traffic on behalf of other ISPs, businesses or other non-ISP organizations, and individuals. ISPs are classified into a 3-tier model that categorizes them depending on the type of Internet services they provide.

A Tier 1 ISP is an Internet provider that only exchanges Internet traffic with other Tier 1 providers on a non-commercial basis. These Tier 1 ISP exchanges of traffic are known as settlement-free peerings.

Tier 1 Internet service providers are the networks that provide the backbone of the Internet. They are referred to as backbone Internet providers. These providers build infrastructure such as the Atlantic Internet sea cables. They provide traffic to all other Internet providers, not end users.

A Tier 2 ISP is a service provider that utilizes a combination of paid transit and peering to deliver traffic to the Internet. Tier 2 ISPs are typically regional or national providers.

A Tier 3 ISP is a provider that strictly purchases Internet transit. A Tier 3 provider is by definition primarily engaged in delivering Internet connections to end customers.

***What is a subnet?**

A subnet, or subnetwork, is a segmented piece of a larger network. More specifically, subnets are a logical partition of an IP network into multiple, smaller network segments. The Internet Protocol (IP)

is the method for sending data from one computer to another over the internet. Each computer, or host, on the internet has at least one IP address as a unique identifier.

Organizations will use a subnet to subdivide large networks into smaller, more efficient subnetworks. One goal of a subnet is to split a large network into a grouping of smaller, interconnected networks to help minimize traffic. This way, traffic doesn't have to flow through unnecessary routs, increasing network speeds.

Subnetting, the segmentation of a network address space, improves address allocation efficiency. It is described in the formal document, Request for Comments 950, and is tightly linked to IP addresses, subnet masks and Classless Inter-Domain Routing (CIDR) notation.

How do subnets work?

Each subnet allows its connected devices to communicate with each other, while routers are used to communicate between subnets. The size of a subnet depends on the connectivity requirements and the network technology employed. A point-to-point subnet allows two devices to connect, while a data center subnet might be designed to connect many more devices.

Each organization is responsible for determining the number and size of the subnets it creates, within the limits of the address space available for its use. Additionally, the details of subnet segmentation within an organization remain local to that organization.

An IP address is divided into two fields: a Network Prefix (also called the Network ID) and a Host ID. What separates the Network Prefix and the Host ID depends on whether the address is a Class A, B or C address. Figure 1 shows an IPv4 Class B address, 172.16.37.5. Its Network Prefix is 172.16.0.0, and the Host ID is 37.5.

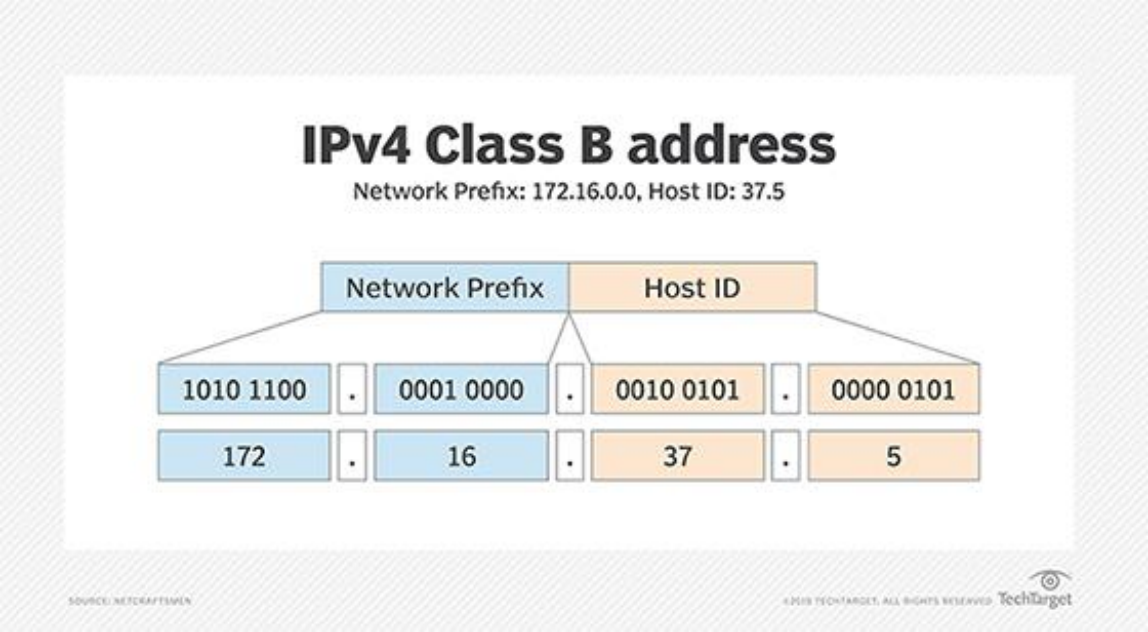


Figure 1. Class B IP address

The subnet mechanism uses a portion of the Host ID field to identify individual subnets. Figure 2, for example, shows the third group of the 172.16.0.0 network being used as a Subnet ID. A subnet mask

is used to identify the part of the address that should be used as the Subnet ID. The subnet mask is applied to the full network address using a binary AND operation. AND operations operate, assuming an output is "true" only when both inputs are "true." Otherwise, the output is "false." Only when two bits are both 1. This results in the Subnet ID.

Figure 2 shows the AND of the IP address, as well as the mask producing the Subnet ID. Any remaining address bits identify the Host ID. The subnet in Figure 2 is identified as 172.16.2.0, and the Host ID is 5. In practice, network staff will typically refer to a subnet by just the Subnet ID. It would be common to hear someone say, "Subnet 2 is having a problem today," or, "There is a problem with the dot-two subnet."

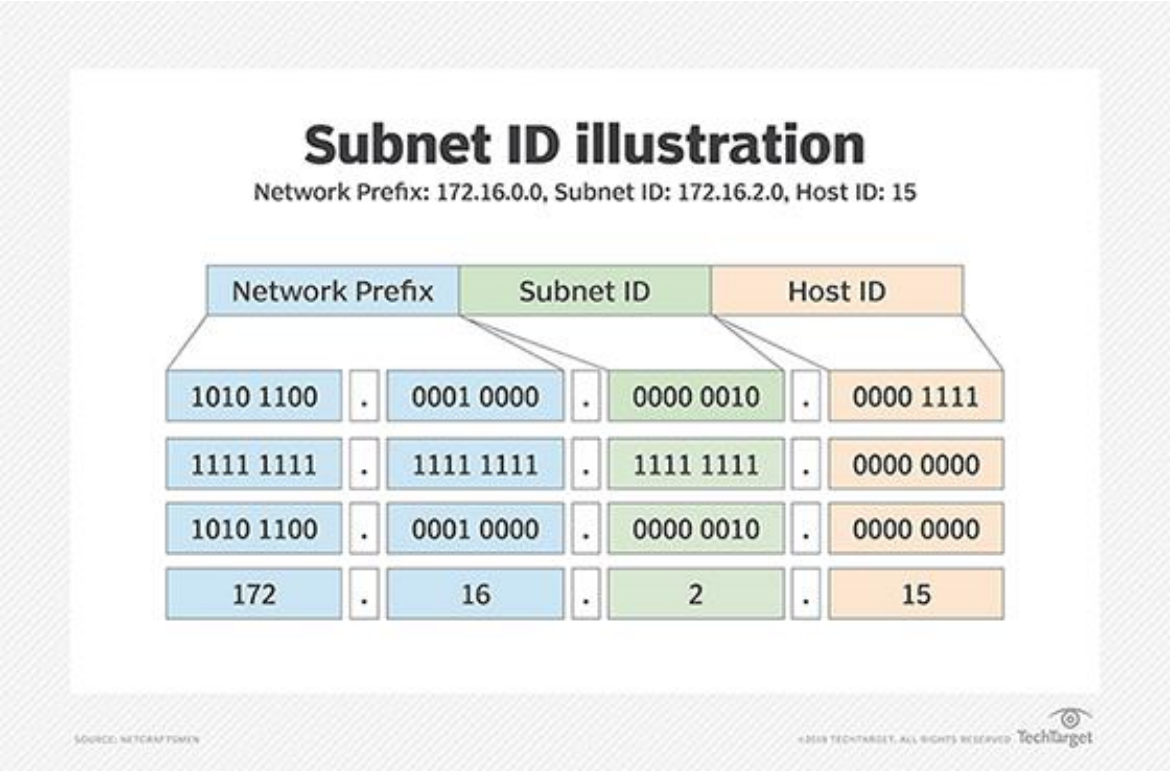


Figure 2. Subnet ID

The Subnet ID is used by routers to determine the best route between subnetworks. Figure 3 shows the 172.16.0.0 network, with the third grouping as the Subnet ID. Four of the 256 possible subnets are shown connected to one router. Each subnet is identified either by its Subnet ID or the subnet address with the Host ID set to .0. The router interfaces are assigned the Host ID of .1 -- e.g., 172.16.2.1.

When the router receives a packet addressed to a host on a different subnet than the sender -- host A to host C, for example -- it knows the subnet mask and uses it to determine the Subnet ID of host C. It examines its routing table to find the interface connected to host C's subnet and forwards the packet on that interface.

Subnet segmentation

A subnet itself also may be segmented into smaller subnets, giving organizations the flexibility to create smaller subnets for things like point-to-point links or for subnetworks that support a few devices.

The example below uses an 8-bit Subnet ID. The number of bits in the subnet mask depends on the organization's requirements for subnet size and the number of subnets. Other subnet mask lengths are common. While this adds some complexity to network addressing, it significantly improves the efficiency of network address utilization.

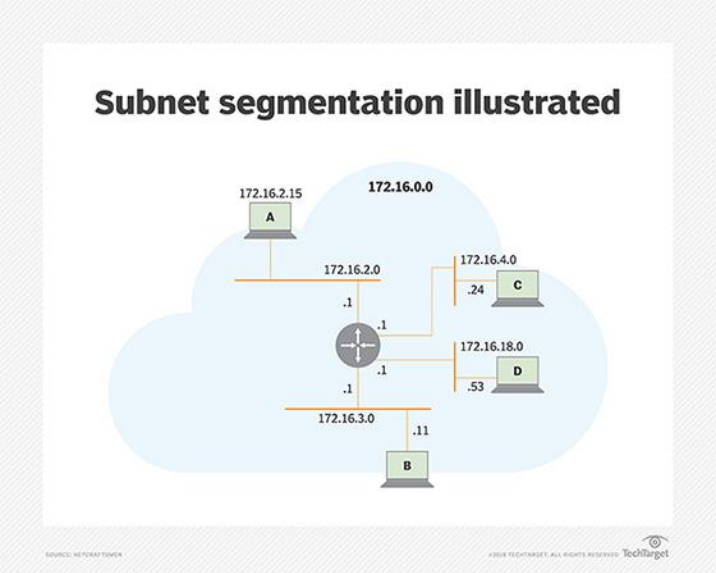


Figure 3. Subnet segmentation

A subnet can be delegated to a suborganization, which itself may apply the subnetting process to create additional subnets, as long as sufficient address space is available. Subnetting performed by a delegated organization is hidden from other organizations. As a result, the Subnet ID field length and where subnets are assigned can be hidden from the parent (delegating) organization, a key characteristic that allows networks to be scaled up to large sizes.

In modern routing architectures, routing protocols distribute the subnet mask with routes and provide mechanisms to summarize groups of subnets as a single routing table entry. Older routing architectures relied on the default Class A, B and C IP address classification to determine the mask to use.

CIDR notation is used to identify Network Prefix and Mask, where the subnet mask is a number that indicates the number of ones in the Mask (e.g., 172.16.2.0/24). This is also known as Variable-Length Subnet Masking (VLSM) and CIDR. Subnets and subnetting are used in both IPv4 and IPv6 networks, based on the same principles.

What are subnets used for?

Reallocating IP addresses. Each class has a limited number of host allocations; for example, networks with more than 254 devices need a Class B allocation. If a network administrator is working with a Class B or C network and needs to allocate 150 hosts for three physical networks located in three different cities, they would need to either request more address blocks for each network -- or divide a network into subnets that enable administrators to use one block of addresses on multiple physical networks.

Relieving network congestion. If much of an organization's traffic is meant to be shared regularly between the same cluster of computers, placing them on the same subnet can reduce network traffic. Without a subnet, all computers and servers on the network would see data packets from every other computer.

Improving network security. Subnetting allows network administrators to reduce network-wide threats by quarantining compromised sections of the network and by making it more difficult for trespassers to move around an organization's network.

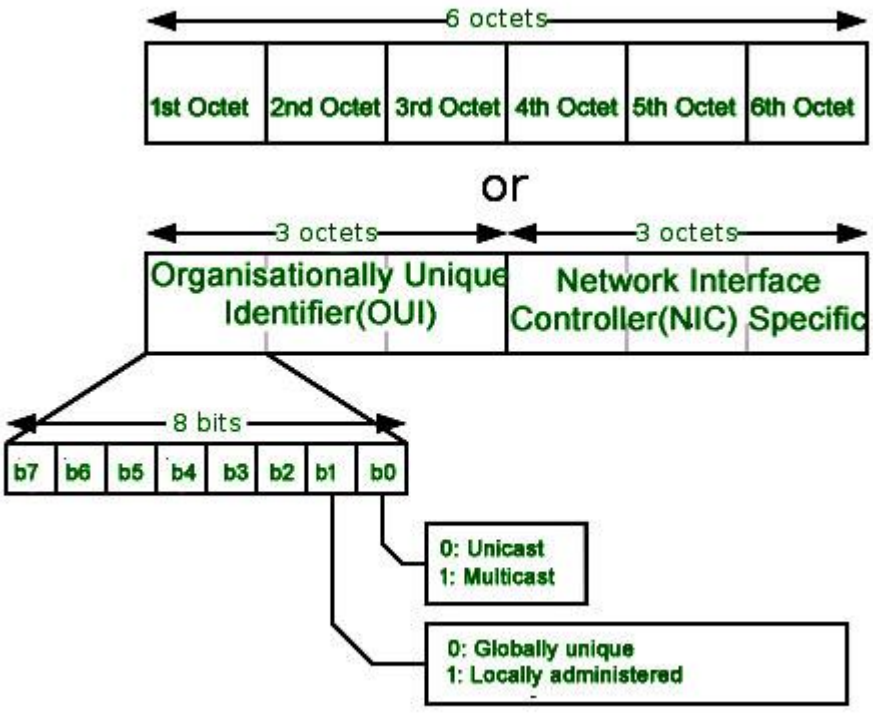
***Media Access Control (MAC) Address –**

MAC Addresses are unique 48-bits hardware number of a computer, which is embedded into network card (known as Network Interface Card) during the time of manufacturing. MAC Address is also known as Physical Address of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers –

Logical Link Control(LLC) Sublayer

Media Access Control(MAC) Sublayer

MAC address is used by Media Access Control (MAC) sublayer of Data-Link Layer. MAC Address is worldwide unique, since millions of network devices exists and we need to uniquely identify each.



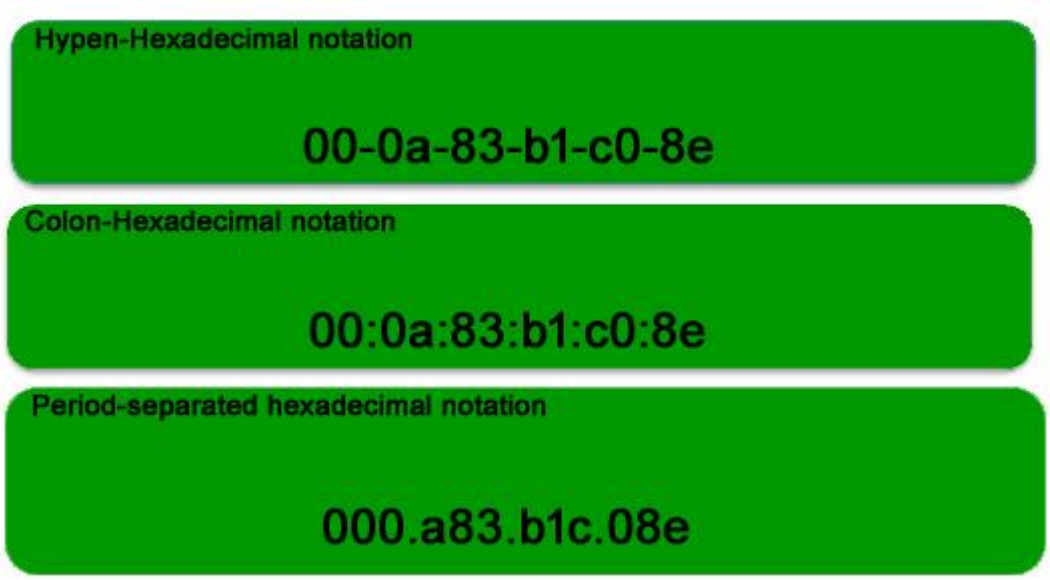
Format of MAC Address –

MAC Address is a 12-digit hexadecimal number (6-Byte binary number), which is mostly represented by Colon-Hexadecimal notation. First 6-digits (say 00:40:96) of MAC Address identifies the manufacturer, called as OUI (Organizational Unique Identifier). IEEE Registration Authority Committee assign these MAC prefixes to its registered vendors.

Here are some OUI of well known manufacturers :

The rightmost six digits represents Network Interface Controller, which is assigned by manufacturer.

As discussed above, MAC address is represented by Colon-Hexadecimal notation. But this is just a conversion, not mandatory. MAC address can be represented using any of the following formats –



Note: Colon-Hexadecimal notation is used by Linux OS and Period-separated Hexadecimal notation is used by Cisco Systems.

How to find MAC address –

Command for UNIX/Linux - ifconfig -a

ip link list

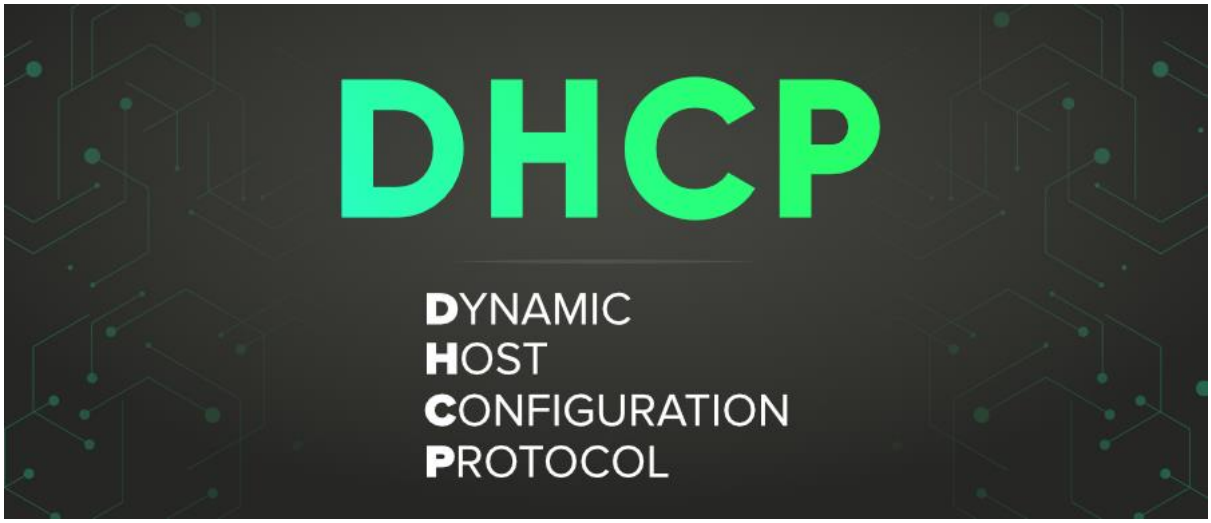
ip address show

Command for Windows OS - ipconfig /all

MacOS - TCP/IP Control Panel

Note – LAN technologies like Token Ring, Ethernet use MAC Address as their Physical address but there are some networks (AppleTalk) which does not use MAC address.

***DHCP** stands for Dynamic Host Configuration Protocol. It is the critical feature on which the users of an enterprise network communicate. DHCP helps the enterprises to smoothly manage the allocation of IP addresses to the end-user clients' devices such as desktops, laptops, cellphones, etc.



History

DHCP was used for the first time in 1993. It was built on the Bootstrap Protocol (BOOTP) of 1985. The definition of the Dynamic Host Configuration Protocol is in RFC 2131 and can be found under the UDP port numbers 67 and 68.

Basic Functioning

Upon dynamically configuring a device with dynamic IP from a DHCP server, three things come into play, the IP address (of course), subnet mask and the default gateway.
Configuring a DHCP server to hand out IP addresses on a subnet is known as a DHCP pool. This pool of addresses is usually a range of consecutive numbers within a single IP subnet. If any of the addresses within the range needs to be blocked, it can be done by the administrator. The subnet mask tells devices how large the subnetwork is that they are connected to; this is critical from a broadcast perspective. Finally, the default gateway is the IP address that signifies the exit point of the subnetwork to which the device belongs.

Characteristics

Centralized and automated TCP/IP configuration.

The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable devices that move to different locations on a wireless network.

The forwarding of initial DHCP messages by using a DHCP relay agent, which eliminates the need for a DHCP server on every subnet.

The ability to define TCP/IP configurations from a central location.

DHCP Lease Time

In most cases, DHCP will work with default settings that largely are the same from server to server. However, different DHCP servers assign IP addresses for different periods of time before which it is altered with a fresh IP address on a particular end-device. In majority cases, the DHCP lease time is 14 days. However, with the growing number of users and mobile environments, the enterprises have found that their pool of available addresses can run out quickly.
To solve this, DHCP lease times can be reduced to stay with a specific device for a few hours or less. The process of determining optimal DHCP lease times depends on the type of users, the size of the DHCP subnets, and how much load the DHCP server can handle.

DHCP Relay Agent

A DHCP relay agent is a way for the network to listen to DHCP server discovery broadcast messages from client devices, convert broadcast requests into a unicast packet, and forward requests onto the DHCP server that's in a different part of the network. This centralizes the management of IP addresses on the network.

Advantages

Easy use and configuration, as the network parameters have to be entered only once.

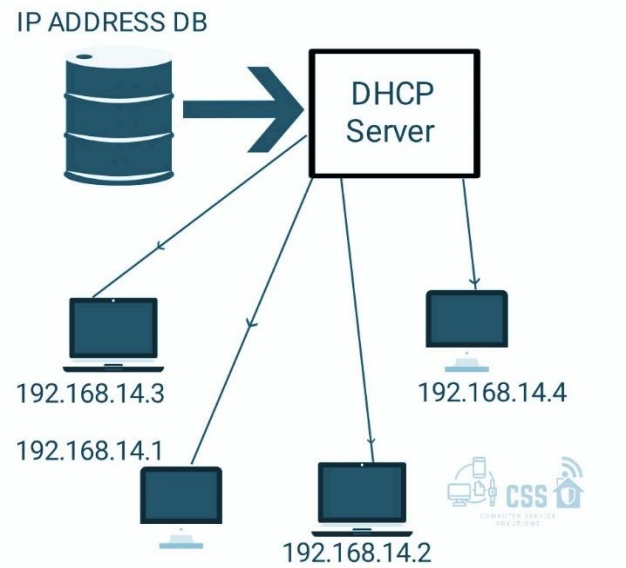
Furthermore, the existing IP addresses can be used optimally.

Because of the frequently changed locations, it is almost impossible that mobile devices configure themselves constantly. Here, the automatic DHCP system offers the advantage of uncomplicated and simple applicability.

Disadvantages

The problem with DHCP is that clients accept any server. Accordingly, when another server is in the vicinity, the client may connect with this server, and this server may possibly send invalid data to the client.

Security of MAC address is also not provided.



***Types of Computer Networks Explained**

Technology made a huge breakthrough in 1936 when the first computer was invented. However, it wasn't until years later in 1969 that the first-ever computer-to-computer link was established. This development was what ultimately paved the way for the Internet-driven world we live in today.

So, what is a network? It's the connection of two or more computers that are linked in order to share files, resources, and allow communication. The type of network depends on the number of devices, as well as the location and distance between each.

Do you know what network your home or business utilizes? If not, find out by checking out 7 different types of commonly utilized networks in the list below.

1. **PERSONAL AREA NETWORK (PAN)**

This is the smallest and most basic network that you'll find. It's meant to cover a very small area (typically a single room or building). A PAN is most commonly used for one individual and to connect just a handful of devices such as a computer, smart phone, and printer. Probably the most well-known PAN technology is Bluetooth connection. So, next time you connect your phone to your car to play music, you can thank your Personal Area Network!

2. **LOCAL AREA NETWORK (LAN)**

This is an extremely common and well-known type of network. Just as the name suggests, a LAN connects a group of computers or devices together across a local area. This type of network can be utilized to connect devices throughout one building or even 2-3 buildings depending on the proximity to each other. Whether your office location utilizes wired or wireless connection, it's almost surely using a LAN connection. This brings us to the next type of network…

3. **WIRELESS LOCAL AREA NETWORK (WLAN)**

A WLAN is simply a LAN that does not rely on cables to connect to the network. So, when you're using WiFi, you're using a WLAN. WLANs are typically used in the same scenario as LANs, it just depends on whether you'd prefer an on premises or remote cloud solution (wires or wireless).

4. METROPOLITAN AREA NETWORK (MAN)

Larger than a LAN but smaller than a WAN, a MAN incorporates elements of both types of networks. It connects multiple LANs together and spans an entire geographical area such as a city or town (or sometimes a campus). Ownership and management can be handled by a single person, but it's more likely done by a larger company or organization.

5. **WIDE AREA NETWORK (WAN)**

Like LANs, you very well may recognize the term "WAN." WANs do the same thing as LANs but across a larger area while connecting more devices. Even when miles apart, a WAN can connect devices together remotely. In fact, the most basic example of a WAN is the Internet which connects

computers and devices worldwide. Since it's much larger, this type of network is typically maintained by multiple administrators and ownership is distributed across various organizations.

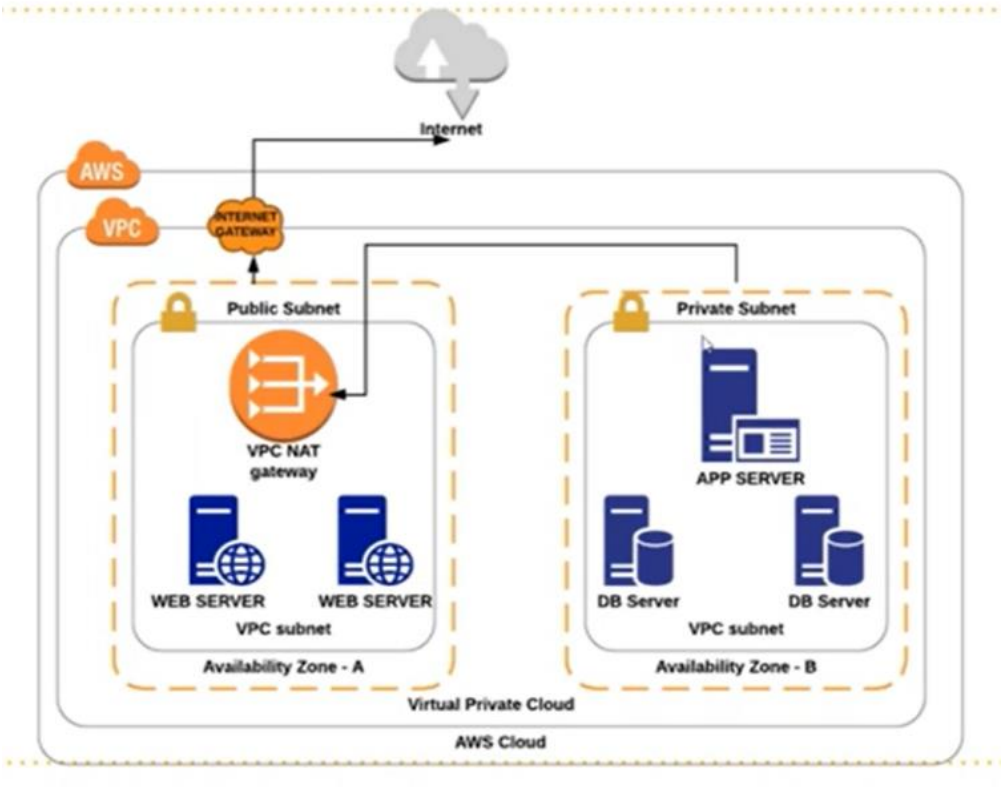
6. **STORAGE AREA NETWORK (SAN)**

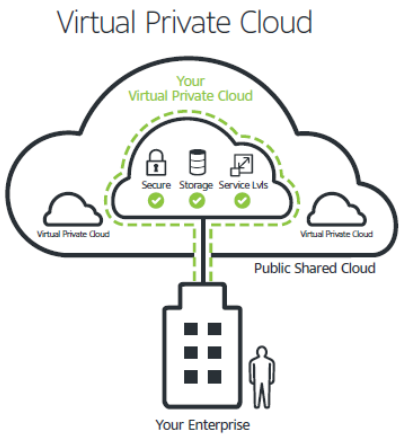
A SAN is another type of LAN that's designed to handle large data transfers and storage. This purpose of this network is to move larger, more complex storage resources away from the network into a separate, high-performance atmosphere. Doing this not only allows for easy retrieval and storage of the data but it also frees up space and improves overall performance of the original network.

7. **VIRTUAL PRIVATE NETWORK (VPN)**

The point of a VPN is to increase security and privacy while accessing a network. The VPN acts as a middleman between you and the network by encrypting your data and hiding your identity. This is a great option for sending and receiving sensitive information, however, using a VPN is ideal anytime you connect to the Internet. Anytime you're on a public network, you run the risk of being targeted by a hacker, so using a VPN is you best bet at ensuring your cybersecurity.

At Sierra Experts, we provide various networking services from planning and design to implementing and monitoring. After all, at the core of any successful business is a computer network that's running at peak performance. Even if you think you have a high-functioning, reliable network, it couldn't hurt to have us check it out. We provide services such as network mapping and penetration testing which can help provide insight on how your network is functioning and what can be improved.

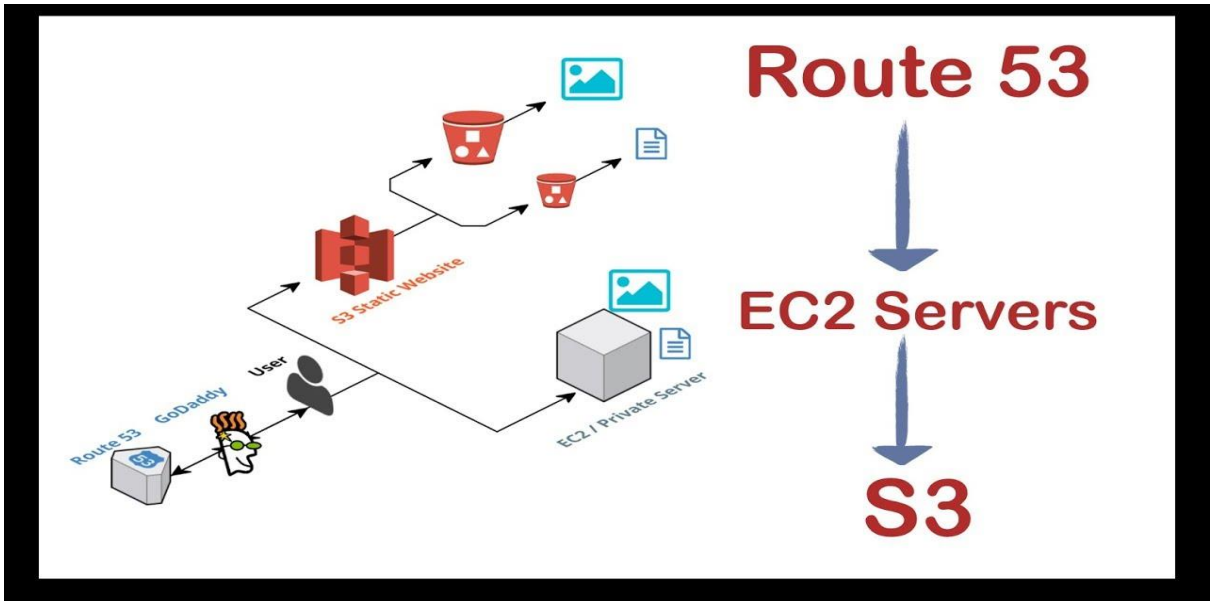




***Amazon Route 53** is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost effective way to route end users to Internet applications by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other. Amazon Route 53 is fully compliant with IPv6 as well.

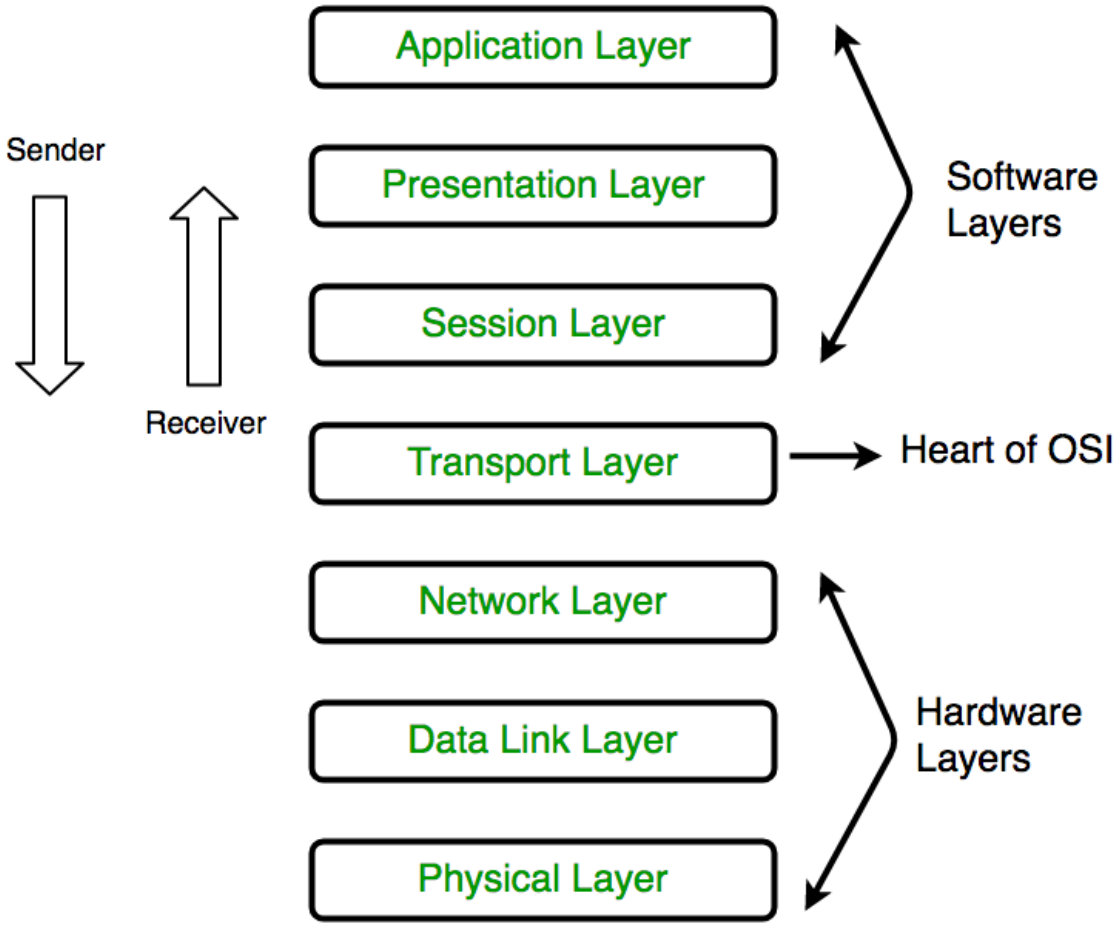
Amazon Route 53 effectively connects user requests to infrastructure running in AWS – such as Amazon EC2 instances, Elastic Load Balancing load balancers, or Amazon S3 buckets – and can also be used to route users to infrastructure outside of AWS. You can use Amazon Route 53 to configure DNS health checks, then continuously monitor your applications' ability to recover from failures and control application recovery with Route 53 Application Recovery Controller.

Amazon Route 53 Traffic Flow makes it easy for you to manage traffic globally through a variety of routing types, including Latency Based Routing, Geo DNS, Geoproximity, and Weighted Round Robin—all of which can be combined with DNS Failover in order to enable a variety of low-latency, fault-tolerant architectures. Using Amazon Route 53 Traffic Flow's simple visual editor, you can easily manage how your end-users are routed to your application's endpoints—whether in a single AWS region or distributed around the globe. Amazon Route 53 also offers Domain Name Registration – you can purchase and manage domain names such as example.com and Amazon Route 53 will automatically configure DNS settings for your domains.


S3 Static Website
User
Route 53
GoDaddy
EC2 / Private Server
Route 53
EC2 Servers
S3

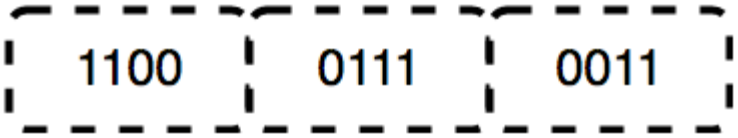
***Layers of OSI Model**

OSI stands for Open Systems Interconnection. It has been developed by ISO – 'International Organization for Standardization, in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



1. Physical Layer (Layer 1) :

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



The functions of the physical layer are :

Bit synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.

Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.

Transmission mode: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

* Hub, Repeater, Modem, Cables are Physical Layer devices.
** Network Layer, Data Link Layer, and Physical Layer are also known as Lower Layers or Hardware Layers.

2. Data Link Layer (DLL) (Layer 2) :

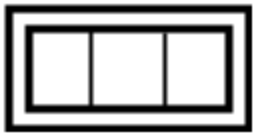
The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.
Data Link Layer is divided into two sublayers:

Logical Link Control (LLC)

Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.



The functions of the Data Link layer are :

Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

Physical addressing: After creating frames, the Data link layer adds physical addresses (MAC address) of the sender and/or receiver in the header of each frame.

Error control: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

Flow Control: The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving acknowledgement.

Access control: When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

* Packet in Data Link layer is referred to as Frame.
** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.
*** Switch & Bridge are Data Link Layer devices.

3. Network Layer (Layer 3) :

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.
The functions of the Network layer are :

Routing: The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.

Logical Addressing: In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

* Segment in Network layer is referred to as Packet.

** Network layer is implemented by networking devices such as routers.

4. Transport Layer (Layer 4) :

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.
• At sender's side:

Transport layer receives the formatted data from the upper layers, performs Segmentation, and also implements Flow & Error control to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.
Note: The sender needs to know the port number associated with the receiver's application. Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.
• At receiver's side:
Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are :

Segmentation and Reassembly: This layer accepts the message from the (session) layer, breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.

Service Point Addressing: In order to deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

Connection-Oriented Service: It is a three-phase process that includes
– Connection Establishment
– Data Transfer
– Termination / disconnection
In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

Connectionless service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

* Data in the Transport Layer is called as Segments.
** Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.
Transport Layer is called as Heart of OSI model.

5. Session Layer (Layer 5) :

This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.
The functions of the session layer are :

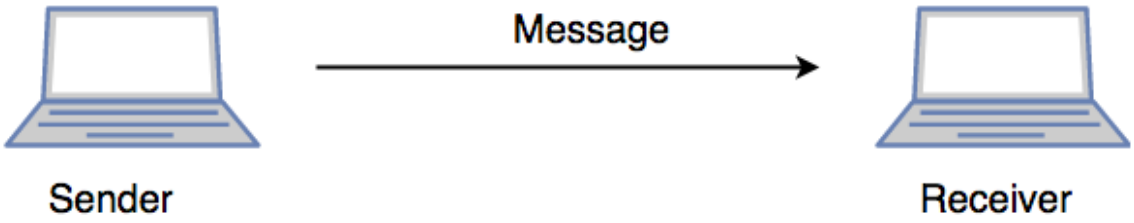
Session establishment, maintenance, and termination: The layer allows the two processes to establish, use and terminate a connection.

Synchronization: This layer allows a process to add checkpoints which are considered synchronization points into the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.

Dialog Controller: The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

**All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as “Application Layer”.
**Implementation of these 3 layers is done by the network application itself. These are also known as Upper Layers or Software Layers.

SCENARIO:
Let’s consider a scenario where a user wants to send a message through some Messenger application running in his browser. The “Messenger” here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0’s and 1’s) so that it can be transmitted.



6. Presentation Layer (Layer 6) :

The presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
The functions of the presentation layer are :

Translation: For example, ASCII to EBCDIC.

Encryption/ Decryption: Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

Compression: Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
Ex: Application – Browsers, Skype Messenger, etc.
**Application Layer is also called Desktop Layer.

The functions of the Application layer are :

Network Virtual Terminal

FTAM-File transfer access and management

Mail Services

Directory Services

OSI model acts as a reference model and is not implemented on the Internet because of its late invention. The current model being used is the TCP/IP model.

***TCP/IP Protocol**

The OSI Model we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

Process/Application Layer

Host-to-Host/Transport Layer

Internet Layer

Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :

TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer

OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Difference between TCP/IP and OSI Model:

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.
Transport layer in TCP/IP does not provide assurance delivery of packets.	In OSI model, transport layer provides assurance delivery of packets.
TCP/IP model network layer only provides connection less services.	Connection less and connection oriented both services are provided by network layer in OSI model.
Protocols cannot be replaced easily in TCP/IP model.	While in OSI model, Protocols are better covered and is easy to replace with the change in technology.

The first layer is the Process layer on the behalf of the sender and Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer –

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

IP – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:

IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.

ICMP – stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.

ARP – stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host Layer –

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

Transmission Control Protocol (TCP) – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.

User Datagram Protocol (UDP) – On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Application Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: **HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD.** Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

HTTP and HTTPS – HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.

SSH – SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.

NTP – NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

*__Application Layer Protocols used in cloud server and client:-__

The application layer is present at the top of the OSI model. It is the layer through which users interact. It provides services to the user.

Application Layer protocol:-

1. TELNET:

Telnet stands for the TELetype NETwork. It helps in terminal emulation. It allows Telnet clients to access the resources of the Telnet server. It is used for managing files on the internet. It is used for the initial setup of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. Port number of telnet is 23.

Command

telnet [\\RemoteServer]

\\RemoteServer : Specifies the name of the server to which you want to connect

2. FTP:

FTP stands for file transfer protocol. It is the protocol that actually lets us transfer files. It can facilitate this between any two machines using it. But FTP is not just a protocol but it is also a program.FTP promotes sharing of files via remote computers with reliable and efficient data transfer. The Port number for FTP is 20 for data and 21 for control.

Command

ftp machinename

3. TFTP:

The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it. It's a technology for transferring files between network devices and is a simplified version of FTP. The Port number for TFTP is 69.

Command

tftp [options...] [host [port]] [-c command]

4. NFS:

It stands for a network file system. It allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. This enables system administrators to consolidate resources onto centralized servers on the network. The Port number for NFS is 2049.

Command

service nfs start

5. SMTP:

It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol. Using a process called “store and forward,” SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. The Port number for SMTP is 25.

Command

MAIL FROM:<mail@abc.com?

6. LPD:

It stands for Line Printer Daemon. It is designed for printer sharing. It is the part that receives and processes the request. A “daemon” is a server or agent. The Port number for LPD is 515.

Command

lpd [-d] [-l] [-D DebugOutputFile]

7. X window:

It defines a protocol for the writing of graphical user interface–based client/server applications. The idea is to allow a program, called a client, to run on one computer. It is primarily used in networks of interconnected mainframes. Port number for X window starts from 6000 and increases by 1 for each server.

Command

Run xdm in runlevel 5

8. SNMP:

It stands for Simple Network Management Protocol. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. It is a way that servers can share information about their current state, and also a channel through which an administrate can modify pre-defined values. The Port number of SNMP is 161(TCP) and 162(UDP).

Command

snmpget -mALL -v1 -cpublic snmp_agent_Ip_address sysName.0

9. DNS:

It stands for Domain Name System. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.abc.com might translate to 198.105.232.4.
The Port number for DNS is 53.

*__Transport Layer Security (TLS)__

Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Service Layer (SSL). TLS ensures that no third party may eavesdrops or tampers with any message.

There are several benefits of TLS:

Encryption:
TLS/SSL can help to secure transmitted data using encryption.

Interoperability:
TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.

Algorithm flexibility:
TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.

Ease of Deployment:
Many applications TLS/SSL temporarily on a windows server 2003 operating systems.

Ease of Use:
Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

***Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter)**

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

***Types of Hub**

Active Hub:- These are the hubs that have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.

Passive Hub :- These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

Intelligent Hub :- It works like active hubs and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

3. Bridge – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

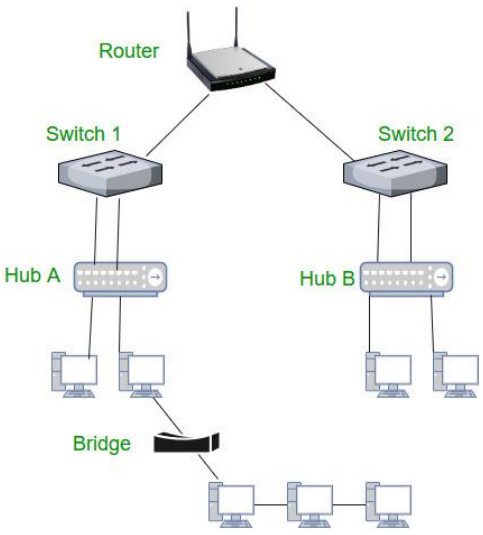
Types of Bridges

Transparent Bridges:- These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.

Source Routing Bridges:- In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but broadcast domain remains the same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. Gateway is also called a protocol converter.

7. Brouter – It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks, and working as the bridge, it is capable of filtering local area network traffic.

8. NIC – NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and router or modem. NIC card is a layer 2 device which means that it works on both physical and data link layer of the network model.

***LAN Technologies | ETHERNET**

Local Area Network (LAN) is a data communication network connecting various terminals or computers within a building or limited geographical area. The connection among the devices could be wired or wireless. Ethernet, Token Ring and Wireless LAN using IEEE 802.11 are examples of standard LAN technologies.

LAN has the following topologies:

Star Topology

Bus Topology

Ring Topology

Mesh Topology

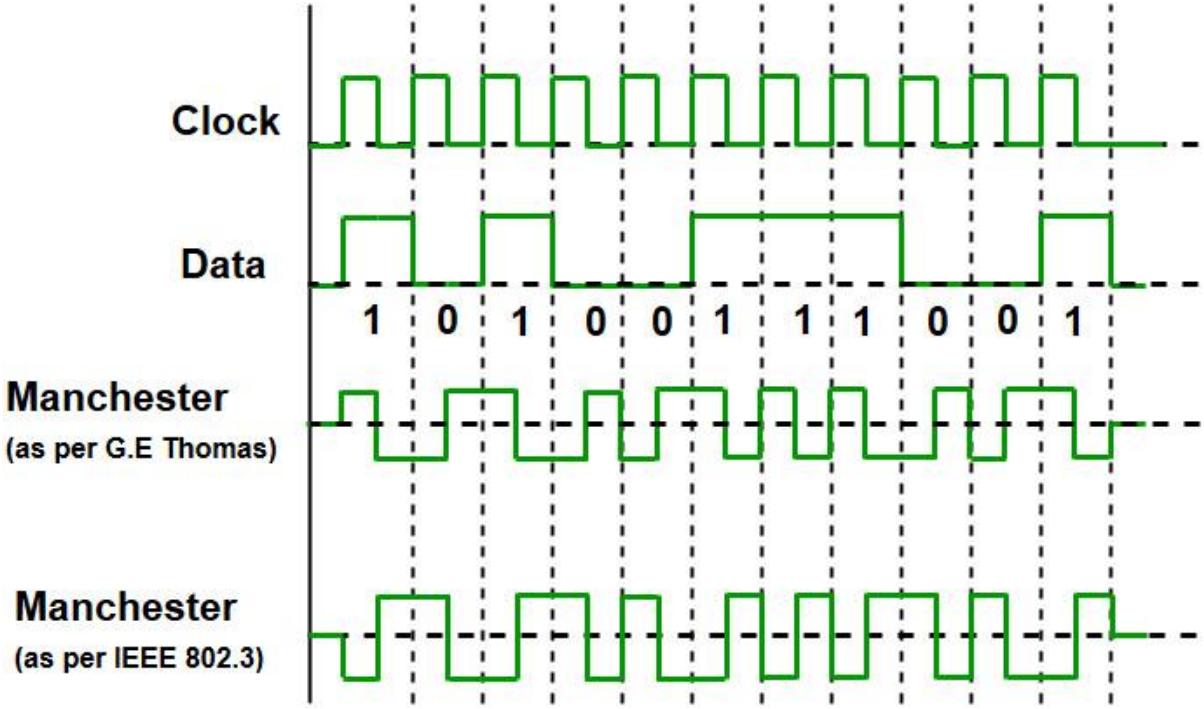
Hybrid Topology

Tree Topology

Ethernet:-

Ethernet is the most widely used LAN technology, which is defined under IEEE standards 802.3. The reason behind its wide usability is Ethernet is easy to understand, implement, maintain, and allows low-cost network implementation. Also, Ethernet offers flexibility in terms of topologies that are allowed. Ethernet generally uses Bus Topology. Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer. For Ethernet, the protocol data unit is Frame since we mainly deal with DLL. In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD.

Manchester Encoding Technique is used in Ethernet.



Since we are talking about IEEE 802.3 standard Ethernet, therefore, 0 is expressed by a high-to-low transition, a 1 by the low-to-high transition. In both Manchester Encoding and Differential Manchester, the Encoding Baud rate is double of bit rate.

Baud rate = 2* Bit rate

Ethernet LANs consist of network nodes and interconnecting media or links. The network nodes can be of two types:
Data Terminal Equipment (DTE):- Generally, DTEs are the end devices that convert the user information into signals or reconvert the received signals. DTEs devices are: personal computers, workstations, file servers or print servers also referred to as end stations. These devices are either the source or the destination of data frames. The data terminal equipment may be a single piece of equipment or multiple pieces of equipment that are interconnected and perform all the required functions to allow the user to communicate. A user can interact with DTE or DTE may be a user.

Data Communication Equipment (DCE):- DCEs are the intermediate network devices that receive and forward frames across the network. They may be either standalone devices such as repeaters, network switches, routers, or maybe communications interface units such as interface cards and modems. The DCE performs functions such as signal conversion, coding, and maybe a part of the DTE or intermediate equipment.

Currently, these data rates are defined for operation over optical fibers and twisted-pair cables:
i) Fast Ethernet
Fast Ethernet refers to an Ethernet network that can transfer data at a rate of 100 Mbit/s.

ii) Gigabit Ethernet
Gigabit Ethernet delivers a data rate of 1,000 Mbit/s (1 Gbit/s).

iii) 10 Gigabit Ethernet
10 Gigabit Ethernet is the recent generation and delivers a data rate of 10 Gbit/s (10,000 Mbit/s). It is generally used for backbones in high-end applications requiring high data rates.

ALOHA

The Aloha protocol was designed as part of a project at the University of Hawaii. It provided data transmission between computers on several of the Hawaiian Islands involving packet radio networks. Aloha is a multiple access protocol at the data link layer and proposes how multiple terminals access the medium without interference or collision.

There are two different versions of ALOHA:

1. Pure Aloha

Pure Aloha is an un-slotted, decentralized, and simple to implement protocol. In pure ALOHA, the stations simply transmit frames whenever they want data to send. It does not check whether the channel is busy or not before transmitting. In case, two or more stations transmit simultaneously, the collision occurs and frames are destroyed. Whenever any station transmits a frame, it expects acknowledgement from the receiver. If it is not received within a specified time, the station assumes that the frame or acknowledgement has been destroyed. Then, the station waits for a random amount of time and sends the frame again. This randomness helps in avoiding more collisions. This scheme works well in small networks where the load is not much. But in largely loaded networks, this scheme fails poorly. This led to the development of Slotted Aloha.

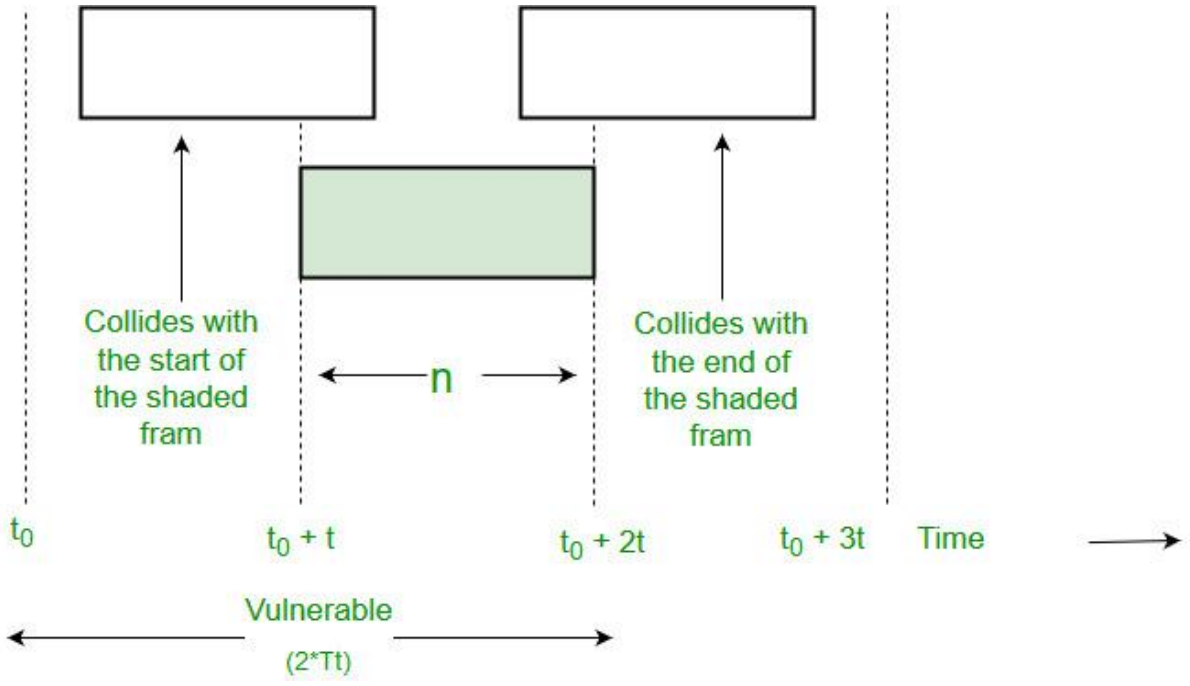
To assure pure aloha: Its throughput and rate of transmission of the frame to be predicted.

For that to make some assumptions:

i) All the frames should be the same length.

ii) Stations can not generate frames while transmitting or trying to transmit frames.

iii)The population of stations attempts to transmit (both new frames and old frames that collided) according to a Poisson distribution.



Vulnerable Time = 2 * Tt

The efficiency of Pure ALOHA:

Spure= G * e^-2G

where G is number of stations wants to transmit in Tt slot.

Maximum Efficiency:

Maximum Efficiency will be obtained when G=1/2

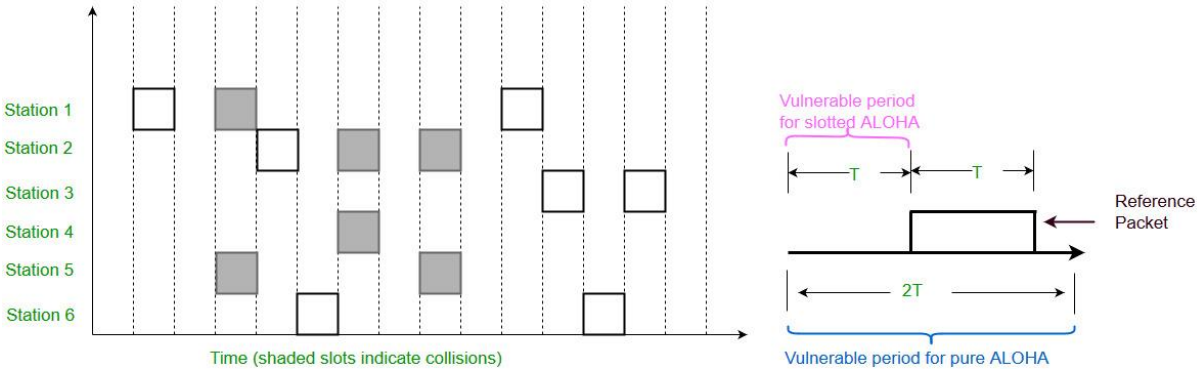
(Spure)max = 1/2 * e^-1

= 0.184

Which means, in Pure ALOHA, only about 18.4% of the time is used for successful transmissions.

2. Slotted Aloha

This is quite similar to Pure Aloha, differing only in the way transmissions take place. Instead of transmitting right at demand time, the sender waits for some time. In slotted ALOHA, the time of the shared channel is divided into discrete intervals called Slots. The stations are eligible to send a frame only at the beginning of the slot and only one frame per slot is sent. If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the beginning of the next time slot. There is still a possibility of collision if two stations try to send at the beginning of the same time slot. But still, the number of collisions that can possibly take place is reduced by a large margin and the performance becomes much well compared to Pure Aloha.



Collision is possible for only the current slot. Therefore, Vulnerable Time is Tt.

The efficiency of Slotted ALOHA:

Sslotted = G * e^-G

Maximum Efficiency:

(Sslotted)max = 1 * e^-1

= 1/e = 0.368

Maximum Efficiency, in Slotted ALOHA, is 36.8%.

2P (Peer To Peer) File Sharing

Introduction
In Computer Networking, P2P is a file-sharing technology, allowing the users to access mainly the multimedia files like videos, music, e-books, games, etc. The individual users in this network are referred to as peers. The peers request files from other peers by establishing TCP or UDP connections.

How P2P works(Overview)
A peer-to-peer network allows computer hardware and software to communicate without the need for a server. Unlike client-server architecture, there is no central server for processing requests in a P2P architecture. The peers directly interact with one another without the requirement of a central server.

Now, when one peer makes a request, it is possible that multiple peers have a copy of that requested object. Now the problem is how to get the IP addresses of all those peers. This is decided by the underlying architecture supported by the P2P systems. By means of one of these methods, the client peer can get to know about all the peers which have the requested object/file and the file transfer takes place directly between these two peers.

Three such Architectures exist:

Centralized Directory

Query Flooding

Exploiting Heterogeneity

1. Centralized Directory

It is somewhat similar to client-server architecture in the sense that it maintains a huge central server to provide directory service. All the peers inform this central server of their IP address and the files they are making available for sharing. The server queries the peers at regular intervals to make sure if the peers are still connected or not. So basically this server maintains a huge database regarding which file is present at which IP addresses.

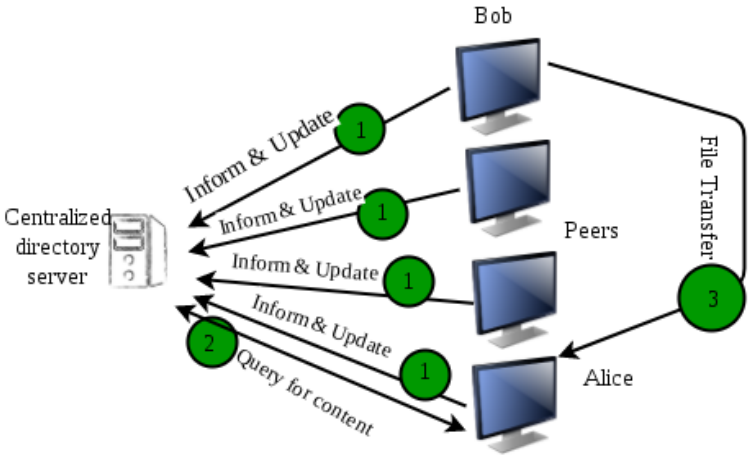
Working:

Now whenever a requesting peer comes in, it sends its query to the server.

Since the server has all the information of its peers, so it returns the IP addresses of all the peers having the requested file to the peer.

Now the file transfer takes place between these two peers.

The first system which made use of this method was Napster, for the purpose of Mp3 distribution.



P2P paradigm with a centralised directory

The major problem with such an architecture is that there is a single point of failure. If the server crashes, the whole P2P network crashes. Also, since all of the processing is to be done by a single server so a huge amount of the database has to be maintained and regularly updated.

2. Query Flooding

Unlike the centralized approach, this method makes use of distributed systems.

In this, the peers are supposed to be connected to an overlay network. It means if a connection/path exists from one peer to another, it is a part of this overlay network.

In this overlay network, peers are called nodes, and the connection between peers is called an edge between the nodes, thus resulting in a graph-like structure.

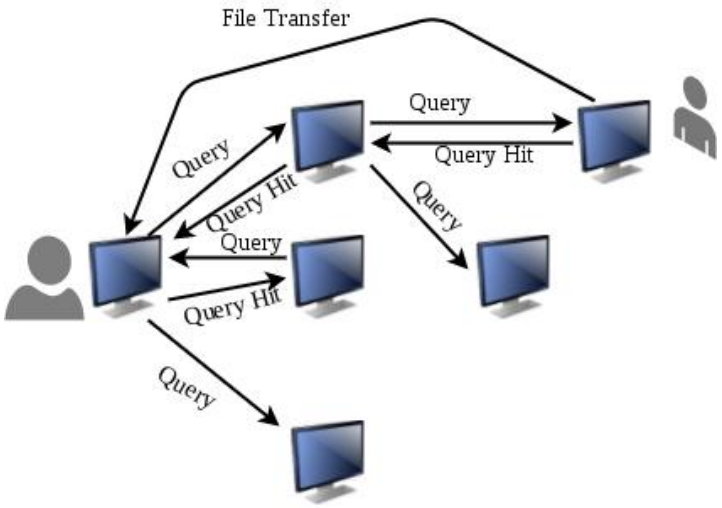
Working

Now when one peer requests for some file, this request is sent to all its neighboring nodes i.e. to all nodes which are connected to this node. If those nodes don't have the required file, they pass on the query to their neighbors and so on. This is called query flooding.

When the peer with the requested file is found (referred to as query hit), the query flooding stops and it sends back the file name and file size to the client, thus following the reverse path.

If there are multiple query hits, the client selects from one of these peers.

Gnutella was the first decentralized peer-to-peer network.



This method also has some disadvantages like, the query has to be sent to all the neighboring peers unless a match is found. This increases traffic in the network.

3. Exploiting heterogeneity

This P2P architecture makes use of both the above-discussed systems.

It resembles a distributed system like Gnutella because there is no central server for query processing.

But unlike Gnutella, it does not treat all its peers equally. The peers with higher bandwidth and network connectivity are at a higher priority and are called group leaders/supernodes. The rest of the peers are assigned to these supernodes.

These supernodes are interconnected and the peers under these supernodes inform their respective leaders about their connectivity, IP address, and the files available for sharing.

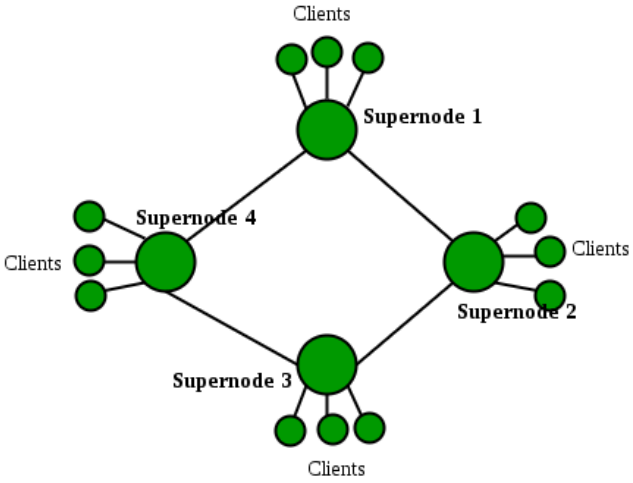
KaZaA technology is such an example that makes use of Napster and Gnutella.
Thus, the individual group leaders along with their child peers from a Napster-like structure. These group leaders then interconnect among themselves to resemble a Gnutella-like structure.

Working

This structure can process the queries in two ways.

The first one is that the supernodes could contact other super nodes and merge their databases with their own database. Thus, this supernode now has information of a large number of peers.

Another approach is that when a query comes in, it is forwarded to the neighboring super nodes until a match is found, just like in Gnutella. Thus query flooding exists but with limited scope as each supernode has many child peers. Hence, such a system exploits the heterogeneity of the peers by designating some of them as group leaders/supernodes and others as their child peers.



***Basic Network Attacks in Computer Network**

Many people rely on the Internet for many of their professional, social and personal activities. But there are also people who attempt to damage our Internet-connected computers, violate our privacy and render inoperable the Internet services.

Given the frequency and variety of existing attacks as well as the threat of new and more destructive future attacks, network security has become a central topic in the field of computer networking.

How are computer networks vulnerable? What are some of the more prevalent types of attacks today?

Malware – short for malicious software which is specifically designed to disrupt, damage, or gain authorized access to a computer system. Much of the malware out there today is self-replicating: once it infects one host, from that host it seeks entry into other hosts over the Internet, and from the newly infected hosts, it seeks entry into yet more hosts. In this manner, self-replicating malware can spread exponentially fast.

Virus – A malware which requires some form of user's interaction to infect the user's device. The classic example is an e-mail attachment containing malicious executable code. If a user receives and opens such an attachment, the user inadvertently runs the malware on the device.

Worm – A malware which can enter a device without any explicit user interaction. For example, a user may be running a vulnerable network application to which an attacker can send malware. In some cases, without any user intervention, the application may accept the malware from the Internet and run it, creating a worm.

Botnet – A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam.

DoS (Denial of Service) – A DoS attack renders a network, host, or other pieces of infrastructure unusable by legitimate users. Most Internet DoS attacks fall into one of three categories :

• Vulnerability attack: This involves sending a few well-crafted messages to a vulnerable application or operating system running on a targeted host. If the right sequence of packets is sent to a vulnerable application or operating system, the service can stop or, worse, the host can crash.

• Bandwidth flooding: The attacker sends a deluge of packets to the targeted host—so many packets that the target's access link becomes clogged, preventing legitimate packets from reaching the server.

• Connection flooding: The attacker establishes a large number of half-open or fully open TCP connections at the target host. The host can become so bogged down with these bogus connections that it stops accepting legitimate connections.

DDoS (Distributed DoS) – DDoS is a type of DOS attack where multiple compromised systems, are used to target a single system causing a Denial of Service (DoS) attack. DDoS attacks leveraging botnets with thousands of comprised hosts are a common occurrence today. DDoS attacks are much harder to detect and defend against than a DoS attack from a single host.

Packet sniffer – A passive receiver that records a copy of every packet that flies by is called a packet sniffer. By placing a passive receiver in the vicinity of the wireless transmitter, that receiver can obtain a copy of every packet that is transmitted! These packets can contain all kinds of sensitive information, including passwords, social security numbers, trade secrets, and private personal messages. some of the best defenses against packet sniffing involve cryptography.

IP Spoofing – The ability to inject packets into the Internet with a false source address is known as IP spoofing, and is but one of many ways in which one user can masquerade as another user. To solve this problem, we will need end-point authentication, that is, a mechanism that will allow us to determine with certainty if a message originates from where we think it does.

Man-in-the-Middle Attack – As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

Compromised-Key Attack – A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack.

Phishing – The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

DNS spoofing – Also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect IP address.

Rootkit – Rootkits are stealthy packages designed to benefit administrative rights and get the right of entry to a community tool. Once installed, hackers have complete and unrestricted get right of entry to the tool and can, therefore, execute any movement including spying on customers or stealing exclusive data with no hindrance.

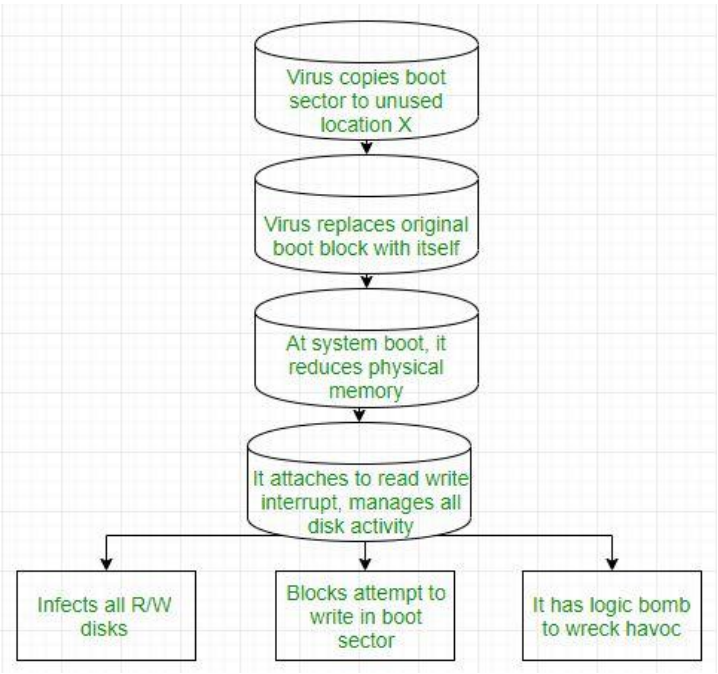
Types of Viruses

A virus is a fragment of code embedded in a legitimate program. Viruses are self-replicating and are designed to infect other programs. They can wreak havoc in a system by modifying or destroying files causing system crashes and program malfunctions. On reaching the target machine a virus dropper(usually a trojan horse) inserts the virus into the system.
For more details, refer to this.

Various types of viruses:

File Virus:
This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called a Parasitic virus because it leaves no file intact but also leaves the host functional.

Boot sector Virus:
It infects the boot sector of the system, executing every time system is booted and before the operating system is loaded. It infects other bootable media like floppy disks. These are also known as memory viruses as they do not infect the file systems.



Macro Virus:
Unlike most viruses which are written in a low-level language(like C or assembly language), these are written in a high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, the macro viruses can be contained in spreadsheet files.

Source code Virus:
It looks for source code and modifies it to include virus and to help spread it.

Polymorphic Virus:
A virus signature is a pattern that can identify a virus(a series of bytes that make up virus code). So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The functionality of the virus remains the same but its signature is changed.

Encrypted Virus:
In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then executes.

Stealth Virus:
It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of viruses becomes very difficult. For example, it can change the read system call such that whenever the user asks to read a code modified by a virus, the original form of code is shown rather than infected code.

Tunneling Virus:
This virus attempts to bypass detection by antivirus scanner by installing itself in the interrupt handler chain. Interception programs, which remain in the background of an operating system and catch viruses, become disabled during the course of a tunneling virus. Similar viruses install themselves in device drivers.

Multipartite Virus:
This type of virus is able to infect multiple parts of a system including the boot sector, memory, and files. This makes it difficult to detect and contain.

Armored Virus:
An armored virus is coded to make it difficult for antivirus to unravel and understand. It uses a variety of techniques to do so like fooling antivirus to believe that it lies somewhere else than its real location or using compression to complicate its code.

Browser Hijacker:
As the name suggests this virus is coded to target the user's browser and can alter the browser settings. It is also called the browser redirect virus because it redirects your browser to other malicious sites that can harm your computer system.

Resident Virus: Resident viruses installation store for your RAM and meddle together along with your device operations. They're so sneaky that they could even connect themselves for your anti-virus software program files.

What is encryption?

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a cryptographic key: a set of mathematical values that both the sender and the recipient of an encrypted message agree on.

Although encrypted data appears random, encryption proceeds in a logical, predictable way, allowing a party that receives the encrypted data and possesses the right key to decrypt the data, turning it back into plaintext. Truly secure encryption will use keys complex enough that a third party is highly unlikely to decrypt or break the ciphertext by brute force — in other words, by guessing the key.

Data can be encrypted "at rest," when it is stored, or "in transit," while it is being transmitted somewhere else.

What is a key in cryptography?

A cryptographic key is a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) it.

What are the different types of encryption?

The two main kinds of encryption are symmetric encryption and asymmetric encryption. Asymmetric encryption is also known as public key encryption.

In symmetric encryption, there is only one key, and all communicating parties use the same (secret) key for both encryption and decryption. In asymmetric, or public key, encryption, there are two keys: one key is used for encryption, and a different key is used for decryption. The decryption key is kept private (hence the "private key" name), while the encryption key is shared publicly, for anyone to use (hence the "public key" name). Asymmetric encryption is a foundational technology for TLS (often called SSL).

Why is data encryption necessary?

Privacy: Encryption ensures that no one can read communications or data at rest except the intended recipient or the rightful data owner. This prevents attackers, ad networks, Internet service providers, and in some cases governments from intercepting and reading sensitive data.

Security: Encryption helps prevent data breaches, whether the data is in transit or at rest. If a corporate device is lost or stolen and its hard drive is properly encrypted, the data on that device will still be secure. Similarly, encrypted communications enable the communicating parties to exchange sensitive data without leaking the data.

Data integrity: Encryption also helps prevent malicious behavior such as on-path attacks. When data is transmitted across the Internet, encryption (along with other integrity protections) ensures that what the recipient receives has not been tampered with on the way.

Authentication: Public key encryption, among other things, can be used to establish that a website's owner owns the private key listed in the website's TLS certificate. This allows users of the website to be sure that they are connected to the real website (see What is public key encryption? to learn more).

Regulations: For all these reasons, many industry and government regulations require companies that handle user data to keep that data encrypted. Examples of regulatory and compliance standards that require encryption include HIPAA, PCI-DSS, and the GDPR.

What is an encryption algorithm?

An encryption algorithm is the method used to transform data into ciphertext. An algorithm will use the encryption key in order to alter the data in a predictable way, so that even though the encrypted data will appear random, it can be turned back into plaintext by using the decryption key.

What are some common encryption algorithms?

Commonly used symmetric encryption algorithms include:

AES

3-DES

SNOW

Commonly used asymmetric encryption algorithms include:

RSA

Elliptic curve cryptography

What is a brute force attack in encryption?

A brute force attack is when an attacker who does not know the decryption key attempts to determine the key by making millions or billions of guesses. Brute force attacks are much faster with modern computers, which is why encryption has to be extremely strong and complex. Most modern encryption methods, coupled with high-quality passwords, are resistant to brute force attacks, although they may become vulnerable to such attacks in the future as computers become more and more powerful. Weak passwords are still susceptible to brute force attacks.

How is encryption used to keep Internet browsing secure?

Encryption is foundational for a variety of technologies, but it is especially important for keeping HTTP requests and responses secure, and for authenticating website origin servers. The protocol responsible for this is called HTTPS (Hypertext Transfer Protocol Secure). A website served over HTTPS instead of HTTP will have a URL that begins with https:// instead of http://, usually represented by a secured lock in the address bar.

HTTPS uses the encryption protocol called Transport Layer Security (TLS). In the past, an earlier encryption protocol called Secure Sockets Layer (SSL) was the standard, but TLS has replaced SSL. A website that implements HTTPS will have a TLS certificate installed on its origin server. Learn more about TLS and HTTPS.

–

What is a VLAN?

A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs). A LAN is a group of computers and devices that share a communications line or wireless link to a server within the same geographical area.

VLANs make it easy for network administrators to partition a single switched network to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure. VLANs are often set up by larger businesses to re-partition devices for better traffic management.

VLANs are also important because they can help improve the overall performance of a network by grouping together devices that communicate most frequently. VLANs also provide security on larger networks by allowing a higher degree of control over which devices have access to each other. VLANs tend to be flexible because they are based on logical connections, rather than physical.

One or more network switches may support multiple, independent VLANs, creating Layer 2 (data link) implementations of subnets. A VLAN is associated with a broadcast domain. It is usually composed of one or more network switches.

Types of VLANs

Types of VLANs include Protocol based, static and dynamic VLANs.

A Protocol VLAN- which has traffic handled based on its protocol. A switch will segregate or forward traffic based on the traffics protocol.

Static VLAN- also referred to as port-based VLAN, needs a network administrator to assign the ports on a network switch to a virtual network; while:

Dynamic VLAN- allows a network administrator just to define network membership based on device characteristics, as opposed to switch port location.

How VLAN works

Ports (interfaces) on switches can be assigned to one or more VLANs, enabling systems to be divided into logical groups -- based on which department they are associated with -- and establish rules about how systems in the separate groups are allowed to communicate with each other. These groups can range from the simple and practical (computers in one VLAN can see the printer on that VLAN, but computers outside that VLAN cannot), to the complex and legal (for example, computers in the retail banking departments cannot interact with computers in the trading departments).

Each VLAN provides data link access to all hosts connected to switch ports configured with the same VLAN ID. The VLAN tag is a 12-bit field in the Ethernet header that provides support for up to 4,096 VLANs per switching domain. VLAN tagging is standardized in IEEE (Institute of Electrical and Electronics Engineers) 802.1Q and is often called Dot1Q.

When an untagged frame is received from an attached host, the VLAN ID tag configured on that interface is added to the data link frame header, using the 802.1Q format. The 802.1Q frame is then forwarded toward the destination. Each switch uses the tag to keep each VLAN's traffic separate from other VLANs, forwarding it only where the VLAN is configured. Trunk links between switches handle multiple VLANs, using the tag to keep them segregated. When the frame reaches the destination switch port, the VLAN tag is removed before the frame is to be transmitted to the destination device.

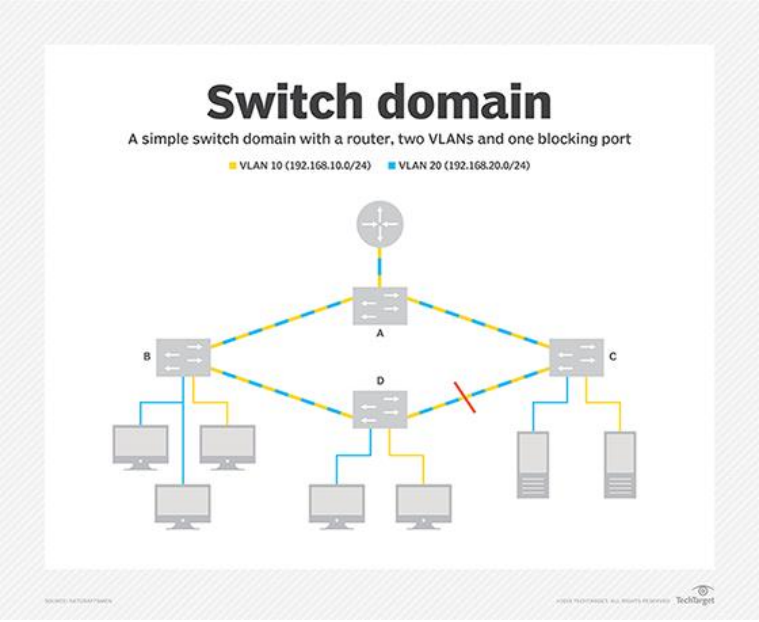
Multiple VLANs can be configured on a single port using a trunk configuration in which each frame sent via the port is tagged with the VLAN ID, as described above. The neighboring device's interface, which may be on another switch or on a host that supports 802.1Q tagging, will need to support trunk mode configuration to transmit and receive tagged frames. Any untagged Ethernet frames are assigned to a default VLAN, which can be designated in the switch configuration.

When a VLAN-enabled switch receives an untagged Ethernet frame from an attached host, it adds the VLAN tag assigned to the ingress interface. The frame is forwarded to the port of the host with the destination MAC address(media access control address). Broadcast, unknown unicast and multicast (BUM traffic) is forwarded to all ports in the VLAN. When a previously unknown host replies to an unknown unicast frame, the switches learn the location of this host and do not flood subsequent frames addressed to that host.

The switch-forwarding tables are kept up to date by two mechanisms. First, old forwarding entries are removed from the forwarding tables periodically, often a configurable timer. Second, any topology change causes the forwarding table refresh timer to be reduced, triggering a refresh.

The Spanning Tree Protocol (STP) is used to create loop-free topology among the switches in each Layer 2 domain. A per-VLAN STP instance can be used, which enables different Layer 2 topologies or a multi-instance STP (MISTP) can be used to reduce STP overhead if the topology is the same among multiple VLANs. STP blocks forwarding on links that might produce forwarding loops, creating a spanning tree from a selected root switch. This blocking means that some links will not be used for forwarding until a failure in another part of the network causes STP to make the link part of an active forwarding path.

The figure below shows a switch domain with four switches with two VLANs. The switches are connected in a ring topology. STP causes one port to go into blocking state so that a tree topology is formed (i.e., no forwarding loops). The port on switch D to switch C is blocking, as indicated by the red bar across the link. The links between the switches and to the router are trunking VLAN 10 (orange) and VLAN 20 (green). The hosts connected to VLAN 10 can communicate with server O. The hosts connected to VLAN 20 can communicate with server G. The router has an IPv4 subnet configured on each VLAN to provide connectivity for any communications between the two VLANs.



NETCRAFTSMEN

Advantages and Disadvantages of VLAN

Advantages to VLAN include reduced broadcast traffic, security, ease of administration and broadcast domain confinement.

However, a disadvantage of VLANs includes the limitation of 4,096 VLANs per switching domain creates problems for large hosting providers, which often need to allocate tens or hundreds of VLANs for each customer. To address this limitation, other protocols, like VXLAN(Virtual Extensible LAN), NVGRE (Network Virtualization using Generic Routing Encapsulation) and Geneve, support larger tags and the ability to tunnel Layer 2 frames within Layer 3 (network) packets.

Finally, data communications between VLANs is performed by routers. Modern switches often incorporate routing functionality and are called Layer 3 switches.

VLAN membership can be classified by port, MAC address, and protocol type.

Layer 1 VLAN: Membership by Port. ...

Layer 2 VLAN: Membership by MAC Address. ...

Layer 2 VLAN: Membership by Protocol Type. ...

Layer 3 VLAN: Membership by IP Subnet Address. ...

Higher Layer VLAN's.

How internet traffic is routed to your website or web application

All computers on the internet, from your smart phone or laptop to the servers that serve content for massive retail websites, communicate with one another by using numbers. These numbers, known as IP addresses, are in one of the following formats:

Internet Protocol version 4 (IPv4) format, such as 192.0.2.44

Internet Protocol version 6 (IPv6) format, such as 2001:0db8:85a3:0000:0000:abcd:0001:2345

When you open a browser and go to a website, you don't have to remember and enter a long string of characters like that. Instead, you can enter a domain name like example.com and still end up in the right place. A DNS service such as Amazon Route 53 helps to make that connection between domain names and IP addresses.

Overview of how you configure Amazon Route 53 to route internet traffic for your domain

How Amazon Route 53 routes traffic for your domain

Overview of how you configure Amazon Route 53 to route internet traffic for your domain

Here's an overview of how to use the Amazon Route 53 console to register a domain name and configure Route 53 to route internet traffic to your website or web application.

You register the domain name that you want your users to use to access your content. For an overview, see How domain registration works.

After you register your domain name, Route 53 automatically creates a public hosted zone that has the same name as the domain. For more information, see Working with public hosted zones.

To route traffic to your resources, you create records, also known as resource record sets, in your hosted zone. Each record includes information about how you want to route traffic for your domain, such as the following:

Name

The name of the record corresponds with the domain name (example.com) or subdomain name (www.example.com, retail.example.com) that you want Route 53 to route traffic for.

The name of every record in a hosted zone must end with the name of the hosted zone. For example, if the name of the hosted zone is example.com, all record names must end in example.com. The Route 53 console does this for you automatically.

Type

The record type usually determines the type of resource that you want traffic to be routed to. For example, to route traffic to an email server, you specify MX for Type. To route traffic to a web server that has an IPv4 IP address, you specify A for Type.

Value

Value is closely related to Type. If you specify MX for Type, you specify the names of one or more email servers for Value. If you specify A for Type, you specify an IP address in IPv4 format, such as 192.0.2.136.

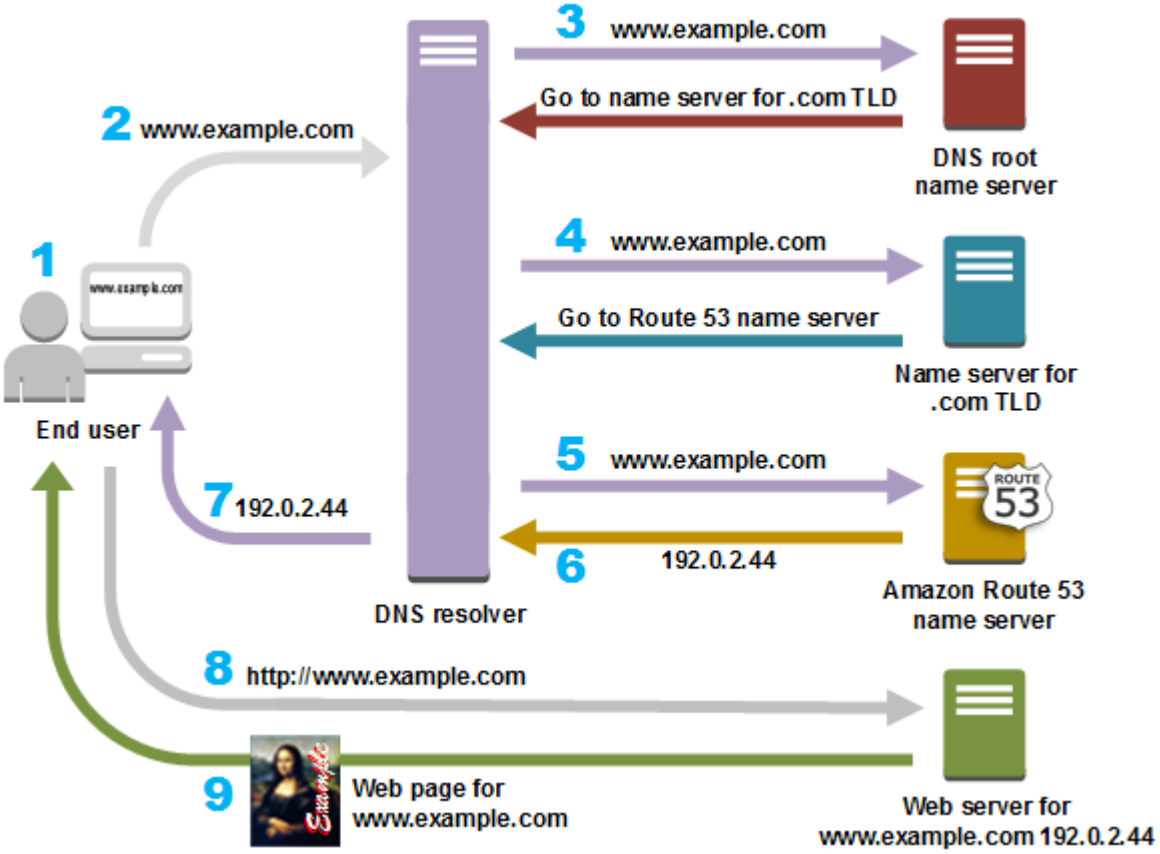
For more information about records, see Working with records.

You can also create special Route 53 records, called alias records, that route traffic to Amazon S3 buckets, Amazon CloudFront distributions, and other AWS resources. For more information, see Choosing between alias and non-alias records and Routing internet traffic to your AWS resources.

For more information about routing internet traffic to your resources, see Configuring Amazon Route 53 as your DNS service.

How Amazon Route 53 routes traffic for your domain

After you configure Amazon Route 53 to route your internet traffic to your resources, such as web servers or Amazon S3 buckets, here's what happens in just a few milliseconds when someone requests content for www.example.com:



A user opens a web browser, enters www.example.com in the address bar, and presses Enter.

The request for www.example.com is routed to a DNS resolver, which is typically managed by the user's internet service provider (ISP), such as a cable internet provider, a DSL broadband provider, or a corporate network.

The DNS resolver for the ISP forwards the request for www.example.com to a DNS root name server.

The DNS resolver forwards the request for www.example.com again, this time to one of the TLD name servers for .com domains. The name server for .com domains responds to the request with the names of the four Route 53 name servers that are associated with the example.com domain.

The DNS resolver caches (stores) the four Route 53 name servers. The next time someone browses to example.com, the resolver skips steps 3 and 4 because it already has the name servers for example.com. The name servers are typically cached for two days.

The DNS resolver chooses a Route 53 name server and forwards the request for www.example.com to that name server.

The Route 53 name server looks in the example.com hosted zone for the www.example.com record, gets the associated value, such as the IP address for a web server, 192.0.2.44, and returns the IP address to the DNS resolver.

The DNS resolver finally has the IP address that the user needs. The resolver returns that value to the web browser.

Note

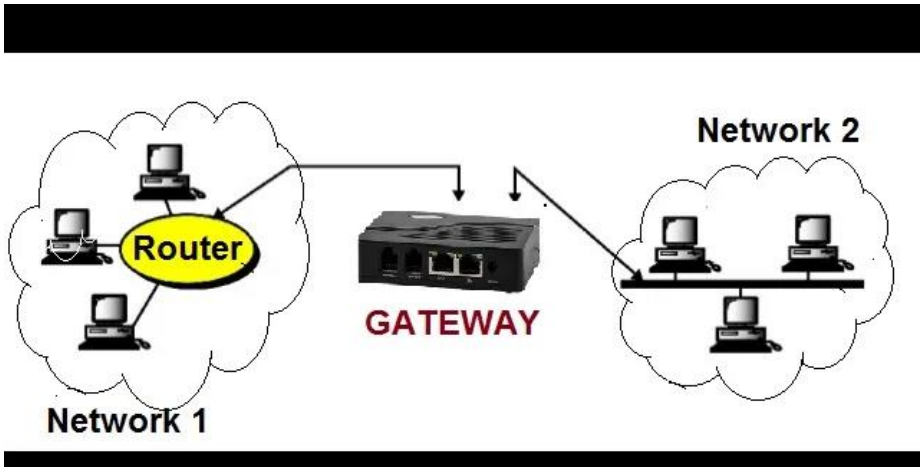
The DNS resolver also caches the IP address for example.com for an amount of time that you specify so that it can respond more quickly the next time someone browses to example.com. For more information, see time to live (TTL).

The web browser sends a request for www.example.com to the IP address that it got from the DNS resolver. This is where your content is, for example, a web server running on an Amazon EC2 instance or an Amazon S3 bucket that's configured as a website endpoint.

The web server or other resource at 192.0.2.44 returns the web page for www.example.com to the web browser, and the web browser displays the page.

What is Gateway in Computer Network

Definition: Gateway is a network hardware device that is used for making communication in between two networks with different transmission protocol together, and it is an entry and exit "Gate" for the networks that helps to bypass the all data with the gateway prior to being routed. Gateways can be used for both WAN and LAN interconnects.



The gateway acts as a "Translator" in between two different systems that is used dissimilar communication protocols, data format or different architectures. It may be a server, router, firewall or other network device that allows to flow the traffic in and out of the network.

Types of Gateways in Networking

There are two different types of network gateways which are divided on the basis of direction of data flow; below explain each one –

Unidirectional Gateways

Bidirectional Gateways

Unidirectional Gateways: These gateways allow to broadcast the data only single direction. All changes are made in the source terminal, and they are replicated to destination node or application. But, they do not permit any change in the destination node are not replicated in the source node. These types of gateway work as archiving tools.

Examples of Gateway

You can also say examples of gateway in the computer network; below mention the list –

VoiP Trunk Gateway

Network Gateway

Internet-To-Orbit Gateway

Media Gateway

Payment Gateway

Default Gateway

IoT Gateway

Cloud Storage Gateway

Email Security Gateway

Web Application Firewalls.

Network Gateway: This gateway provides the best interface in between two dissimilar networks which are operated by different kinds of protocols.

Internet-To-Orbit Gateway: This gateway helps to make connection in between the devices (which are connected with Internet) to satellites and spacecraft orbiting the earth. Examples are – Project HERMES and GENSO (Global Educational Network for Satellite Operations).

VoiP Trunk Gateway: This gateway allows to transmit data in between the plain old telephone service devices such as landline phones and fax machines with the help of VoIP (voice over Internet Protocol).

Media Gateway: This gateway allows to broadcast data into audio and video transmissions.

Payment Gateway: This gateway provides the security for receiving and paying the online payments.

Default Gateway: Default gateway allows to get access external networks while not specifying another gateway.

IoT Gateway: This gateway allows to assimilate the sensor data from IoT (Internet of Things) devices into the field and then it translates them in between many sensor protocols before firing it to the cloud network. They are getting to make connection with user applications, cloud network, and IoT devices.

Cloud Storage Gateway: This gateway allows to make translation for storage requests along with different kinds of cloud storage service API calls like as – SOAP (Simple Object Access Protocol) or REST (REpresentational State Transfer).

Email Security Gateway: It allows to facilitate the transmission of all messages the break organization strategy or will move data with malignant purpose.

Web Application Firewalls: It allows to push the traffic to and from a web server and monitors the application layer data.

Functions of Gateway in Computer Network

Gateway is used to perform various functions in the computer network; such as –

It allows to move the all information over the Web and provides the entry gate for several networks then users are able to perform many tasks like as send email, navigate the Web Page, buy any product and services over the Web, etc.

It plays the role as bridge in between the sensors internet devices.

With using of gateway, battery life of sensors and other devices is getting to boost up.

With using of gateway, it allows to make communication with sensors and internet devices over the various protocols and then translate data into standard protocol that to be transmitted to the cloud.

It helps to reduce the latency while preparing the information.

It allows to get reduction of the number of sensors and devices connected to the web.

Working of Gateway | How does it Work?

Network gateway is a center point of the many networks that has ability to access other networks. In the Intranet, router plays the role as a gateway node that attaches the network is known as the "Gateway". But, in the large scale organizations, the special computer controls the traffic in between the networks as a gateway points. In the commercial enterprise, the computer server acts as gateway nodes and it can also plays the role as proxy server or firewall at times.

Gateway can be connected with router because router has all information that where to send data packets then network switch take decision for in and out path of gateway for arriving the designated packet, and here operating system is used for sharing internet behaves such as gateway and built the connection along with internal networks.

What Is an Example of an API? When you use an application on your mobile phone, the application connects to the Internet and sends data to a server. ... That's where the waiter or API comes in. The waiter is the messenger – or API – that takes your request or order and tells the kitchen – the system – what to do.

API Gateway

An API gateway is an API management tool that sits between a client and a collection of backend services. An API gateway acts as a reverse proxy to accept all application programming interface (API) calls, aggregate the various services required to fulfill them, and return the appropriate result.

Why use an API gateway?

Most enterprise APIs are deployed via API gateways. It's common for API gateways to handle common tasks that are used across a system of API services, such as user authentication, rate limiting, and statistics.

At its most basic, an API service accepts a remote request and returns a response. But real life is never that simple. Consider your various concerns when you host large-scale APIs.

You want to protect your APIs from overuse and abuse, so you use an authentication service and rate limiting.

You want to understand how people use your APIs, so you've added analytics and monitoring tools.

If you have monetized APIs, you'll want to connect to a billing system.

You may have adopted a microservices architecture, in which case a single request could require calls to dozens of distinct applications.

Over time you'll add some new API services and retire others, but your clients will still want to find all your services in the same place.

Your challenge is offering your clients a simple and dependable experience in the face of all this complexity. An API gateway is a way to decouple the client interface from your backend implementation. When a client makes a request, the API gateway breaks it into multiple requests, routes them to the right places, produces a response, and keeps track of everything.

An API gateway's role in API management

An API gateway is one part of an API management system. The API gateway intercepts all incoming requests and sends them through the API management system, which handles a variety of necessary functions.

Exactly what the API gateway does will vary from one implementation to another. Some common functions include authentication, routing, rate limiting, billing, monitoring, analytics, policies, alerts, and security.

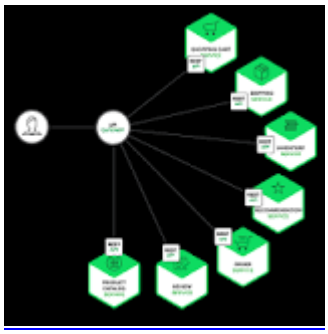
How an API gateway supports DevOps and serverless environments

In organizations that follow a DevOps approach, developers use microservices to build and deploy apps in a fast-paced, iterative way. APIs are one of the most common ways that microservices communicate.

Additionally, modern cloud development, including the serverless model, depends on APIs for provisioning infrastructure. You can deploy serverless functions and manage them using an API gateway.

In general, as integration and interconnectivity become more important, so do APIs. And as API complexity increases and usage grows, so does the value of an API gateway.

What is API Gateway example?



A great example of an API Gateway is the Netflix API Gateway. The Netflix streaming service is available on hundreds of different kinds of devices including televisions, set-top boxes, smartphones, gaming systems, tablets, etc. Initially, Netflix attempted to provide a one-size-fits-all API for their streaming service.

What is the need of API gateway?

API gateways help to prevent malicious attacks by providing an additional layer of protection from attack vectors such as SQL Injection, XML Parser exploits, and denial-of-service (DoS) attacks. Enables support for mixing communication protocols

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services. Using API Gateway, you can create RESTful APIs and WebSocket APIs that enable real-time two-way communication applications. API Gateway supports containerized and serverless workloads, as well as web applications.

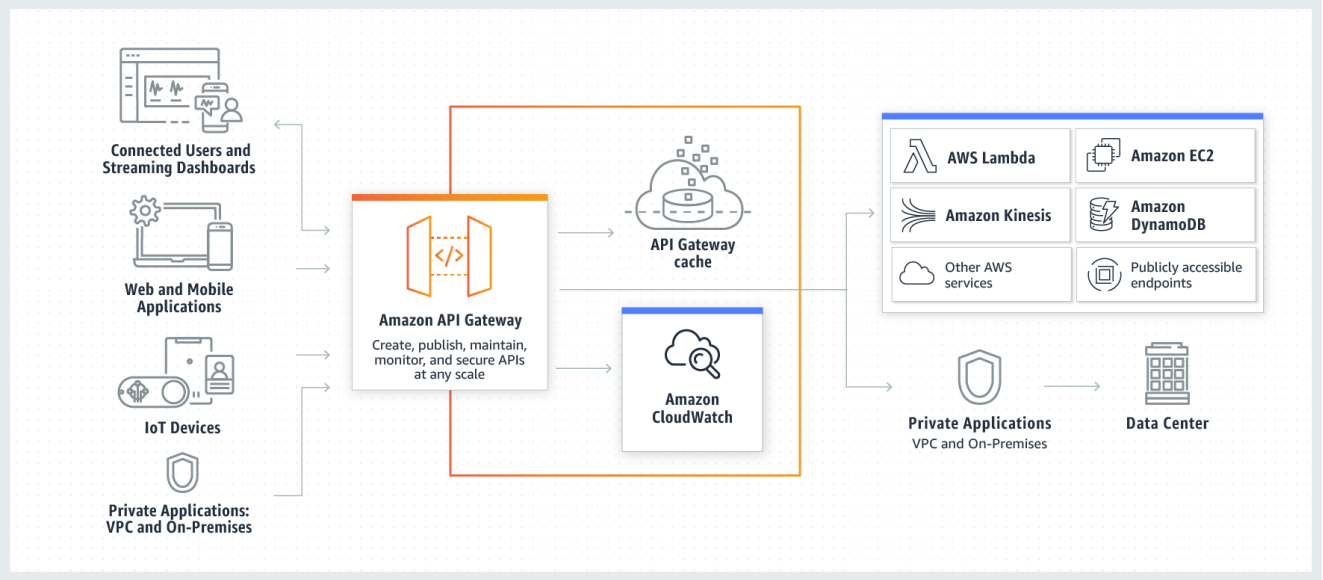
API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, CORS support, authorization and access control, throttling, monitoring, and API version management. API Gateway has no minimum fees or startup costs. You pay for the API calls you receive and the amount of data transferred out and, with the API Gateway tiered pricing model, you can reduce your cost as your API usage scales.

RESTful APIs

Build RESTful APIs optimized for serverless workloads and HTTP backends using HTTP APIs. HTTP APIs are the best choice for building APIs that only require API proxy functionality. If your APIs require API proxy functionality and API management features in a single solution, API Gateway also offers REST APIs.

WEBSOCKET APIs

Build real-time two-way communication applications, such as chat apps and streaming dashboards, with WebSocket APIs. API Gateway maintains a persistent connection to handle message transfer between your backend service and your clients.



NAT Gateway

A NAT gateway is a Network Address Translation (NAT) service. You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances. ... You route traffic from the NAT gateway to the internet gateway for the VPC.

Purpose

A NAT gateway gives cloud resources without public IP addresses access to the internet without exposing those resources to incoming internet connections.

Why do we need NAT gateway?

NAT Gateway, also known as Network Address Translation Gateway, is used to enable instances present in a private subnet to help connect to the internet or AWS services. In addition to this, the gateway makes sure that the internet doesn't initiate a connection with the instances.

What is difference between NAT gateway and Internet gateway?

Internet Gateway (IGW) allows instances with public IPs to access the internet. NAT Gateway (NGW) allows instances with no public IPs to access the internet.

Do you need Internet gateway for NAT?

Internet Gateway is required to provide internet access to the NAT Gateway. ... A NAT Gateway enables instances in a private subnet to connect to services outside your VPC using the NAT Gateway's IP address.

How do I connect to my NAT gateway?

After ensuring that prerequisites are met, follow these steps:

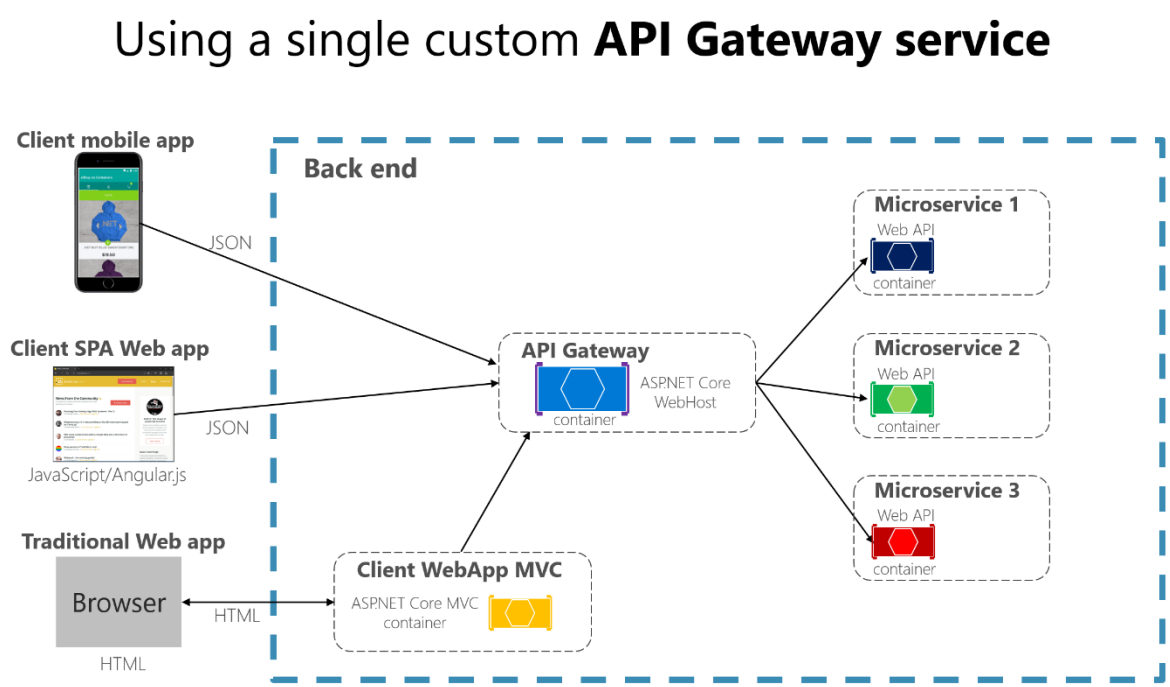
Sign in to the AWS Management Console.

Open the Amazon VPC console.

Choose NAT Gateway from the navigation bar on the left.

Choose Create NAT Gateway and then select the public subnet and EIP that you have provisioned for the NAT gateway.

Service Gateway:



Why have a service gateway?

A service gateway is a single access point and acts as a proxy for multiple services. A service gateway enables transformations, routing, and common processing across all the services. A service gateway module is a single mediation that handles the requests for multiple service consumers and providers.

What Is a VPN? - Virtual Private Network

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

How does a virtual private network (VPN) work?

A VPN extends a corporate network through encrypted connections made over the Internet. Because the traffic is encrypted between the device and the network, traffic remains private as it travels. An employee can work outside the office and still securely connect to the corporate network. Even smartphones and tablets can connect through a VPN.

What is secure remote access?

Secure remote access provides a safe, secure way to connect users and devices remotely to a corporate network. It includes VPN technology that uses strong ways to authenticate the user or device. VPN technology is available to check whether a device meets certain requirements, also called a device's posture, before it is allowed to connect remotely.

Is VPN traffic encrypted?

Yes, traffic on the virtual network is sent securely by establishing an encrypted connection across the Internet known as a tunnel. VPN traffic from a device such as a computer, tablet, or smartphone is encrypted as it travels through this tunnel. Offsite employees can then use the virtual network to access the corporate network.

Types of VPNs

Remote access

A remote access VPN securely connects a device outside the corporate office. These devices are known as endpoints and may be laptops, tablets, or smartphones. Advances in VPN technology have allowed security checks to be conducted on endpoints to make sure they meet a certain posture before connecting. Think of remote access as computer to network.

AnyConnect VPN Meraki Auto VPN Duo Security (Multi-Factor Authentication)

Site-to-site

A site-to-site VPN connects the corporate office to branch offices over the Internet. Site-to-site VPNs are used when distance makes it impractical to have direct network connections between these offices. Dedicated equipment is used to establish and maintain a connection. Think of site-to-site access as network to network.

Connecting your branch offices

How does a VPN work?

A VPN creates a "tunnel" where you can send data securely using encryption and authentication tools. Businesses often use VPN connections because they're a more secure way to help employees remotely access private company networks, even when they're working outside the office.

The VPN lets remote devices, like laptops, operate as though they're on the same local network. Many VPN router devices can support dozens of tunnels at the same time, using easy configuration tools—ensuring all workers have access to company data, no matter where they are.

Why does your business need a VPN?

At their most basic, VPNs protect businesses and users and their confidential data. Here are other reasons why your business could benefit from a VPN:

Convenience

VPNs are a convenient way to give employees, including remote workers, easy access to your business network without having to be physically present—while maintaining the security of private networks and business resources.

Better security

Communication with a VPN connection provides a higher level of security compared to other methods of remote communication, keeping private networks closed to people who don’t have authorized access. The actual geographic locations of users are protected and not exposed to public or shared networks like the Internet.

Easier administration

It’s easy to add new users or groups of users to networks using flexible VPN software tools. That's good for businesses that are growing faster than their budgets since it means you can often expand network footprints without adding new components or building complicated network configurations.

Are there downsides to using VPNs?

A VPN's success depends on other parts of your network infrastructure. Here are factors that could cause performance issues for your VPN:

Configuration security risks

Design and implementation of a VPN can be complicated. If you’re not sure how to keep it up and running safely, consider bringing in an experienced network security professional to make sure VPN security hasn’t been compromised.

Reliability

Since VPN connections run off the Internet, you need to choose an Internet service provider (ISP) that consistently delivers excellent service with minimal to no downtime.

Scalability

If you need to add new infrastructure or create new configurations, you may run into technical problems due to incompatibility—especially if you're adding new products from different vendors.

Slow connection speeds

If you're using a VPN client that provides free VPN service, your connection speed may be slow, as these providers do not usually offer high-speed connections. Consider whether the speed is sufficient for business needs.

Should you create your own VPN, or buy one?

Instead of trying to build one yourself, you can buy a prebuilt VPN solution. If you're shopping for VPN solutions, ask questions about the ease of configuration.

Steps for setting up a VPN

6 steps to set up a VPN

Step 1: Line up key VPN components

To get started, you'll need a VPN client, a VPN server, and a VPN router. The downloadable client connects you to servers around the world, so employees everywhere can access your small business network. The client can be used on devices like smartphones and laptops, even if workers are using public Wi-Fi networks.

To secure and encrypt all network traffic, you'll also need a VPN router. Many routers come with VPN clients built-in.

Step 2: Prep devices

On occasion, VPN clients can conflict with other clients, or fail to work properly. It's a good idea to prepare your network system before you set up a VPN so that you can avoid problems down the road.

As a first step, uninstall any existing VPN client software that you don’t need. In theory, the VPN clients should be able to work well together, but competing clients can also be a source of problems, so it’s best to remove them.

This is also a good time to consider network configuration. If you plan to install a VPN for workers who'll access online resources in several ways—such as Wi-Fi, 4G modems, and wired connections—you may need to spend more time configuring the VPN client. Simplifying networks by unplugging unused devices can help.

Step 3: Download and install VPN clients

The simplest way to get your VPN up and running is to install clients from your VPN provider. However, they may not offer software for every platform you need, such as Windows, iOS, and Android. Even if they don't, it's better to install what they offer first and then confirm that your VPN account is operating correctly.

Look for the "downloads" page on your VPN provider's website. You should also download apps for the mobile devices that your workers use since you’ll want to protect connections from as many devices as possible.

If the initial client you install works right off the bat, then you can contact the VPN provider about clients for other platforms. And if you can’t log in at all, then you can pass along that information to the VPN provider's support team.

Step 4: Find a setup tutorial

If, for some reason, your VPN provider doesn't offer software for the devices your business uses, check the provider's website for guides on manual setup. Hopefully, you'll find the documentation you need. If you don't, search for other providers' setup guides that use the same devices.

For example, if your business uses Chromebooks, you can search for tutorials specifically for these devices.

Step 5: Log in to the VPN

After you install the VPN client apps, it's time to enter login information. In general, the username and password will be the ones you used when you signed up with the VPN provider, although some companies ask you to create a separate login for the VPN client itself.

Once you're logged in, the VPN app usually connects to the server nearest to your current location.

Step 6: Choose VPN protocols

VPN protocols decide how data is routed between your computer and the VPN server. Some protocols help improve speed, while others help improve data privacy and security.

OpenVPN

This is an open-source protocol, which means you can view its code. OpenVPN is also rapidly becoming an industry standard.

L2TP/IPSec

The Layer 2 Tunnel Protocol is another popular protocol. It has strong security protections and is often bundled with the IPSec protocol, which authenticates and encrypts packets of data sent over the VPN.

SSTP

The Secure Socket Tunneling Protocol is fully integrated with the Microsoft operating system.

PPTP

Point-to-Point Tunneling Protocol is one of the oldest VPN protocols. But it is becoming less widely used since there are faster and more secure protocols available.

Step 7: Troubleshoot

Usually, your VPN provider's client will start working right away. But if that's not the case, try these steps:

Shut down and reopen the client and try rebooting your device.

If you have any other VPN software running, make sure you're disconnected, then close it down.

VPN clients need appropriate software drivers to work correctly. In some cases, you can click on the "repair" setting to reload drivers. Check the settings page to see if this feature is available.

If you're having trouble logging in, double-check your login credentials. Some VPN clients generate their own logins, and some let you choose your own.

Be sure you're using the correct login, and if necessary, read any welcome emails or quick-start guides you may have received from the provider.

You can also try switching servers. Choose to connect to a different server that's close to your physical location.

Another option: Try connecting with different protocols, assuming the VPN client allows you to change them. For example, you can use OpenVPN using TCP, then switch to L2TP and PPTP.

If you're still running into problems, other software programs may be the culprit. Sometimes, firewalls or security software can disrupt VPN connections. You can temporarily disable software

that might be causing the problem—just make sure to turn it back on once you connect so you don’t leave critical business systems vulnerable to attack.

Step 8: Fine-tune the connection

Once you have the basics out of the way, it's time for improvements. Make sure the settings you've applied to the VPN suit your business's needs.

For example, decide whether you'd like the VPN to run as soon as people start their devices. This may be a good idea if you need the protection of a VPN all the time—for example, if most people work outside the office. But if you think that you'll only need to use the VPN occasionally, you can set it to launch only when required, freeing up network resources for other uses.

Another fine-tuning option is to choose commonly used servers as your defaults or "favorites." This can save you a bit of time since you and other employees won't have to search for preferred servers every time you connect.

You may also want to turn on the "kill-switch" if your VPN provider offers it. The kill-switch is designed to prevent a device from sending or receiving data if the VPN becomes disconnected.

What is VCN in cloud?

Oracle virtual cloud networks (VCNs) provide customizable and private cloud networks in Oracle Cloud Infrastructure (OCI). Just like a traditional data center network, the VCN provides customers with complete control over their cloud networking environment.

What is VCN payment?

1. What are VCN accounts? VCN accounts are a 16-digit card number issued under the terms of our contract with Citibank that will be used to pay for hotel room and tax charges. Just like a traditional credit card number, but without the physical card, VCN accounts are transaction specific

Which two connectivity options can you use to give your virtual cloud network VCN access to the Internet?

You can use it with other Networking components and a router in your on-premises network to establish a connection by way of IPSec VPN or Oracle Cloud Infrastructure FastConnect. It can also provide a path for private network traffic between your VCN and another VCN in a different region.

Key differences between public and private IP addresses

The main difference between public and private IP addresses is how far they reach, and what they’re connected to. A public IP address identifies you to the wider internet so that all the information you’re searching for can find you. A private IP address is used within a private network to connect securely to other devices within that same network.

Each device within the same network has a unique private IP address.

Public and private IP address ranges

Your private IP address exists within specific private IP address ranges reserved by the Internet Assigned Numbers Authority (IANA) and should never appear on the internet. There are millions of private networks across the globe, all of which include devices assigned private IP addresses within these ranges:

Class A: 10.0.0.0 — 10.255.255.255

Class B: 172.16.0.0 — 172.31.255.255

Class C: 192.168.0.0 — 192.168.255.255

These might not seem like wide ranges, but they don't really need to be. Because these IP addresses are reserved for private network use only, they can be reused on different private networks all over the world — without consequence or confusion.

And don't be surprised if you have a device or two at home with a so-called 192 IP address, or a private IP address beginning with 192.168. This is the most common default private IP address format assigned to network routers around the globe.

Unsurprisingly, the public IP address range encompasses every number not reserved for the private IP range. Since a public IP address is a unique identifier for each device connected to the internet, it needs to be just that: unique.

Summarizing the differences between private and public IP addresses

Public IP address	Private IP address
External (global) reach	Internal (local) reach
Used for communicating outside your private network, over the internet	Used for communicating within your private network, with other devices in your home or office
A unique numeric code never reused by other devices	A non-unique numeric code that may be reused by other devices in other private networks
Found by Googling: "What is my IP address?"	Found via your device's internal settings
Assigned and controlled by your internet service provider	Assigned to your specific device within a private network
Not free	Free
Any number not included in the reserved private IP address range Example: 8.8.8.8.	10.0.0.0 — 10.255.255.255; 172.16.0.0 — 172.31.255.255; 192.168.0.0 — 192.168.255.255 Example: 10.11.12.13

How can I check which type of IP address I'm using?

When you connect to the internet, your private IP address is replaced with your ISP-assigned public IP address. This protects your private IP and other devices in your network, while also ensuring you can still connect online. Both types of IP addresses are important for your device's connection to the outside world — but how do you find them?

The easiest way to find your public IP address is to Google: "What is my IP address?" Depending on your ISP, you might see both an IPv4 and IPv6 address listed due to the increasing use of IPv6 addresses over IPv4. You can find your private IP address on Windows or macOS with a few quick clicks.

As you learn about private and public IP addresses, remember that they may change. If your ISP assigns you a dynamic IP address vs. a static IP address, for example, you might be subject to more network outages or connectivity issues in the long run.

And if you need to use a VPN to connect to the internet, your public IP address will change each time you connect — each new connection is encrypted to hide your IP address and keep prying eyes away.

Host Name: A host, or website, on the Internet is identified by a host name, such as www.example.com . Host names are sometimes called domain names. Host names are mapped to IP addresses, but a host name and an IP address do not have a one-to-one relationship. A host name is used when a web client makes an HTTP request to a host.

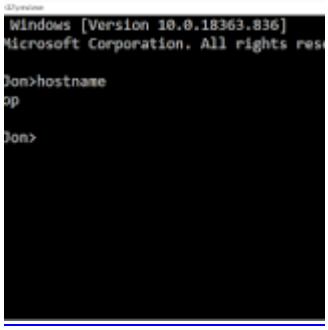
What is host name or IP address?

An IP address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. In contrast, a hostname is a label assigned to a network that sends the user to a specific website or a webpage. This is the main difference between IP address and Hostname

What is host name example?

On the Internet, a hostname is a domain name assigned to a host computer. For example, if Computer Hope had two computers on its network named "bart" and "homer," the domain name "bart.computerhope.com" is connecting to the "bart" computer.

What is host name on WIFI?



A hostname is a label assigned to a device (a host) on a network. It distinguishes one device from another on a specific network or over the internet. The hostname for a computer on a home network may be something like new laptop, Guest-Desktop, or FamilyPC

What is hostname in email address?

The hostname is a freely selectable name for a host. For example, you could call a server in a company network responsible for the central administration of emails “mail” or “mail123”

Is hostname same as server name?

Hostnames are unique identifiers that are used in different modes of communication such as the WWW or email in order to tell a device from another within a domain. Name servers, on the other hand, are fully qualified hostnames. These are basically the servers where you DNS information is actually stored.

How to determine your computer's hostname and hardware (MAC) address

In a network environment, nodes (network enabled equipment or objects on the network) have unique identifiers. The MAC address is the physical address of a network interface. It is unique at the hardware manufacturer level and SCS Computing Facilities utilizes these hardware addresses to uniquely allow access to our network.

Physical Address: Refers to the physical address of the Ethernet connection to your computer or server. This may also be referred to as your MAC (Media Access Control) Address, Host ID or Server ID. It is twelve characters long and is a combination of numbers (0–9) and letters (A–F, a–f). Your physical address is often presented in this format: XX-XX-XX-XX-XX-XX.

Each computer that has an IP address assigned on our network must also posses a hostname (also known as a Computer Name). There must not be to identical computer names within the same network.

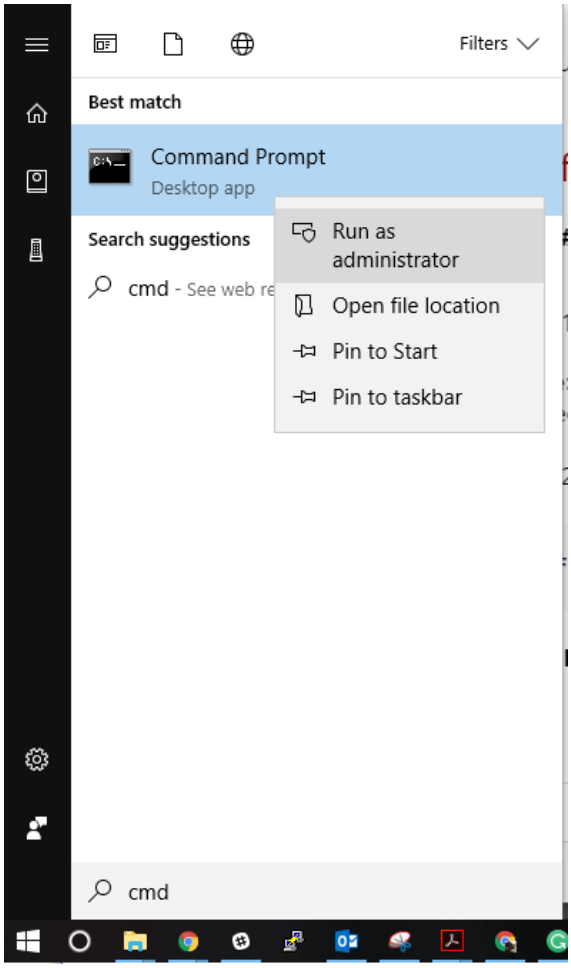
Note: Windows does not permit computer names that exceed 15 characters, and you cannot specify a DNS host name that differs from the NETBIOS host name

Host Name: The unique identifier that serves as name of your computer or server can be as long as 255 characters and consists of numbers and letters.

Below you will find the steps to identifying the hostname of your SCS computer.

Finding the hostname in Windows

Step 1: Click Start, search for cmd. Right click and select run as administrator. If prompted, confirm yes.



Note: If you do not have access to the Command Prompt, please contact your IT department or someone with administrative rights to your machine to help you locate the information.

Step 2: In the command prompt, type: ipconfig /all (then hit enter/return)

Your Host Name will appear at the top, under the section Windows IP Configuration.

C:\WINDOWS\system32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : hostname
Primary Dns Suffix . . . . . : andrew.ad.cmu.edu
Node Type . . . . . : Peer-Peer
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : scs.ad.cs.cmu.edu

Find the hardware address in Windows

Press the Start button, type cmd, then press Enter to start up a command shell

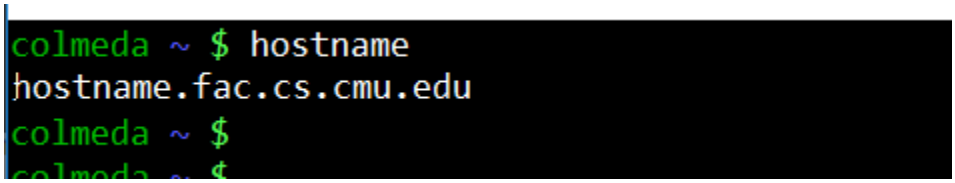
Type ipconfig /all

The hardware address will be listed under "Physical Address"

Finding the hostname in Linux

Step 1: Open the terminal (in Ubuntu, you can search for terminal).

Step 2: In the terminal, type: hostname (then hit enter/return)



userid ~ $ hostname
hostname.fac.cs.cmu.edu

Find the hardware address in Linux

Run /sbin/ifconfig -a

The hardware address for each Ethernet interface will be listed in the output after the string "HWaddr".

Find the hostname in macOS

Open the terminal (in macOS, you can search for terminal via spotlight).

In the terminal, type: hostname (then hit enter/return)

Find the Computer Name in macOS

Select "System Preferences" from the Apple Menu.

Select System Preferences

In System Preferences, open Sharing.

View the Computer Name field to confirm.

Find the hardware address in macOS

Select "System Preferences" from the Apple Menu.

Select Network

Select your Ethernet adapter from the menu on the left

Click the Advanced button

Click the Hardware tab

The hardware (MAC) address will be shown below.

Firewall:

What Firewalls Do?

A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can react quickly and seamlessly to detect and react to outside attacks across the whole network. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.

Why Do We Need Firewalls?

Firewalls, especially Next Generation Firewalls, focus on blocking malware and application-layer attacks. Along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls are able to react quickly and seamlessly to detect and combat attacks across the whole network. Firewalls can act on previously set policies to better protect your network and can carry out quick assessments to detect invasive or suspicious activity, such as malware, and shut it down. By leveraging a firewall for your security infrastructure, you're setting up your network with specific policies to allow or block incoming and outgoing traffic.

Network Layer vs. Application Layer Inspection

Network layer or packet filters inspect packets at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set where the source and destination of the rule set is based upon Internet Protocol (IP) addresses and ports. Firewalls that do network layer inspection perform better than similar devices that do application layer inspection. The downside is that unwanted applications or malware can pass over allowed ports, e.g. outbound Internet traffic over web protocols HTTP and HTTPS, port 80 and 443 respectively.

The Importance of NAT and VPN

Firewalls also perform basic network level functions such as Network Address Translation (NAT) and Virtual Private Network (VPN). Network Address Translation hides or translates internal client or server IP addresses that may be in a "private address range", as defined in RFC 1918 to a public IP address. Hiding the addresses of protected devices preserves the limited number of IPv4 addresses and is a defense against network reconnaissance since the IP address is hidden from the Internet.

Similarly, a virtual private network (VPN) extends a private network across a public network within a tunnel that is often encrypted where the contents of the packets are protected while traversing the Internet. This enables users to safely send and receive data across shared or public networks.

Next Generation Firewalls and Beyond

Next Generation Firewalls inspect packets at the application level of the TCP/IP stack and are able to identify applications such as Skype, or Facebook and enforce security policy based upon the type of application.

Today, UTM (Unified Threat Management) devices and Next Generation Firewalls also include threat prevention technologies such as intrusion prevention system (IPS) or Antivirus to detect and prevent malware and threats. These devices may also include sandboxing technologies to detect threats in files.

As the cyber security landscape continues to evolve and attacks become more sophisticated, Next Generation Firewalls will continue to be an essential component of any organization's security solution, whether you're in the data center, network, or cloud. To learn more about the essential capabilities your Next Generation Firewall needs to have, download the Next Generation Firewall (NGFW) Buyer's Guide today.

What are the 3 types of firewalls?

There are three basic types of firewalls that are used by companies to protect their data & devices to keep destructive elements out of network, viz. Packet Filters, Stateful Inspection and Proxy Server Firewalls. Let us give you a brief introduction about each of these.

Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18. 1.1 is allowed to reach destination 172.18. 2.1 over port 22."

What is firewall OS?

A firewall is a security device in the form of computer hardware or software. It can help protect your network by acting as an intermediary between your internal network and outside traffic. It monitors attempts to gain access to your operating system and blocks unwanted incoming traffic and unrecognized sources.

What are advantages of firewall?

Pros of firewall | Advantages of firewall:
A firewall prevents hackers and remote access. It protects data. Better security and network monitoring features. It ensures better privacy and security.

What is firewall in Java?

A firewall controls the flow of data between two or more networks, and manages the links between the networks. A firewall can consist of both hardware and software elements. ... You must configure the inner firewall to allow the HTTP server plug-in to communicate with the Application Server behind the firewall.

What is firewall in Linux?

A Linux firewall is a device that inspects Network traffic (Inbound /Outbound connections) and makes a decision to pass or filter out the traffic. Iptables is a CLI tool for managing firewall rules on a Linux machine. Network Security evolved with different types of Linux firewall in the era.

Load balancing:

Refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a server farm or server pool.

Modern high-traffic websites must serve hundreds of thousands, if not millions, of concurrent requests from users or clients and return the correct text, images, video, or application data, all in a fast and reliable manner. To cost-effectively scale to meet these high volumes, modern computing best practice generally requires adding more servers.

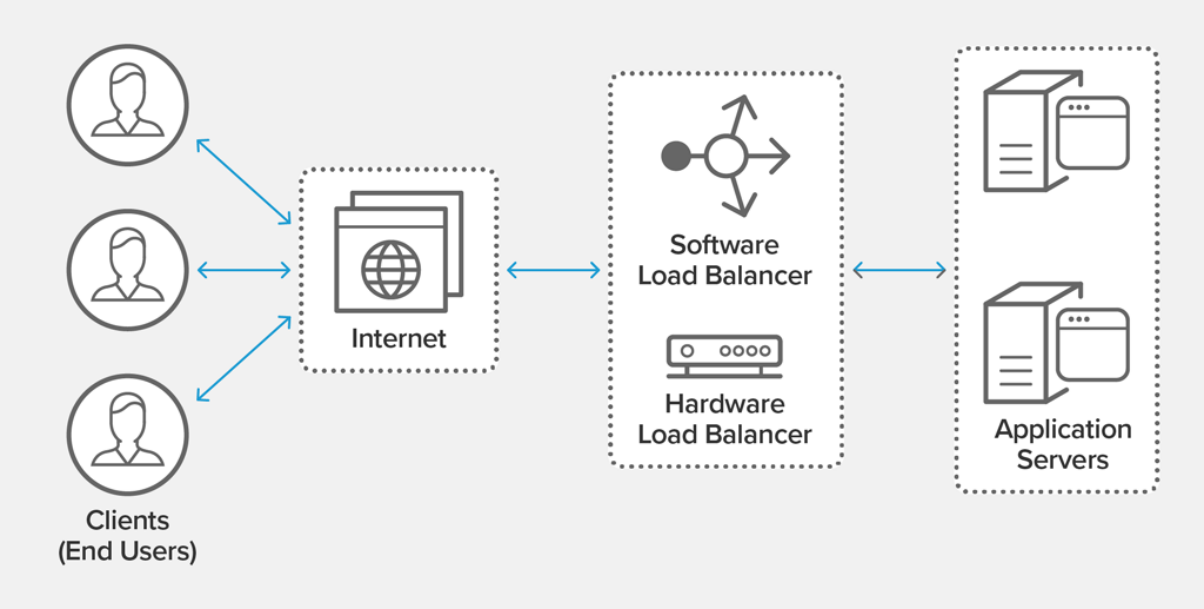
A load balancer acts as the “traffic cop” sitting in front of your servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it.

In this manner, a load balancer performs the following functions:

Distributes client requests or network load efficiently across multiple servers

Ensures high availability and reliability by sending requests only to servers that are online

Provides the flexibility to add or subtract servers as demand dictates



load balancing diagram

Load Balancing Algorithms

Different load balancing algorithms provide different benefits; the choice of load balancing method depends on your needs:

Round Robin – Requests are distributed across the group of servers sequentially.

Least Connections – A new request is sent to the server with the fewest current connections to clients. The relative computing capacity of each server is factored into determining which one has the least connections.

Least Time – Sends requests to the server selected by a formula that combines the fastest response time and fewest active connections. Exclusive to NGINX Plus.

Hash – Distributes requests based on a key you define, such as the client IP address or the request URL. NGINX Plus can optionally apply a consistent hash to minimize redistribution of loads if the set of upstream servers changes.

IP Hash – The IP address of the client is used to determine which server receives the request.

Random with Two Choices – Picks two servers at random and sends the request to the one that is selected by then applying the Least Connections algorithm (or for NGINX Plus the Least Time algorithm, if so configured).

Benefits of Load Balancing

Reduced downtime

Scalable

Redundancy

Flexibility

Efficiency

Classless Inter-Domain Routing (CIDR) explained

What is CIDR?

Classless Inter-Domain Routing (CIDR), also called supernetting, is a way to more flexibly allocate Internet Protocol (IP) addresses by creating unique and more granular identifiers for networks and individual devices. It was introduced in 1993 as an alternative to Internet routers that managed network traffic based on the class of IP addresses and determined subnetworks, for routing, based on IP address class.

The objective of CIDR was to address scalability issues with classful IP addresses which are based on three classes – Class A, Class B, and Class C. It is the capacity of each IP address class that creates scalability issues. Class A capacity is 16,581,375 IP addresses; Class B is 65,536 IP addresses; and Class C is 256 IP addresses. Using classful addressing led to inefficiencies in address use and routing, because of the rigid limitations of the classes (e.g., if 300 addresses were needed, Class B would be required leaving 16,281 unused). CIDR allows IP addresses to be variable and not bound by the size limitations of Classes A, B, and C.

Since it is not bound by Class, CIDR can organize IP addresses into subnetworks independent of the value of the addresses themselves. This is referred to as supernetting because CIDR effectively allows the aggregation of multiple subnets into a supernet for network routing. With this alternative to traditional subnetting, it is possible to specify the number of significant bits that make up the routing or networking portion by adding this to the IP address. This not only reduces wasted address space but also provides a flexible way to specify network addresses in routers.

Classless IP addresses, enabled by CIDR, are required when creating a Virtual Private Cloud (VPC) that is logically isolated from other virtual networks. When creating a VPC, a range of IPv4 addresses must be specified in the form of a CIDR.

What is CIDR example?

CIDR (Classless Inter-Domain Routing) notation is a compact method for specifying IP addresses and their routing suffixes. For example, we can express the idea that the IP address 192.168. 0.1 is associated with the netmask 255.255. 255.0 by using the CIDR notation of 192.168.

Why is CIDR important?

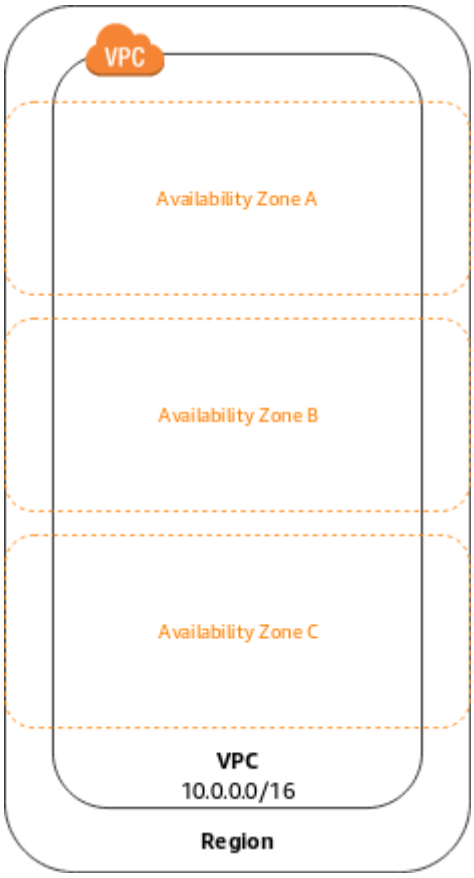
The initial goal of CIDR was to slow the increase of routing tables on routers across the internet and decrease the rapid exhaustion of IPv4 addresses. As a result, the number of available internet addresses has greatly increased

VPC basics

A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC.

When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. This is the primary CIDR block for your VPC. For more information about CIDR notation, see RFC 4632.

A VPC spans all of the Availability Zones in the Region. The following diagram shows a new VPC with an IPv4 CIDR block.



After you create a VPC, you can add one or more subnets in each Availability Zone.

Subnet basics

A subnet is a range of IP addresses in your VPC. You can launch AWS resources, such as EC2 instances, into a specific subnet. When you create a subnet, you specify the IPv4 CIDR block for the subnet, which is a subset of the VPC CIDR block. Each subnet must reside entirely within one Availability Zone and cannot span zones. By launching instances in separate Availability Zones, you can protect your applications from the failure of a single zone.

Note

You can optionally add subnets in a Local Zone, which is an AWS infrastructure deployment that places compute, storage, database, and other select services closer to your end users. A Local Zone enables your end users to run applications that require single-digit millisecond latencies. For more information, see Local Zones in the Amazon EC2 User Guide for Linux Instances.

Subnet types

When you create a subnet, depending on the configurations set for the VPC and the configurations you set for the subnet, you have the following IPv4 and IPv6 options:

IPv4-only: Your VPC is associated with an IPv4 CIDR or both IPv4 and IPv6 CIDRs. If the subnet CIDRs you choose are IPv4 CIDR ranges, any EC2 instances launched within the subnet will communicate over IPv4-only.

Dual-stack (IPv4 and IPv6): Your VPC is associated with an IPv4 CIDR or both IPv4 and IPv6 CIDRs. As a result, any subnets you create in the VPC can be dual-stack subnets. Any EC2 instances launched within the subnet will communicate over the IP of the subnet.

IPv6-only: Your VPC is associated with both IPv4 and IPv6 CIDRs. If you select the IPv6-only option when you create the subnet, any EC2 instances launched within the subnet will communicate over IPv6-only.

Depending on how you configure your VPC, subnets can be considered public, private, or VPN-only:

Public subnet: The subnet's IPv4 or IPv6 traffic is routed to an internet gateway or an egress-only internet gateway and can reach the public internet. For more information, see Enable public subnets to access the internet.

Private subnet: The subnet’s IPv4 or IPv6 traffic is not routed to an internet gateway or egress-only internet gateway and cannot reach the public internet.

VPN-only subnet: The subnet doesn't have a route to the internet gateway, but it has its traffic routed to a virtual private gateway for a Site-to-Site VPN connection. Currently, we do not support IPv6 traffic over a Site-to-Site VPN connection. For more information about Site-to-Site VPN, see What is AWS Site-to-Site VPN? in the AWS Site-to-Site VPN User Guide.

Note

Regardless of the type of subnet, the internal IPv4 address range of the subnet is always private—we do not announce the address block to the internet. For more information about private IP addressing in VPCs, see Modify the IP addressing behavior of your subnets.

Subnet settings

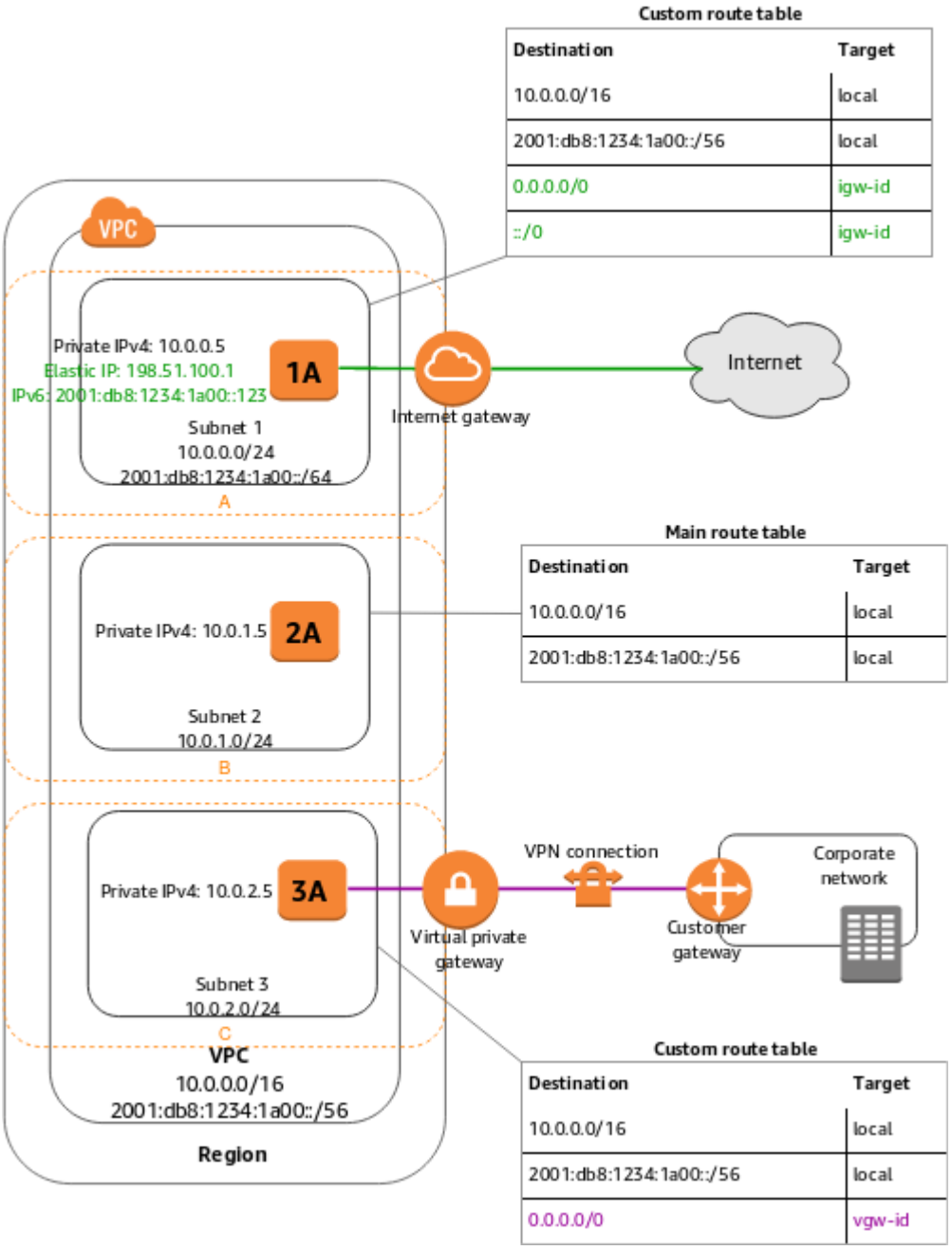
Once you create a subnet, you can modify the following settings for the subnet.

Auto-assign IP settings: Enables you to configure the auto-assign IP settings to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet. For more information about these settings, see Work with IP addresses.

Resource-based Name (RBN) settings: Enables you to specify the hostname type for EC2 instances in this subnet and configure how DNS A and AAAA record queries are handled. For more information about these settings, see Amazon EC2 instance hostname types in the Amazon EC2 User Guide for Linux Instances.

VPC and subnet diagram

The following diagram shows a VPC that has been configured with subnets in multiple Availability Zones.



Note the following:

1A, 2A, and 3A represent instances in your VPC.

Subnet 1 is a public subnet, subnet 2 is a private subnet, and subnet 3 is a VPN-only subnet.

An IPv6 CIDR block is associated with the VPC, and an IPv6 CIDR block is associated with subnet 1.

An internet gateway enables communication over the internet, and a virtual private network (VPN) connection enables communication with your corporate network.

Note

If you have an EC2 instance launched into a public subnet and you want the instance to communicate with the internet, it must have a public IPv4 address (or an Elastic IP address) or an

IPv6 address. For more information about public and private IP addressing for EC2 instances, see Amazon EC2 instance IP addressing in the Amazon EC2 User Guide for Linux Instances.

Additional resources

Create a subnet in your VPC

Create an IPv6-enabled VPC and IPv6-only subnets using the AWS CLI

VPC and subnet sizing

Amazon VPC supports IPv4 and IPv6 addressing, and has different CIDR block size quotas for each. By default, all VPCs and subnets must have IPv4 CIDR blocks—you can't change this behavior. You can optionally associate an IPv6 CIDR block with your VPC.

For more information about IP addressing, see Modify the IP addressing behavior of your subnets.

Contents

VPC and subnet sizing for IPv4

When you create a VPC, you must specify an IPv4 CIDR block for the VPC. The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses). After you've created your VPC, you can associate secondary CIDR blocks with the VPC. For more information, see Manage IPv4 CIDR blocks for a VPC.

When you create a VPC, we recommend that you specify a CIDR block from the private IPv4 address ranges as specified in RFC 1918:

RFC 1918 range	Example CIDR block
10.0.0.0 - 10.255.255.255 (10/8 prefix)	Your VPC must be /16 or smaller, for example, 10.0.0.0/16.
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)	Your VPC must be /16 or smaller, for example, 172.31.0.0/16.
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)	Your VPC can be smaller, for example 192.168.0.0/20.

You can create a VPC with a publicly routable CIDR block that falls outside of the private IPv4 address ranges specified in RFC 1918; however, for the purposes of this documentation, we refer to private IP addresses as the IPv4 addresses that are within the CIDR range of your VPC.

Note

If you're creating a VPC for use with another AWS service, check the service documentation to verify if there are specific requirements for the IP address range or networking components.

The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC), or a subset of the CIDR block for the VPC (for multiple subnets). The allowed block size is between a /28 netmask and /16 netmask. If you create more than one subnet in a VPC, the CIDR blocks of the subnets cannot overlap.

For example, if you create a VPC with CIDR block 10.0.0.0/24, it supports 256 IP addresses. You can break this CIDR block into two subnets, each supporting 128 IP addresses. One subnet uses CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other uses CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255).

There are tools available on the internet to help you calculate and create IPv4 subnet CIDR blocks. You can find tools that suit your needs by searching for terms such as 'subnet calculator' or 'CIDR calculator'. Your network engineering group can also help you determine the CIDR blocks to specify for your subnets.

The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

10.0.0.0: Network address.

10.0.0.1: Reserved by AWS for the VPC router.

10.0.0.2: Reserved by AWS. The IP address of the DNS server is the base of the VPC network range plus two. For VPCs with multiple CIDR blocks, the IP address of the DNS server is located in the primary CIDR. We also reserve the base of each subnet range plus two for all CIDR blocks in the VPC. For more information, see Amazon DNS server.

10.0.0.3: Reserved by AWS for future use.

10.0.0.255: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

If you create a VPC or subnet using a command line tool or the Amazon EC2 API, the CIDR block is automatically modified to its canonical form. For example, if you specify 100.68.0.18/18 for the CIDR block, we create a CIDR block of 100.68.0.0/18.

Manage IPv4 CIDR blocks for a VPC

You can associate secondary IPv4 CIDR blocks with your VPC. When you associate a CIDR block with your VPC, a route is automatically added to your VPC route tables to enable routing within the VPC (the destination is the CIDR block and the target is local).

In the following example, the VPC on the left has a single CIDR block (10.0.0.0/16) and two subnets. The VPC on the right represents the architecture of the same VPC after you've added a second CIDR block (10.2.0.0/16) and created a new subnet from the range of the second CIDR.

Destination	Target
10.0.0.0/16	local

Destination	Target
10.0.0.0/16	local
10.2.0.0/16	local

To add a CIDR block to your VPC, the following rules apply:

The allowed block size is between a /28 netmask and /16 netmask.

The CIDR block must not overlap with any existing CIDR block that's associated with the VPC.

There are restrictions on the ranges of IPv4 addresses you can use. For more information, see IPv4 CIDR block association restrictions.

You cannot increase or decrease the size of an existing CIDR block.

You have a quota on the number of CIDR blocks you can associate with a VPC and the number of routes you can add to a route table. You cannot associate a CIDR block if this results in you exceeding your quotas. For more information, see Amazon VPC quotas.

The CIDR block must not be the same or larger than a destination CIDR range in a route in any of the VPC route tables. For example, in a VPC where the primary CIDR block is 10.2.0.0/16, you have an

existing route in a route table with a destination of 10.0.0.0/24 to a virtual private gateway. You want to associate a secondary CIDR block in the 10.0.0.0/16 range. Because of the existing route, you cannot associate a CIDR block of 10.0.0.0/24 or larger. However, you can associate a secondary CIDR block of 10.0.0.0/25 or smaller.

If you've enabled your VPC for ClassicLink, you can associate CIDR blocks from the 10.0.0.0/16 and 10.1.0.0/16 ranges, but you cannot associate any other CIDR block from the 10.0.0.0/8 range.

The following rules apply when you add IPv4 CIDR blocks to a VPC that's part of a VPC peering connection:

If the VPC peering connection is active, you can add CIDR blocks to a VPC provided they do not overlap with a CIDR block of the peer VPC.

If the VPC peering connection is pending-acceptance, the owner of the requester VPC cannot add any CIDR block to the VPC, regardless of whether it overlaps with the CIDR block of the accepter VPC. Either the owner of the accepter VPC must accept the peering connection, or the owner of the requester VPC must delete the VPC peering connection request, add the CIDR block, and then request a new VPC peering connection.

If the VPC peering connection is pending-acceptance, the owner of the accepter VPC can add CIDR blocks to the VPC. If a secondary CIDR block overlaps with a CIDR block of the requester VPC, the VPC peering connection request fails and cannot be accepted.

If you're using AWS Direct Connect to connect to multiple VPCs through a Direct Connect gateway, the VPCs that are associated with the Direct Connect gateway must not have overlapping CIDR blocks. If you add a CIDR block to one of the VPCs that's associated with the Direct Connect gateway, ensure that the new CIDR block does not overlap with an existing CIDR block of any other associated VPC. For more information, see Direct Connect gateways in the AWS Direct Connect User Guide.

When you add or remove a CIDR block, it can go through various states: associating | associated | disassociating | disassociated | failing | failed. The CIDR block is ready for you to use when it's in the associated state.

You can disassociate a CIDR block that you've associated with your VPC; however, you cannot disassociate the CIDR block with which you originally created the VPC (the primary CIDR block). To view the primary CIDR for your VPC in the Amazon VPC console, choose Your VPCs, select the checkbox for your VPC, and choose the CIDRs tab. To view the primary CIDR using the AWS CLI, use the describe-vpcs command as follows. The primary CIDR is returned in the top-level CidrBlock element.

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d --query Vpcs[*].CidrBlock
```

The following is example output.

```
[
    "10.0.0.0/16",
]
```

IPv4 CIDR block association restrictions

The following table provides an overview of permitted and restricted CIDR block associations, which depend on the IPv4 address range in which your VPC's primary CIDR block resides.

IP address range of the primary CIDR block	Restricted associations	Permitted associations
10.0.0.0/8	CIDR blocks from other RFC 1918* ranges (172.16.0.0/12 and 192.168.0.0/16). If your primary CIDR block is from the 10.0.0.0/15 range (10.0.0.0 to 10.1.255.255), you cannot add a CIDR block from the 10.0.0.0/16 range (10.0.0.0 to 10.0.255.255). CIDR blocks from the 198.19.0.0/16 range.	Any other CIDR block from the 10.0.0.0/8 range that's not restricted. Any publicly routable IPv4 CIDR block (non-RFC 1918), or a CIDR block from the 100.64.0.0/10 range.
172.16.0.0/12	CIDR blocks from other RFC 1918* ranges (10.0.0.0/8 and 192.168.0.0/16). CIDR blocks from the 172.31.0.0/16 range. CIDR blocks from the 198.19.0.0/16 range.	Any other CIDR block from the 172.16.0.0/12 range that's not restricted. Any publicly routable IPv4 CIDR block (non-RFC 1918), or a CIDR block from the 100.64.0.0/10 range.
192.168.0.0/16	CIDR blocks from other RFC 1918* ranges (10.0.0.0/8 and 172.16.0.0/12). CIDR blocks from the 198.19.0.0/16 range.	Any other CIDR block from the 192.168.0.0/16 range. Any publicly routable IPv4 CIDR block (non-RFC 1918), or a CIDR block from the 100.64.0.0/10 range.
198.19.0.0/16	CIDR blocks from the RFC 1918* ranges.	Any publicly routable IPv4 CIDR block (non-RFC 1918), or a CIDR block from the 100.64.0.0/10 range.
Publicly routable CIDR block (non-RFC 1918), or a CIDR block from the 100.64.0.0/10 range	CIDR blocks from the RFC 1918* ranges. CIDR blocks from the 198.19.0.0/16 range.	Any other publicly routable IPv4 CIDR block (non-RFC 1918), or a CIDR block from the 100.64.0.0/10 range.

* RFC 1918 ranges are the private IPv4 address ranges specified in RFC 1918.

VPC and subnet sizing for IPv6

You can associate a single IPv6 CIDR block with an existing VPC in your account, or when you create a new VPC. The CIDR block is a fixed prefix length of /56. You can request an IPv6 CIDR block from Amazon's pool of IPv6 addresses.

If you've associated an IPv6 CIDR block with your VPC, you can associate an IPv6 CIDR block with an existing subnet in your VPC, or when you create a new subnet. A subnet's IPv6 CIDR block is a fixed prefix length of /64.

For example, you create a VPC and specify that you want to associate an Amazon-provided IPv6 CIDR block with the VPC. Amazon assigns the following IPv6 CIDR block to your VPC: 2001:db8:1234:1a00::/56. You cannot choose the range of IP addresses yourself. You can create a subnet and associate an IPv6 CIDR block from this range; for example, 2001:db8:1234:1a00::/64.

There are tools available on the internet to help you calculate and create IPv6 subnet CIDR blocks; for example, IPv6 Address Planner. You can find other tools that suit your needs by searching for terms such as 'IPv6 subnet calculator' or 'IPv6 CIDR calculator'. Your network engineering group can also help you determine the IPv6 CIDR blocks to specify for your subnets.

You can disassociate an IPv6 CIDR block from a subnet, and you can disassociate an IPv6 CIDR block from a VPC. After you've disassociated an IPv6 CIDR block from a VPC, you cannot expect to receive the same CIDR if you associate an IPv6 CIDR block with your VPC again later.

The first four IPv6 addresses and the last IPv6 address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block 2001:db8:1234:1a00/64, the following five IP addresses are reserved:

2001:db8:1234:1a00::

2001:db8:1234:1a00::1

2001:db8:1234:1a00::2

2001:db8:1234:1a00::3

2001:db8:1234:1a00:ffff:ffff:ffff:ffff

Subnet routing

Each subnet must be associated with a route table, which specifies the allowed routes for outbound traffic leaving the subnet. Every subnet that you create is automatically associated with the main route table for the VPC. You can change the association, and you can change the contents of the main route table. For more information, see Managing route tables for your VPC.

In the previous diagram, the route table associated with subnet 1 routes all IPv4 traffic (0.0.0.0/0) and IPv6 traffic (::/0) to an internet gateway (for example, igw-1a2b3c4d). Because instance 1A has an IPv4 Elastic IP address and an IPv6 address, it can be reached from the internet over both IPv4 and IPv6.

Note

(IPv4 only) The Elastic IPv4 address or public IPv4 address that's associated with your instance is accessed through the internet gateway of your VPC. Traffic that goes through an AWS Site-to-Site

VPN connection between your instance and another network traverses a virtual private gateway, not the internet gateway, and therefore does not access the Elastic IPv4 address or public IPv4 address.

The instance 2A can't reach the internet, but can reach other instances in the VPC. You can allow an instance in your VPC to initiate outbound connections to the internet over IPv4 but prevent unsolicited inbound connections from the internet using a network address translation (NAT) gateway or instance. Because you can allocate a limited number of Elastic IP addresses, we recommend that you use a NAT device if you have more instances that require a static public IP address. For more information, see Enable private subnets to access the internet with NAT devices. To initiate outbound-only communication to the internet over IPv6, you can use an egress-only internet gateway. For more information, see Enable outbound traffic only from subnets using egress-only internet gateways.

The route table associated with subnet 3 routes all IPv4 traffic (0.0.0.0/0) to a virtual private gateway (for example, vgw-1a2b3c4d). Instance 3A can reach computers in the corporate network over the Site-to-Site VPN connection.

Subnet security

AWS provides two features that you can use to increase security in your VPC: security groups and network ACLs. Security groups control inbound and outbound traffic for your instances, and network ACLs control inbound and outbound traffic for your subnets. In most cases, security groups can meet your needs; however, you can also use network ACLs if you want an additional layer of security for your VPC. For more information, see Internetwork traffic privacy in Amazon VPC.

By design, each subnet must be associated with a network ACL. Every subnet that you create is automatically associated with the VPC's default network ACL. You can change the association, and you can change the contents of the default network ACL. For more information, see Control traffic to subnets with Network ACLs.

You can create a flow log on your VPC or subnet to capture the traffic that flows to and from the network interfaces in your VPC or subnet. You can also create a flow log on an individual network interface. Flow logs are published to CloudWatch Logs or Amazon S3. For more information, see Logging IP traffic with VPC Flow Logs.

What is a port in network?

In computer networking, a port is a communication endpoint. ... It completes the destination or origination network address of a message. Specific port numbers are reserved to identify specific services so that an arriving packet can be easily forwarded to a running application.

There are different types of ports available:

Serial port.

Parallel port.

USB port.

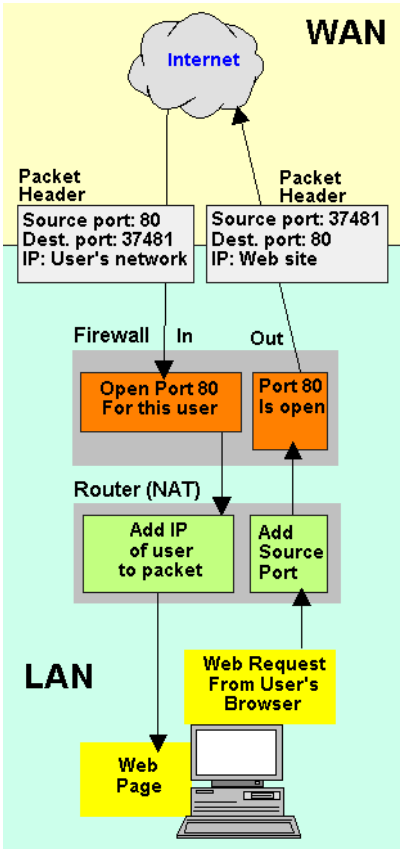
PS/2 port.

VGA port.

Modem port.

FireWire Port.

Sockets.



What is a port?

A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection.

What is a port number?

Ports are standardized across all network-connected devices, with each port assigned a number. Most ports are reserved for certain protocols — for example, all Hypertext Transfer Protocol (HTTP) messages go to port 80. While IP addresses enable messages to go to and from specific devices, port numbers allow targeting of specific services or applications within those devices.

How do ports make network connections more efficient?

Vastly different types of data flow to and from a computer over the same network connection. The use of ports helps computers understand what to do with the data they receive.

Suppose Bob transfers an MP3 audio recording to Alice using the File Transfer Protocol (FTP). If Alice's computer passed the MP3 file data to Alice's email application, the email application would not know how to interpret it. But because Bob's file transfer uses the port designated for FTP (port 21), Alice's computer is able to receive and store the file.

Meanwhile, Alice's computer can simultaneously load HTTP webpages using port 80, even though both the webpage files and the MP3 sound file flow to Alice's computer over the same WiFi connection.

Are ports part of the network layer?

The OSI model is a conceptual model of how the Internet works. It divides different Internet services and processes into 7 layers. These layers are:

Ports are a transport layer (layer 4) concept. Only a transport protocol such as the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) can indicate which port a packet should go to. TCP and UDP headers have a section for indicating port numbers. Network layer protocols — for instance, the Internet Protocol (IP) — are unaware of what port is in use in a given network connection. In a standard IP header, there is no place to indicate which port the data packet should go to. IP headers only indicate the destination IP address, not the port number at that IP address.

Usually, the inability to indicate the port at the network layer has no impact on networking processes, since network layer protocols are almost always used in conjunction with a transport layer protocol. However, this does impact the functionality of testing software, which is software that "pings" IP addresses using Internet Control Message Protocol (ICMP) packets. ICMP is a network layer protocol that can ping networked devices — but without the ability to ping specific ports, network administrators cannot test specific services within those devices.

Some ping software, such as My Traceroute, offers the option to send UDP packets. UDP is a transport layer protocol that can specify a particular port, as opposed to ICMP, which cannot specify a port. By adding a UDP header to ICMP packets, network administrators can test specific ports within a networked device.

Why do firewalls sometimes block specific ports?

A firewall is a security system that blocks or allows network traffic based on a set of security rules. Firewalls usually sit between a trusted network and an untrusted network; often the untrusted network is the Internet. For example, office networks often use a firewall to protect their network from online threats.

Some attackers try to send malicious traffic to random ports in the hopes that those ports have been left "open," meaning they are able to receive traffic. This action is somewhat like a car thief walking down the street and trying the doors of parked vehicles, hoping one of them is unlocked. For this reason, firewalls should be configured to block network traffic directed at most of the available ports. There is no legitimate reason for the vast majority of the available ports to receive traffic.

Properly configured firewalls block traffic to all ports by default except for a few predetermined ports known to be in common use. For instance, a corporate firewall could only leave open ports 25 (email), 80 (web traffic), 443 (web traffic), and a few others, allowing internal employees to use these essential services, then block the rest of the 65,000+ ports.

As a more specific example, attackers sometimes attempt to exploit vulnerabilities in the RDP protocol by sending attack traffic to port 3389. To stop these attacks, a firewall may block port 3389 by default. Since this port is only used for remote desktop connections, such a rule has little impact on day-to-day business operations unless employees need to work remotely.

What are the different port numbers?

There are 65,535 possible port numbers, although not all are in common use. Some of the most commonly used ports, along with their associated networking protocol, are:

Ports 20 and 21: File Transfer Protocol (FTP). FTP is for transferring files between a client and a server.

Port 22: Secure Shell (SSH). SSH is one of many tunneling protocols that create secure network connections.

Port 25: Simple Mail Transfer Protocol (SMTP). SMTP is used for email.

Port 53: Domain Name System (DNS). DNS is an essential process for the modern Internet; it matches human-readable domain names to machine-readable IP addresses, enabling users to load websites and applications without memorizing a long list of IP addresses.

Port 80: Hypertext Transfer Protocol (HTTP). HTTP is the protocol that makes the World Wide Web possible.

Port 123: Network Time Protocol (NTP). NTP allows computer clocks to sync with each other, a process that is essential for encryption.

Port 179: Border Gateway Protocol (BGP). BGP is essential for establishing efficient routes between the large networks that make up the Internet (these large networks are called autonomous systems). Autonomous systems use BGP to broadcast which IP addresses they control.

Port 443: HTTP Secure (HTTPS). HTTPS is the secure and encrypted version of HTTP. All HTTPS web traffic goes to port 443. Network services that use HTTPS for encryption, such as DNS over HTTPS, also connect at this port.

Port 500: Internet Security Association and Key Management Protocol (ISAKMP), which is part of the process of setting up secure IPsec connections.

Port 3389: Remote Desktop Protocol (RDP). RDP enables users to remotely connect to their desktop computers from another device.

What Are the Top File Transfer Protocols?

1. FTP

The original file transfer protocol, FTP, is a popular file transfer method that has been around for decades. FTP exchanges data using two separate channels known as the command channel to authenticate the user, and the data channel to transfer the files.

With FTP, both channels are unencrypted, leaving any data sent over these channels vulnerable to being taken advantage of. However, it does require an authenticated username and password for access.

Related Reading: Replace Your FTP Scripts to Increase Security

2. FTPS

Short for FTP over SSL/TLS (Secure Sockets Layer/ Transport Layer Security), FTPS is a secure file transfer protocol that allows you to transfer files securely with trading partners, customers, and users. The transfers can be authenticated through FTPS-supported methods like client certificates, server certificates, and passwords.

Related Reading: SFTP vs. FTPS: The Key Differences

3. SFTP

SFTP stands for FTP over SSH (Secure Shell). It is a secure FTP protocol and a great alternative to unsecure FTP tools or manual scripts. SFTP exchanges data over an SSH connection and provides organizations with a high level of protection for file transfers shared between their systems, trading partners, employees, and the cloud.

Related Reading: Are SFTP and FTP the Same?

Request a Demo

4. SCP

An older protocol, SCP or Secure Copy Protocol, is a network protocol that supports file transfers between hosts on a computer network. It's somewhat similar to FTP, however, SCP supports encryption and authentication features.

Related Reading: SCP vs. SFTP: Which is Better?

5. HTTP & HTTPS

As the backbone of the WWW (World Wide Web), HTTP (Hyper Text Transfer Protocol) is the foundation of data communication. It defines the format of messages through which web browsers and web servers communicate and defines how a web browser should response to a web request. HTTP uses TCP (Transmission Control Protocol) as an underlying transport and is a stateless protocol. This means each command is executed independently and no session information is retained by the receiver.

HTTPS (Hyper Text Transfer Protocol Secure) is the secure version of HTTP where communications are encrypted by TLS or SSL.

Related Reading: Comparing Transfer Methods: HTTP vs. FTP

6. AS2, AS3, & AS4

AS2, AS3, and AS4 (Applicability Statement 2, 3, and 4) are all popular protocols used to send and secure critical file transfers.

AS2 is used to transmit sensitive data securely and reliably over the internet. AS2 utilizes digital certificates and encryption standards to protect critical information while it's in transit across systems, networks, and locations. AS2 messages can be compressed, signed, encrypted, and sent over a secure SSL tunnel.

AS3 is a standard that can be used to transmit virtually any file type. It provides a layer of security for data transmission through digital signatures and data encryption. It was created initially to transfer data files like XML and EDI documents for business-to-business data. Unlike AS2, which is a defined transfer protocol, AS3 is a message standard and focuses on how a message should be formatted when transmitting from server to server. Once an AS3 message has been composed, it can be transmitted via any other protocol (FTP, SFTP, HTTPS, etc.) as long as both parties can access the location in which the message has been placed.

AS4 is a protocol that allows businesses to securely exchange data with their partners. It builds on the foundations originally set by AS2 but works with web services and provides improved delivery notifications. As a business-to-business standard, AS4 helps make exchanging documents over the internet secure and simple.

Related Reading: What's the Difference Between AS2, AS3, and AS4?

7. PeSIT

PeSIT, short for Protocol d'Echanges pour un Systeme Interbancaire de Telecompensation, is an end-to-end file transfer protocol that was developed in by the French Interbank Teleclearing Systems Economic Interest Grouping (GSIT). It's less widely used in North America and is primarily used to meet European banking standards and transfer communications to and from banks in Europe.

Top Protocols For Secure File Transfer

The original File Transfer Protocol established an easy method for transferring files over a network. But FTP was designed in the 1970s, long before data security was much of a concern. FTP is still around, but its usage has drastically diminished with the introduction of secure file transfer protocols.

So what is a secure file transfer protocol? Most people will answer SFTP, which is half the answer. Basically, whereas FTP is known as an insecure protocol because it doesn't provide encryption, secure file transfer protocols do.

SSH File Transfer Protocol (SFTP)

SFTP is a protocol developed by the Internet Engineering Task Force (IETF), and is perhaps the most common file transfer protocol in use today. SFTP is built on Secure Shell cryptography to encrypt data being transferred. This encryption is done in part by transferring information in packets as opposed to plain text, which generally leads to faster transmission times when compared to FTP. SFTP supports the use of key pairs as well as host-based authentication, making SFTP useful for sensitive data such as personally information.

File Transfer Protocol Over SSL (FTPS)

FTPS is an attempt to make FTP secure using Secure Sockets Layer (SSL). SSL however was deprecated in 2015 so even though most FTPS servers are using Transport Layer Security (TLS), we still refer to it as FTPS. TLS uses certificates to authenticate users and to prevent information from being accessed by unauthorized parties. FTPS requires two ports on the client server which can make it more difficult to get FTPS transfers through a firewall. There is also explicit FTPS (FTPES) which provides extra functionality for secure file sharing.

Applicability Statement 2 (AS2)

The AS2 protocol is widely used between trading partners in the retail and automotive industries. AS2 is based on S/MIME and HTTPS for sending encrypted messages. AS2 also enables digital signatures and Message Disposition Notification (MDN), which provide the sender with receipts for non-repudiation.

ODETTE File Transfer Protocol 2 (OFTP2)

OFTP2 is a TCP/IP protocol that is popular among automotive companies, especially those based in Europe. OFTP2, much like AS2, supports non-repudiation through receipts. Importantly, OFTP2 can compress large amounts of data, making OFTP2 an efficient means of transferring large files. The original OFTP was introduced in 1986 by the Organisation for Data Exchange by Tele-Transmission in Europe (ODETTE).

Additionally, OFTP2 can operate through Value Added Networks (VANs), with both push and pull modes.

User Datagram Protocol (UDP)

UDP is a transport layer protocol similar to TCP. UDP however doesn't include much of the "overhead" implied by other protocols, such as handshakes, certificates or receipts. This makes UDP a much faster method of sending data such as video or audio files, especially when transfers are occurring over long-distance networks that are experiencing high-latency. That speed however comes with noticeable drawbacks, including packet loss.

What is a DMZ in networking?

In computer networks, a DMZ, or demilitarized zone, is a physical or logical subnet that separates a local area network (LAN) from other untrusted networks -- usually, the public internet. DMZs are also known as perimeter networks or screened subnetworks.

Any service provided to users on the public internet should be placed in the DMZ network. External-facing servers, resources and services are usually located there. Some of the most common of these services include web, email, domain name system, File Transfer Protocol and proxy servers.

Servers and resources in the DMZ are accessible from the internet, but the rest of the internal LAN remains unreachable. This approach provides an additional layer of security to the LAN as it restricts a hacker's ability to directly access internal servers and data from the internet.

Hackers and cybercriminals can reach the systems running services on DMZ servers. Those servers must be hardened to withstand constant attack. The term DMZ comes from the geographic buffer zone that was set up between North Korea and South Korea at the end of the Korean War.

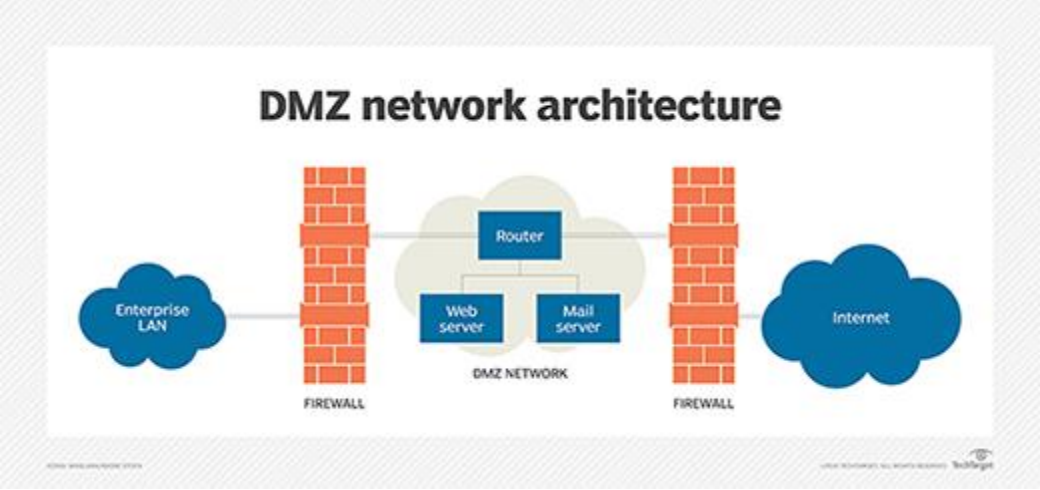
Why are DMZs important?

DMZs provide a level of network segmentation that helps protect internal corporate networks. These subnetworks restrict remote access to internal servers and resources, making it difficult for attackers to access the internal network. This strategy is useful for both individual use and large organizations.

Businesses place applications and servers that are exposed to the internet in a DMZ, separating them from the internal network. The DMZ isolates these resources so, if they are compromised, the attack is unlikely to cause exposure, damage or loss.

How does a DMZ work?

DMZs function as a buffer zone between the public internet and the private network. The DMZ subnet is deployed between two firewalls. All inbound network packets are then screened using a firewall or other security appliance before they arrive at the servers hosted in the DMZ.



A network DMZ sits between two firewalls, creating a semisafe buffer zone between the internet and the enterprise LAN.

If better-prepared threat actors pass through the first firewall, they must then gain unauthorized access to the services in the DMZ before they can do any damage. Those systems are likely to be hardened against such attacks.

Finally, assuming well-resourced threat actors take over a system hosted in the DMZ, they must still break through the internal firewall before they can reach sensitive enterprise resources. Determined attackers can breach even the most secure DMZ architecture. However, a DMZ under attack will set off alarms, giving security professionals enough warning to avert a full breach of their organization.

What are the benefits of using a DMZ?

The primary benefit of a DMZ is that it offers users from the public internet access to certain secure services, while maintaining a buffer between those users and the private internal network. There are several security benefits from this buffer, including the following:

Access control. A DMZ network provides access control to services outside an organization's network perimeters that are accessed from the internet. It simultaneously introduces a level of network segmentation that increases the number of obstacles a user must bypass before gaining access to an organization's private network. In some cases, a DMZ includes a proxy server, which centralizes the flow of internal -- usually, employee -- internet traffic and makes recording and monitoring that traffic simpler.

Network reconnaissance prevention. A DMZ also prevents an attacker from being able to scope out potential targets within the network. Even if a system within the DMZ is compromised, the internal firewall still protects the private network, separating it from the DMZ. This setup makes external active reconnaissance more difficult. Although the servers in the DMZ are publicly exposed, they are backed by another layer of protection. The public face of the DMZ keeps attackers from seeing the contents of the internal private network. If attackers do manage to compromise the servers within the DMZ, they are still isolated from the private network by the DMZ's internal barrier.

Protection against Internet Protocol (IP) spoofing. In some cases, attackers attempt to bypass access control restrictions by spoofing an authorized IP address to impersonate another device on the network. A DMZ can stall potential IP spoofers, while another service on the network verifies the IP address's legitimacy by testing whether it is reachable.

What DMZs are used for

DMZ networks have been an important part of enterprise network security for almost as long as firewalls have been in use. They are deployed for similar reasons: to protect sensitive organizational systems and resources. DMZ networks are often used for the following:

isolate and keep potential target systems separate from internal networks;

reduce and control access to those systems by external users; and

host corporate resources to make some of them available to authorized external users.

More recently, enterprises have opted to use virtual machines or containers to isolate parts of the network or specific applications from the rest of the corporate environment. Cloud technologies have largely removed the need for many organizations to have in-house web servers. Many of the external facing infrastructure once located in the enterprise DMZ has migrated to the cloud, such as software-as-a service apps.

Architecture and design of DMZ networks

There are various ways to design a network with a DMZ. The two basic methods are to use either one or two firewalls, though most modern DMZs are designed with two firewalls. This approach can be expanded to create more complex architectures.

A single firewall with at least three network interfaces can be used to create a network architecture containing a DMZ. The external network is formed by connecting the public internet -- via an internet service provider connection -- to the firewall on the first network interface. The internal network is formed from the second network interface, and the DMZ network itself is connected to the third network interface.

Different sets of firewall rules for monitoring traffic between the internet and the DMZ, the LAN and the DMZ, and the LAN and the internet tightly control which ports and types of traffic are allowed into the DMZ from the internet, limit connectivity to specific hosts in the internal network and prevent unrequested connections either to the internet or the internal LAN from the DMZ.

The more secure approach to creating a DMZ network is a dual-firewall configuration, in which two firewalls are deployed with the DMZ network positioned between them. The first firewall -- also called the perimeter firewall -- is configured to allow only external traffic destined for the DMZ. The second, or internal, firewall only allows traffic from the DMZ to the internal network.

The dual-firewall approach is considered more secure because two devices must be compromised before an attacker can access the internal LAN. Security controls can be tuned specifically for each network segment. For example, a network intrusion detection and intrusion prevention system located in a DMZ could be configured to block all traffic except Hypertext Transfer Protocol Secure requests to Transmission Control Protocol port 443.

Examples of DMZs

Some of the various ways DMZs are used include the following:

Cloud services. Some cloud services, such as Microsoft Azure, use a hybrid security approach in which a DMZ is implemented between an organization's on-premises network and the virtual network. This method is typically used in situations where the organization's applications run partly on premises and partly on the virtual network. It's also used where outgoing traffic must be audited or where granular traffic control is required in between the virtual network and the on-premises data center.

Home networks. A DMZ can also be useful in a home network in which computers and other devices are connected to the internet using a broadband router and configured into a LAN. Some home routers include a DMZ host feature. This can be contrasted with the DMZ subnetwork used in organizations with many more devices than would be found in a home. The DMZ host feature designates one device on the home network to function outside of the firewall, where it acts as the DMZ while the rest of the home network lies inside the firewall. In some cases, a gaming console is chosen to be the DMZ host so that the firewall doesn't interfere with gaming. Also, the console is a good candidate for a DMZ host because it likely holds less sensitive information than a personal computer.

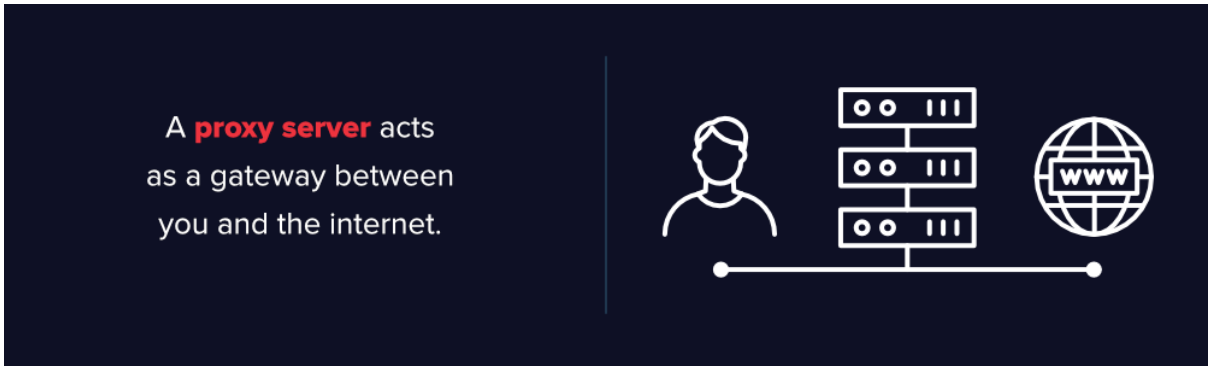
Industrial control systems (ICS). DMZs provide a potential solution to the security risks of ICSes. Industrial equipment, such as turbine engines, or ICSes are being merged with information technology (IT), which makes production environments smarter and more efficient, but it also

creates a larger threat surface. Much of the industrial or operational technology (OT) equipment connecting to the internet is not designed to handle attacks in the same way IT devices are. A DMZ can provide increased network segmentation that can make it harder for ransomware or other network threats to bridge the gap between IT systems and their more vulnerable OT counterparts.

What's a Proxy Server?

A proxy server acts as a gateway between you and the internet. It's an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.

If you're using a proxy server, internet traffic flows through the proxy server on its way to the address you requested. The request then comes back through that same proxy server (there are exceptions to this rule), and then the proxy server forwards the data received from the website to you.



If that's all it does, why bother with a proxy server? Why not just go straight from to the website and back?

Modern proxy servers do much more than forwarding web requests, all in the name of data security and network performance. Proxy servers act as a firewall and web filter, provide shared network connections, and cache data to speed up common requests. A good proxy server keeps users and the internal network protected from the bad stuff that lives out in the wild internet. Lastly, proxy servers can provide a high level of privacy.

How Does a Proxy Server Operate?

Every computer on the internet needs to have a unique Internet Protocol (IP) Address. Think of this IP address as your computer's street address. Just as the post office knows to deliver your mail to your street address, the internet knows how to send the correct data to the correct computer by the IP address.

A proxy server is basically a computer on the internet with its own IP address that your computer knows. When you send a web request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the web server, and forwards you the web page data so you can see the page in your browser.

When the proxy server forwards your web requests, it can make changes to the data you send and still get you the information that you expect to see. A proxy server can change your IP address, so the web server doesn't know exactly where you are in the world. It can encrypt your data, so your

data is unreadable in transit. And lastly, a proxy server can block access to certain web pages, based on IP address.

Why Should You Use a Proxy Server?

There are several reasons organizations and individuals use a proxy server.

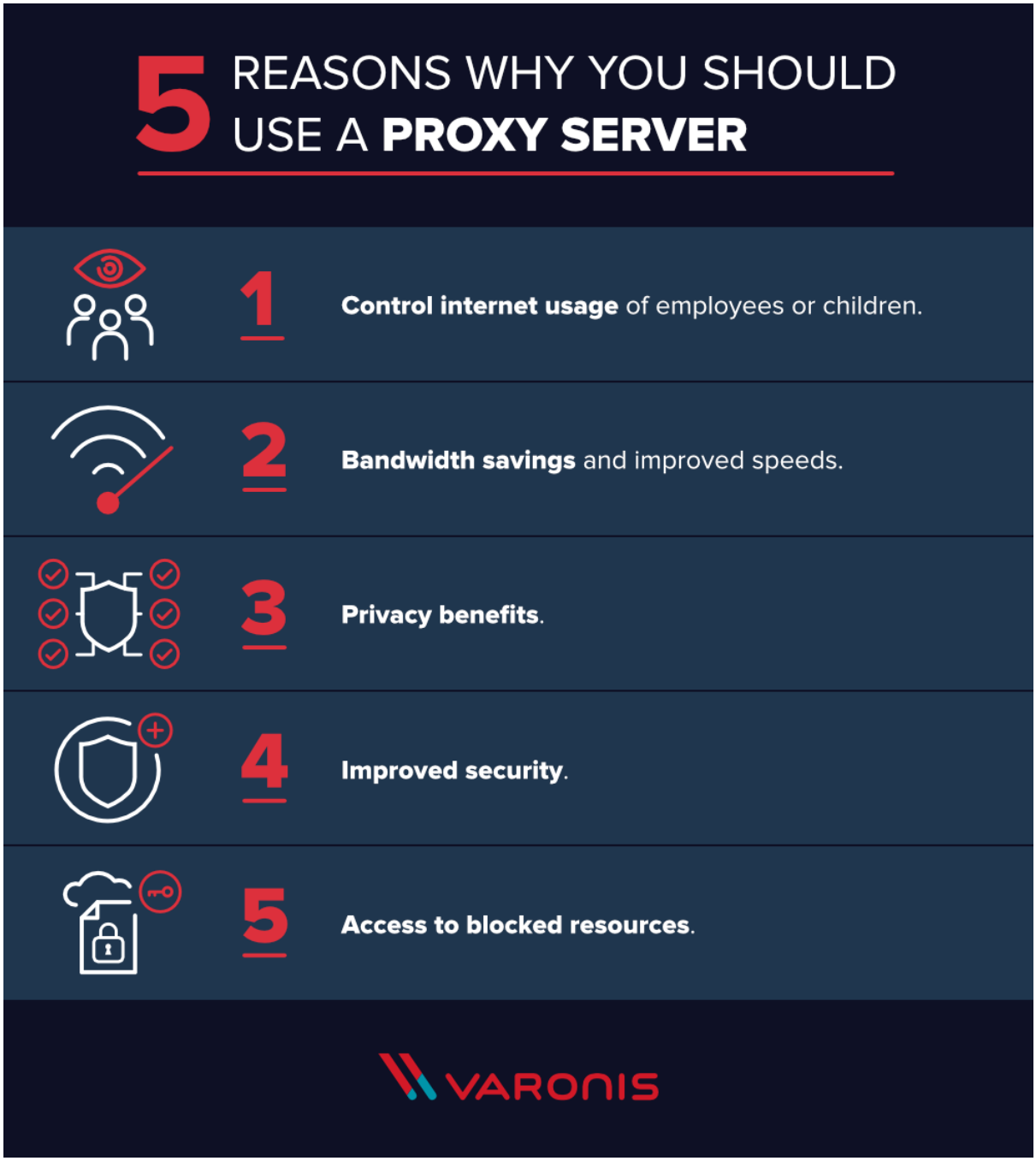
To control internet usage of employees and children: Organizations and parents set up proxy servers to control and monitor how their employees or kids use the internet. Most organizations don't want you looking at specific websites on company time, and they can configure the proxy server to deny access to specific sites, instead of redirecting you with a nice note asking you to refrain from looking at said sites on the company network. They can also monitor and log all web requests, so even though they might not block the site, they know how much time you spend cyberloafing.

Bandwidth savings and improved speeds: Organizations can also get better overall network performance with a good proxy server. Proxy servers can cache (save a copy of the website locally) popular websites – so when you ask for www.varonis.com, the proxy server will check to see if it has the most recent copy of the site, and then send you the saved copy. What this means is that when hundreds of people hit www.varonis.com at the same time from the same proxy server, the proxy server only sends one request to varonis.com. This saves bandwidth for the company and improves the network performance.

Privacy benefits: Individuals and organizations alike use proxy servers to browse the internet more privately. Some proxy servers will change the IP address and other identifying information the web request contains. This means the destination server doesn't know who actually made the original request, which helps keeps your personal information and browsing habits more private.

Improved security: Proxy servers provide security benefits on top of the privacy benefits. You can configure your proxy server to encrypt your web requests to keep prying eyes from reading your transactions. You can also prevent known malware sites from any access through the proxy server. Additionally, organizations can couple their proxy server with a Virtual Private Network (VPN), so remote users always access the internet through the company proxy. A VPN is a direct connection to the company network that companies provide to external or remote users. By using a VPN, the company can control and verify that their users have access to the resources (email, internal data) they need, while also providing a secure connection for the user to protect the company data.

Get access to blocked resources: Proxy servers allow users to circumvent content restrictions imposed by companies or governments. Is the local sportsball team's game blacked out online? Log into a proxy server on the other side of the country and watch from there. The proxy server makes it look like you are in California, but you actually live in North Carolina. Several governments around the world closely monitor and restrict access to the internet, and proxy servers offer their citizens access to an uncensored internet.



Now that you have an idea about why organizations and individuals use a proxy server, take a look at the risks below.

Proxy Server Risks

You do need to be cautious when you choose a proxy server: a few common risks can negate any of the potential benefits:

Free proxy server risks

You know the old saying “you get what you pay for?” Well, using one of the many free proxy server services can be quite risky, even the services using ad-based revenue models.

Free usually means they aren't investing heavily in backend hardware or encryption. You'll likely see performance issues and potential data security issues. If you ever find a completely "free" proxy server, tread very carefully. Some of those are just looking to steal your credit card numbers.

Browsing history log

The proxy server has your original IP address and web request information possibly unencrypted saved locally. Make sure to check if your proxy server logs and saves that data – and what kind of retention or law enforcement cooperation policies they follow.

If you expect to use a proxy server for privacy, but the vendor is just logging and selling your data you might not be receiving the expected value for the service.

No encryption

If you use a proxy server without encryption, you might as well not use a proxy server. No encryption means you are sending your requests as plain text. Anyone who is listening will be able to pull usernames and passwords and account information really easily. Make sure whatever proxy server you use provides full encryption capability.

Types of Proxy Servers

Not all proxy servers work the same way. It's important to understand exactly what functionality you're getting from the proxy server and ensure that the proxy server meets your use case.

Transparent Proxy

A transparent proxy tells websites that it is a proxy server and it will still pass along your IP address, identifying you to the webserver. Businesses, public libraries, and schools often use transparent proxies for content filtering: they're easy to set up both client and server-side.

Anonymous Proxy

An anonymous proxy will identify itself as a proxy, but it won't pass your IP address to the website – this helps prevent identity theft and keep your browsing habits private. They can also prevent a website from serving you targeted marketing content based on your location. For example, if CNN.com knows you live in Raleigh, NC, they will show you news stories they feel are relevant to Raleigh, NC. Browsing anonymously will prevent a website from using some ad targeting techniques, but is not a 100% guarantee.

Distorting proxy

A distorting proxy server passes along a false IP address for you while identifying itself as a proxy. This serves similar purposes as the anonymous proxy, but by passing a false IP address, you can appear to be from a different location to get around content restrictions.

High Anonymity proxy

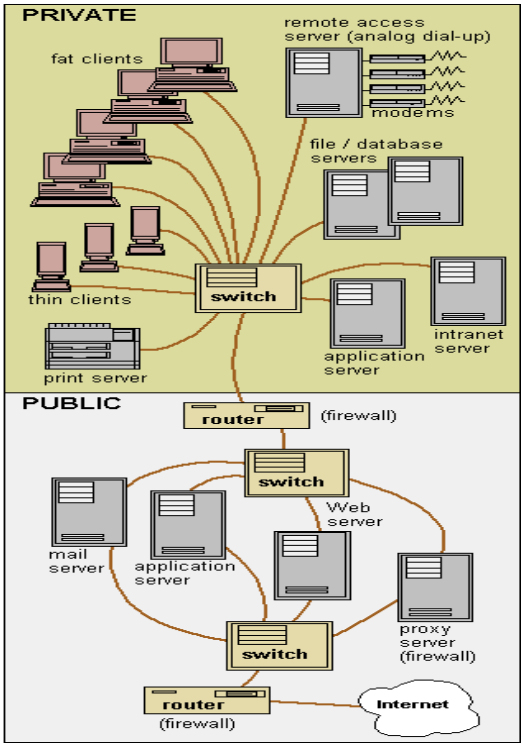
High Anonymity proxy servers periodically change the IP address they present to the web server, making it very difficult to keep track of what traffic belongs to who. High anonymity proxies, like the TOR Network, is the most private and secure way to read the internet.

Proxy servers are a hot item in the news these days with the controversies around Net Neutrality and censorship. By removing net neutrality protections in the United States, Internet Service Providers (ISP) are now able to control your bandwidth and internet traffic. ISPs can

potentially tell you what sites you can and cannot see. While there's a great amount of uncertainty around what is going to happen with Net Neutrality, it's possible that proxy servers will provide some ability to work around an ISPs restrictions.

Varonis analyzes data from proxy servers to protect you from data breaches and cyber-attacks. The addition of proxy data gives more context to better analyze user behavior trends for abnormalities. You can get an alert on that suspicious activity with actionable intelligence to investigate and deal with the incident.

For example, a user accessing GDPR data might not be significant on its own. But if they access GDPR data and then try to upload it to an external website, it could be an exfiltration attempt and a potential data breach. Without the context provided by file system monitoring, proxy monitoring, and Varonis threat models, you might see these events in a vacuum and not realize you need to prevent a data breach.



Network Classes or IP Classes

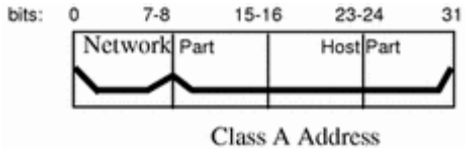
The first step in planning for IP addressing on your network is to determine which network class is appropriate for your network. After you have done this, you can take the crucial second step: obtain the network number from the InterNIC addressing authority.

Currently there are three classes of TCP/IP networks. Each class uses the 32-bit IP address space differently, providing more or fewer bits for the network part of the address. These classes are class A, class B, and class C.

Class A Network Numbers

A class A network number uses the first eight bits of the IP address as its "network part." The remaining 24 bits comprise the host part of the IP address, as illustrated in Figure 3-2 below.

Figure 3-2 Byte Assignment in a Class A Address

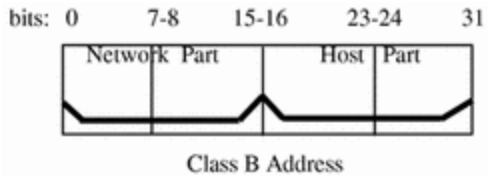


The values assigned to the first byte of class A network numbers fall within the range 0-127. Consider the IP address 75.4.10.4. The value 75 in the first byte indicates that the host is on a class A network. The remaining bytes, 4.10.4, establish the host address. The InterNIC assigns only the first byte of a class A number. Use of the remaining three bytes is left to the discretion of the owner of the network number. Only 127 class A networks can exist. Each one of these numbers can accommodate up to 16,777,214 hosts.

Class B Network Numbers

A class B network number uses 16 bits for the network number and 16 bits for host numbers. The first byte of a class B network number is in the range 128-191. In the number 129.144.50.56, the first two bytes, 129.144, are assigned by the InterNIC, and comprise the network address. The last two bytes, 50.56, make up the host address, and are assigned at the discretion of the owner of the network number. Figure 3-3 graphically illustrates a class B address.

Figure 3-3 Byte Assignment in a Class B Address



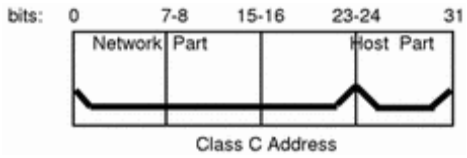
Class B is typically assigned to organizations with many hosts on their networks.

Class C Network Numbers

Class C network numbers use 24 bits for the network number and 8 bits for host numbers. Class C network numbers are appropriate for networks with few hosts--the maximum being 254. A class C network number occupies the first three bytes of an IP address. Only the fourth byte is assigned at

the discretion of the network owners. Figure 3-4 graphically represents the bytes in a class C address.

Figure 3-4 Byte Assignment in a Class C Address



The first byte of a class C network number covers the range 192-223. The second and third each cover the range 1- 255. A typical class C address might be 192.5.2.5. The first three bytes, 192.5.2, form the network number. The final byte in this example, 5, is the host number.

Administering Network Numbers

If your organization has been assigned more than one network number, or uses subnets, appoint a centralized authority within your organization to assign network numbers. That authority should maintain control of a pool of assigned network numbers, assigning network, subnet, and host numbers as required. To prevent problems, make sure that duplicate or random network numbers do not exist in your organization.

Designing Your IP Addressing Scheme

After you have received your network number, you can then plan how you will assign the host parts of the IP address.

Table 3-1 shows the division of the IP address space into network and host address spaces. For each class, "range" specifies the range of decimal values for the first byte of the network number. "Network address" indicates the number of bytes of the IP address that are dedicated to the network part of the address, with each byte represented by xxx. "Host address" indicates the number of bytes dedicated to the host part of the address. For example, in a class A network address, the first byte is dedicated to the network, and the last three are dedicated to the host. The opposite is true for a class C network.

Table 3-1 Division of IP Address Space

Class	Range	Network Address	Host Address
A	0-127	xxx	xxx.xxx.xxx
B	128-191	xxx.xxx	xxx.xxx
C	192-223	xxx.xxx.xxx	xxx

The numbers in the first byte of the IP address define whether the network is class A, B, or C and are always assigned by the InterNIC. The remaining three bytes have a range from 0-255. The numbers 0

and 255 are reserved; you can assign the numbers 1-254 to each byte depending on the network number assigned to you.

Table 3-2 shows which bytes of the IP address are assigned to you and the range of numbers within each byte that are available for you to assign to your hosts.

Table 3-2 Range of Available Numbers

Network Class	Byte 1 Range	Byte 2 Range	Byte 3 Range	Byte 4 Range
A	0-127	1-254	1-254	1-254
B	128-191	Preassigned by Internet	1-254	1-254
C	192-223	Preassigned by Internet	Preassigned by Internet	1-254

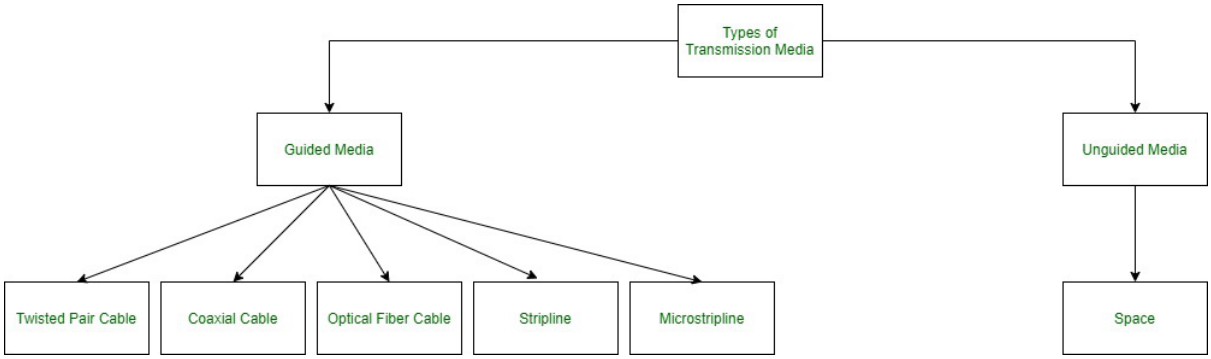
Transmission media

Types of Transmission Media

Difficulty Level : Easy

Last Updated : 22 Nov, 2021

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



1. Guided Media:
It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.
Features:

High Speed

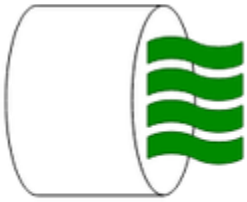
Secure

Used for comparatively shorter distances

There are 3 major types of Guided Media:

(i) Twisted Pair Cable –
It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

Unshielded Twisted Pair (UTP):
UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.



Unshielded Twisted Pair

Advantages:

⇢ Least expensive

⇢ Easy to install

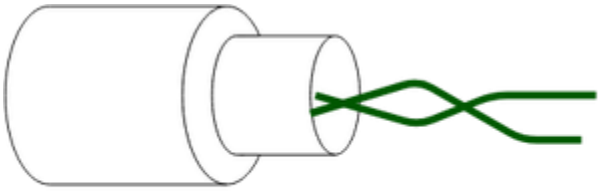
⇢ High-speed capacity

⇢ Susceptible to external interference

⇢ Lower capacity and performance in comparison to STP

⇢ Short distance transmission due to attenuation

Shielded Twisted Pair (STP):
This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



Shielded Twisted Pair

Advantages:

⇢ Better performance at a higher data rate in comparison to UTP

⇢ Eliminates crosstalk

⇢ Comparatively faster

⇢ Comparatively difficult to install and manufacture

⇢ More expensive

⇢ Bulky

(ii) Coaxial Cable –
It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

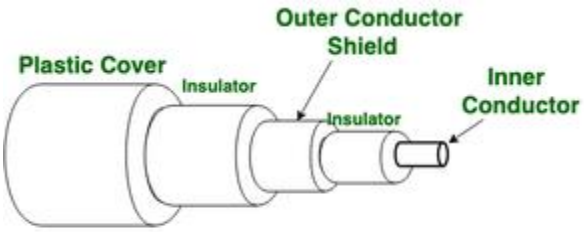


Figure of Coaxial Cable

Advantages:

High Bandwidth

Better noise Immunity

Easy to install and expand

Inexpensive

Disadvantages:

Single cable failure can disrupt the entire network

(iii) Optical Fiber Cable –
It uses the concept of reflection of light through a core made up of glass or plastic. The core is

surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.

The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

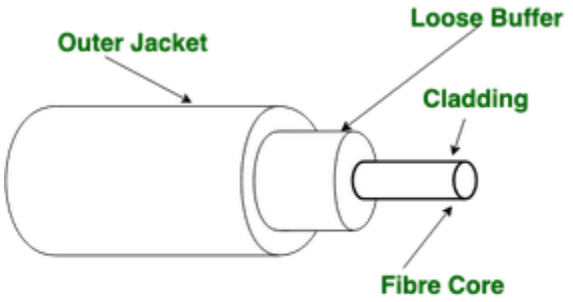


Figure of Optical Fibre Cable

Advantages:

Increased capacity and bandwidth

Lightweight

Less signal attenuation

Immunity to electromagnetic interference

Resistance to corrosive materials

Disadvantages:

Difficult to install and maintain

High cost

Fragile

(iv) Stripline

Stripline is a transverse electromagnetic (TEM) transmission line medium invented by Robert M. Barrett of the Air Force Cambridge Research Centre in the 1950s. Stripline is the earliest form of the planar transmission line. It uses a conducting material to transmit high-frequency waves it is also called a waveguide. This conducting material is sandwiched between two layers of the ground plane which are usually shorted to provide EMI immunity.

(v) Microstripline

In this, the conducting material is separated from the ground plane by a layer of dielectric.

2. Unguided Media:
It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

Features:

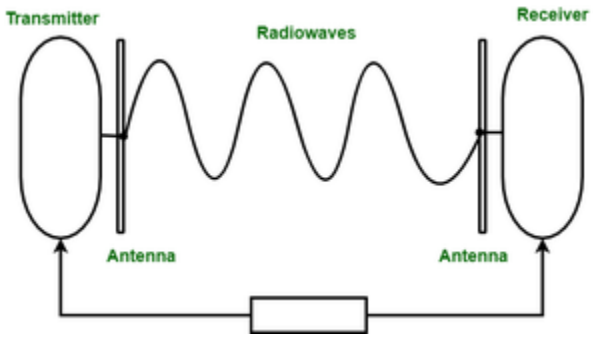
The signal is broadcasted through air

Less Secure

Used for larger distances

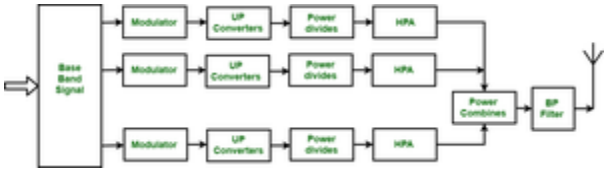
There are 3 types of Signals transmitted through unguided media:

(i) Radio waves –
These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.



Further Categorized as (i) Terrestrial and (ii) Satellite.

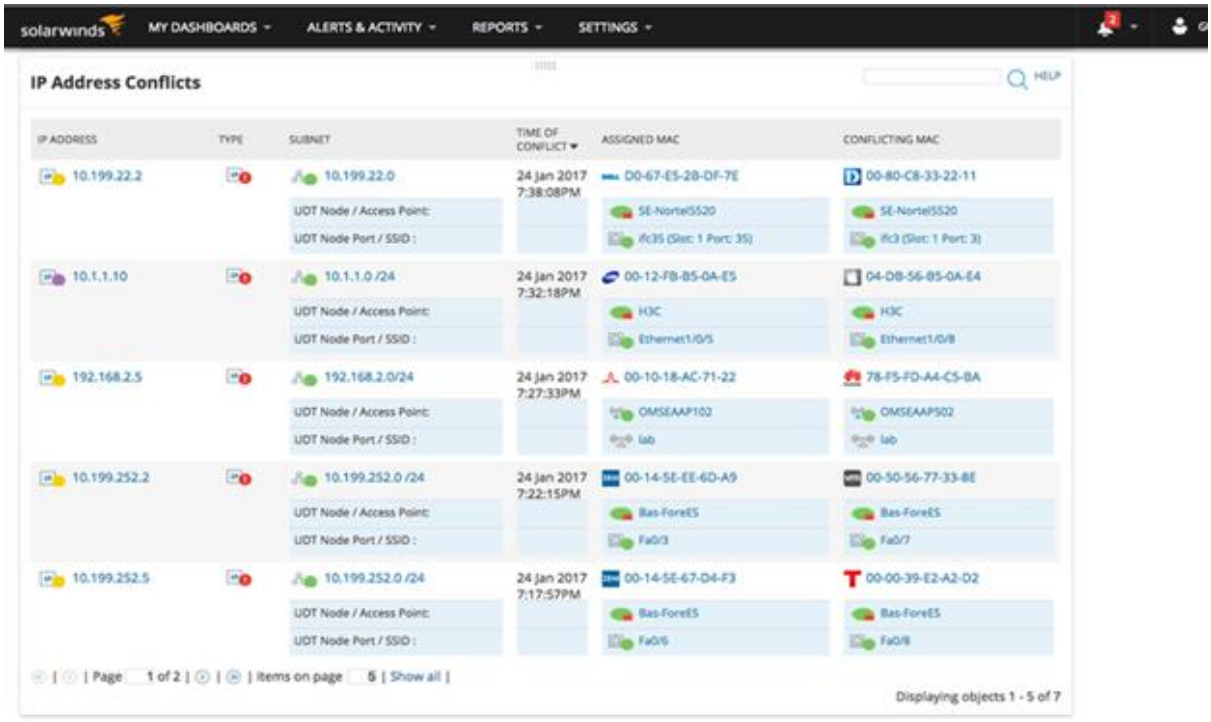
(ii) Microwaves –
It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.



(iii) Infrared –
Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

To best solve IP address conflicts, I recommend investing in IP conflict detection software. IP conflict detection tools are designed to help you find IP conflicts and assess how to solve IP conflicts quickly. An IP conflict scanner can help you avoid and identify IP conflicts, and most IP conflict software is also designed to improve network reliability. On top of this, many IP conflict tools enable you to manage your IP addresses, disable problematic devices, and catch problems right away using customizable alerts and alarms.

This article discusses IP addresses and IP address conflicts and goes through some ways you can use IP conflict finders to fix IP address conflicts. For an easy, effective, and consistent IP address conflict fix, I recommend using the SolarWinds® IP Control Bundle (IPCB), which includes the capabilities of both IP Address Manager (IPAM) and User Device Tracker (UDT). With this bundle, you can take immediate action to resolve IP address conflict and dive deep into details of specific issues. IPCB is also designed to organize your IP addresses and identify affected subsets, helping you manage your IP environment to better understand how to troubleshoot IP conflicts. A 30-day free trial of the SolarWinds IP Control Bundle is available for download.



What Is an IP Address Conflict?

An IP conflict occurs when two or more devices in the same network share an IP address. This clash causes one or both devices to stop communicating with the rest of the network, which could lead to a slew of problems. Figuring out how to find IP conflicts, as well as how to fix an IP conflict when it occurs, is crucial to the health of your network and its devices.

What Is an IP Address?

An IP ("internet protocol") address is the identification number given to a specific device in a network such as a computer, cell phone, router, switch, etc. This code allows devices to communicate across your network, which helps information flow properly. A device's IP address is made up of 32 numbers joined together by periods and must be unique within its network to function.

You can think of an IP address as a device's ZIP code within a network. An IP address helps your network's devices send and receive data swiftly, and accurately. But, if there's more than one IP address in use, there can be problems getting the right data to the right places.

Almost every device on a given network has a public IP address and a private IP address. As the names suggest, a public IP address links you to the outside world while a private IP address handles local activities on your network. Besides private and public, there are two main categories of IP addresses. Dynamic IP addresses automatically change over time, are easiest for an ISP server to process, and are usually generated using DHCP (Dynamic Host Configuration Protocol). Static IP addresses stay the same over time, are easiest for identification management, and are usually assigned manually.

Most personal home IP addresses are generated using a DHCP server and are therefore dynamic. However, when it comes to the vast networks of businesses and organizations, IP addresses can be both dynamic and static. Unfortunately, it's easy to accidentally cause a duplicate IP address if

you're generating IP addresses manually along with using a DHCP. It's also easy to have duplicate IP addresses when using more than one DHCP server—which is exactly why you should never do this.

How to Detect an IP Address Conflict on Networks

Usually, your network operating software will notify you when it encounters an IP address conflict. Depending on the operating system, this could come in the form of an error message—such as a balloon, pop-up, or notification—letting you know there's a duplicate IP address present in the network. When your system finds an IP conflict, the network interface on both ends becomes disabled. This shuts down each device with an affected IP address, disabling functions until the IP address conflict is resolved.

Sometimes, your network won't detect the IP conflict and there will be no notification, causing the problem to go unnoticed. When this happens, you'll see valid IP addresses on your network, but the connectivity simply won't work or will be intermittent. You might also receive vague "network unavailable" error messages, not alerting you to the true cause of the problem.

You may have heard IP address conflicts will amend themselves. But leaving an IP address conflict untouched could lead to further complications across your network. And when an IP address conflict does work itself out, it usually takes a fair amount of time and causes even more problems to manifest under the surface. It's best to search for IP conflict solutions immediately after an issue arises.

There are a few ways an IP address conflict can occur, some of which I've outlined below:

DHCP Errors

Natural errors can occur in your DHCP server, causing DHCP to use the same IP address for multiple devices. Sometimes, DHCP gives a new device a dynamic IP address already in use as a static IP address. DHCP can also lose track of the IP address numbers it has generated.

One proactive way to avoid a DHCP IP address conflict is to define a DHCP scope. A DHCP scope gives DHCP a pool of IP addresses to choose from, so you can reduce the chances of DHCP generating duplicate IP addresses. Most, though not all DHCP servers, will allow for this.

Repeat Static IP Errors

Sometimes an administrator accidentally creates two of the same static IP addresses. It's okay, everybody makes mistakes—it can easily be amended by re-assigning a unique static IP address to each affected device.

Standby Mode Errors

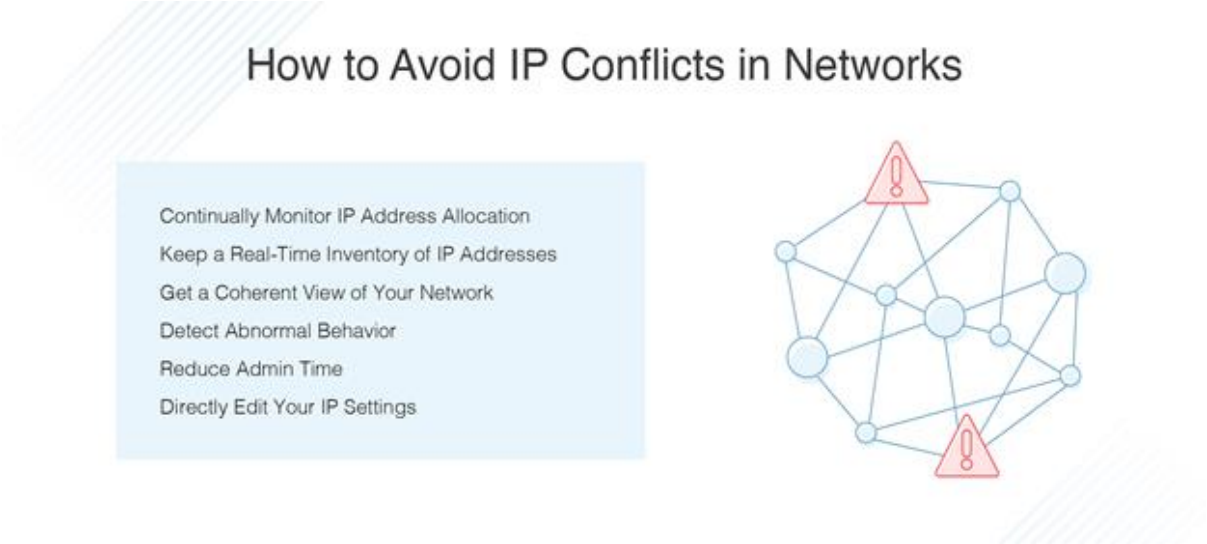
An IP address conflict can occur after a device "wakes up" from not being in use for a while. During this device's hibernated state its IP address may have been recalled and assigned to another device, so when the first device wakes up, it believes it can use the same IP address.

A 0.0.0.0. IP Address

An IP address containing only zeros is a common problematic IP address. This means your device can see the network, but something is interfering with its ability to receive a proper IP address. There are a few ways to potentially fix this issue—temporarily disable the device's firewall, reconfigure the connected DHCP server and ensure it's enabled, and double-check your network adaptor is installed correctly.

How to Avoid IP Conflict in Networks

There is no catch-all IP address conflict fix. Especially for complicated networks with lots of remote network devices, which are harder to identify using a ping or arp utility, you'll have to approach each IP address conflict uniquely.



The best way to avoid an IP address conflict in your network is to use IP conflict software, which can help detect and solve many forms of IP address conflicts. An IP conflict scanner is designed to find IP conflicts and enable you to keep track of all your IP addresses from your core devices. Not only will this save you time and resources but will also help you organize your network's IP addresses to avoid future IP address conflicts.

Here are some features an IP conflict finder can help you achieve.

Continually Monitor IP Address Allocation

By keeping track of which IP address is in use on which device, your IP conflict tool is designed to help avoid IP conflicts in your network.

Keep a Real-Time Inventory of IP Addresses

Continually keeping track of active IP addresses helps prevent you from reassigning IP addresses already in use. Many IP conflict detection programs will create and constantly update an inventory of used IP addresses to further avoid the chance of reassignment.

Get a Coherent View of Your Network

Dive deep into details of your IP addresses in use and from the past, including specifics like subnets, hostnames, and associated devices, plus view past and present statuses and alerts.

Detect Abnormal Behavior

Besides administering IP address conflict solutions, IP conflict software can help pick up on other unexplained activity that could be dangerous or problematic for your network.

Reduce Admin Time

Having your IP addresses managed and monitored for you frees up your schedule and your brainpower, letting you focus on what's really important.

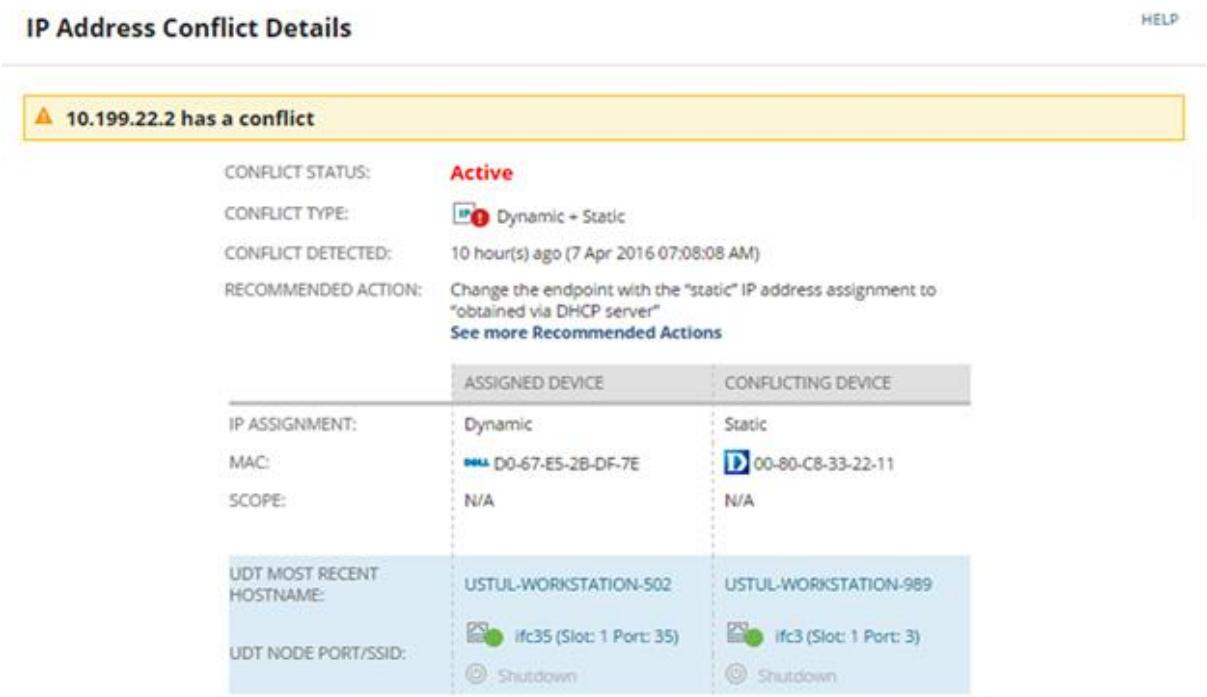
Directly Edit Your IP Settings

You can access the settings for all your IP addresses in an instant, enabling you to fix IP conflicts as you view your IP addresses and their corresponding devices.

Running a network by homestyle spreadsheets and solutions can prove difficult, confusing, and time-consuming. An IP conflict tool will help you manage, discover, and solve IP address conflicts to help ensure a safe and well-maintained network environment.

Recommended Tool for Detecting, Avoiding, and Solving IP Address Conflicts

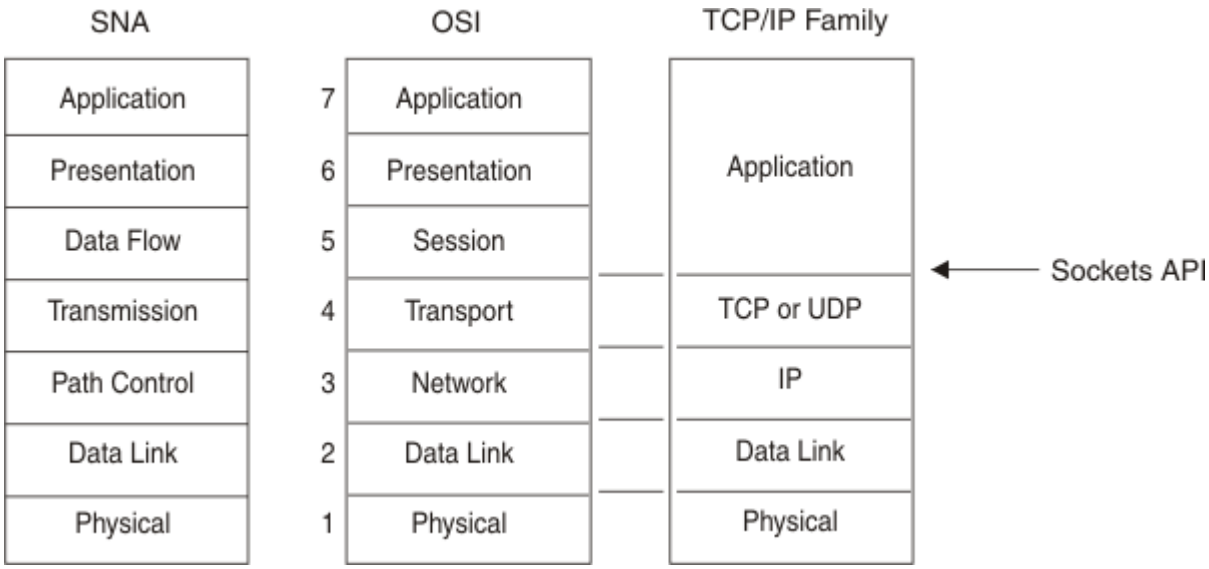
When it comes to IP conflict solution tools, I highly recommend the SolarWinds IP Control Bundle (IPCB), which contains SolarWinds IP Address Manager (IPAM) and SolarWinds User Device Tracker (UDT). The IPCB can enable you to discover what time an IP conflict was detected, all subnets impacted by the conflict, and even what kind of issue it may be—all simply by hovering over a given IP address. The IPCB is designed to resolve IP address conflict by automatically disabling an affected port, which allows your network to function normally until you can fix the IP address conflict. You can also organize your IP addresses and manage your DHCP scopes, switches, and ports. Download a 30-day free trial of the SolarWinds IPCB today.



TCP/IP TCP, UDP, and IP protocols

TCP/IP is a large family of protocols that is named after its two most important members. Figure 1 shows the TCP/IP protocols used by CICS® TCP/IP, in terms of the layered Open Systems Interconnection (OSI) model, which is widely used to describe data communication systems. For CICS users who might be more accustomed to SNA, the left side of Figure 1 shows the SNA layers, which correspond very closely to the OSI layers.

Figure 1. TCP/IP protocols compared to the OSI model and SNA



The protocols implemented by TCP/IP Services and used by CICS TCP/IP are shown in the right hand column in Figure 1:

Transmission Control Protocol (TCP)

In terms of the OSI model, TCP is a transport-layer protocol. It provides a reliable virtual-circuit connection between applications; that is, a connection is established before data transmission begins. Data is sent without errors or duplication and is received in the same order as it is sent. No boundaries are imposed on the data; TCP treats the data as a stream of bytes.

User Datagram Protocol (UDP)

UDP is also a transport-layer protocol and is an alternative to TCP. It provides an unreliable datagram connection between applications. Data is transmitted link by link; there is no end-to-end connection. The service provides no guarantees. Data can be lost or duplicated, and datagrams can arrive out of order.

Internet Protocol (IP)

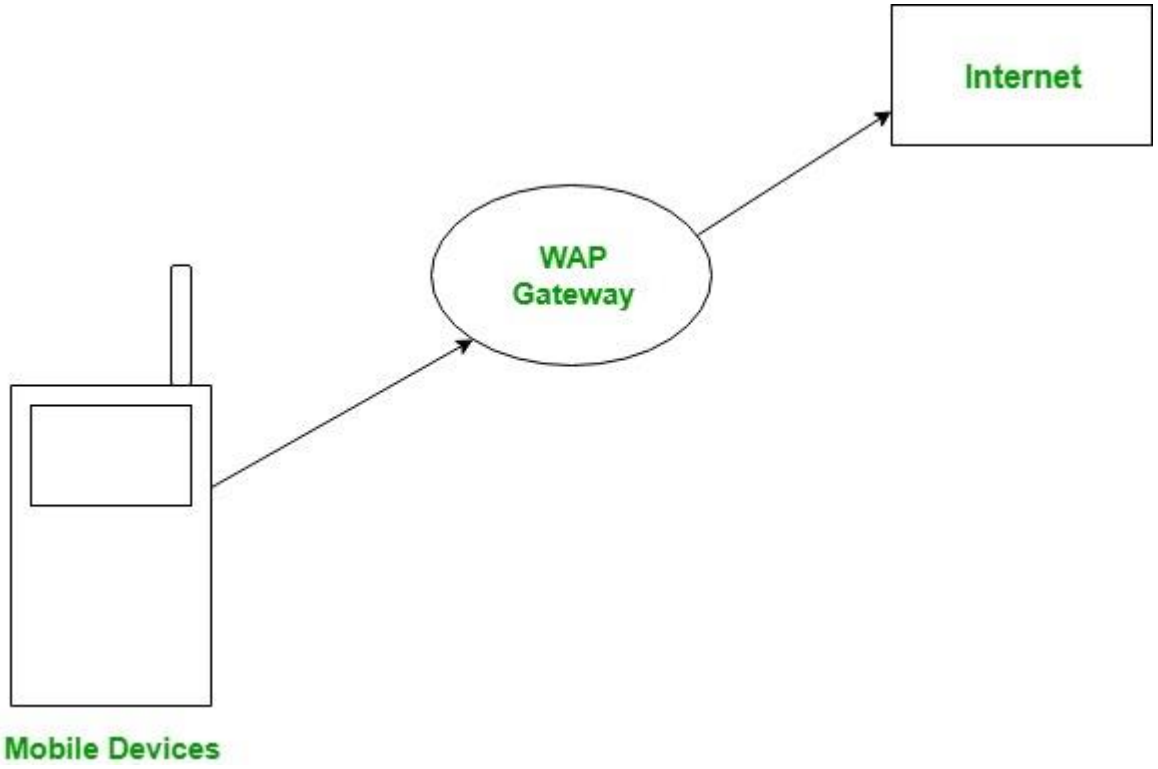
In terms of the OSI model, IP is a network-layer protocol. It provides a datagram service between applications, supporting both TCP and UDP.

Wireless Application Protocol

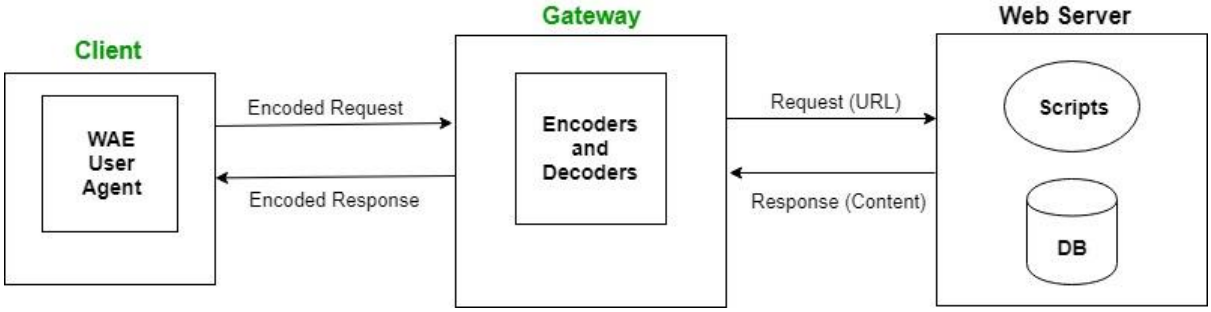
WAP stands for Wireless Application Protocol. It is a protocol designed for micro-browsers and it enables the access of internet in the mobile devices. It uses the mark-up language WML (Wireless Markup Language and not HTML), WML is defined as XML 1.0 application. It enables creating web

applications for mobile devices. In 1998, WAP Forum was founded by Ericson, Motorola, Nokia and Unwired Planet whose aim was to standardize the various wireless technologies via protocols.

WAP protocol was resulted by the joint efforts of the various members of WAP Forum. In 2002, WAP forum was merged with various other forums of the industry resulting in the formation of Open Mobile Alliance (OMA).

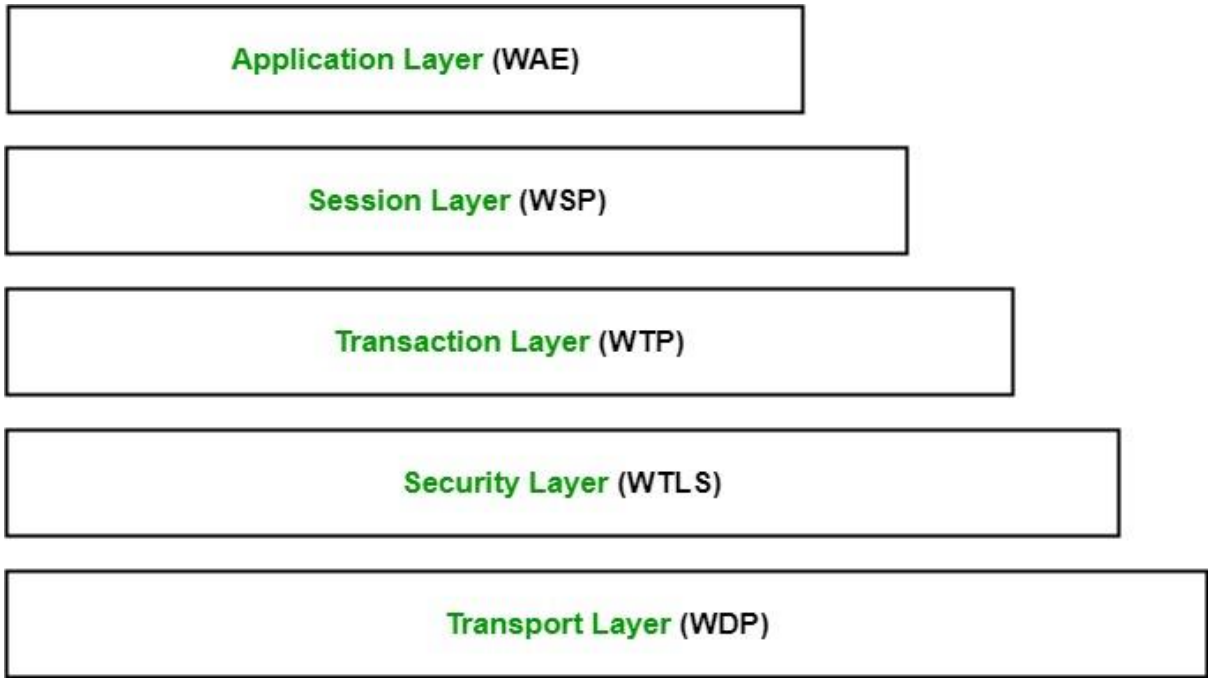


WAP Model:
The user opens the mini-browser in a mobile device. He selects a website that he wants to view. The mobile device sends the URL encoded request via network to a WAP gateway using WAP protocol.



The WAP gateway translates this WAP request into a conventional HTTP URL request and sends it over the internet. The request reaches to a specified Web server and it processes the request just as it would have processed any other request and sends the response back to the mobile device through WAP gateway in WML file which can be seen in the micro-browser.

WAP Protocol stack:



Application Layer:
This layer contains the Wireless Application Environment (WAE). It contains mobile device specifications and content development programming languages like WML.

Session Layer:
This layer contains Wireless Session Protocol (WSP). It provides fast connection suspension and reconnection.

Transaction Layer:
This layer contains Wireless Transaction Protocol (WTP). It runs on top of UDP (User Datagram Protocol) and is a part of TCP/IP and offers transaction support.

Security Layer:
This layer contains Wireless Transaction Layer Security (WTLS). It offers data integrity, privacy and authentication.

Transport Layer:
This layer contains Wireless Datagram Protocol. It presents consistent data format to higher layers of WAP protocol stack.

RAID (Redundant Arrays of Independent Disks)

RAID, or “Redundant Arrays of Independent Disks” is a technique which makes use of a combination of multiple disks instead of using a single disk for increased performance, data redundancy or both. The term was coined by David Patterson, Garth A. Gibson, and Randy Katz at the University of California, Berkeley in 1987.

Why data redundancy?

Data redundancy, although taking up extra space, adds to disk reliability. This means, in case of disk failure, if the same data is also backed up onto another disk, we can retrieve the data and go on with the operation. On the other hand, if the data is spread across just multiple disks without the RAID technique, the loss of a single disk can affect the entire data.

Key evaluation points for a RAID System

Reliability: How many disk faults can the system tolerate?

Availability: What fraction of the total session time is a system in uptime mode, i.e. how available is the system for actual use?

Performance: How good is the response time? How high is the throughput (rate of processing work)? Note that performance contains a lot of parameters and not just the two.

Capacity: Given a set of N disks each with B blocks, how much useful capacity is available to the user?

RAID is very transparent to the underlying system. This means, to the host system, it appears as a single big disk presenting itself as a linear array of blocks. This allows older technologies to be replaced by RAID without making too many changes in the existing code.

Different RAID levels

RAID-0 (Stripping)

Blocks are “stripped” across disks.

Disk 0	Disk 1	Disk 2	Disk 3
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

In the figure, blocks “0,1,2,3” form a stripe.

Instead of placing just one block into a disk at a time, we can work with two (or more) blocks placed into a disk before moving on to the next one.

Disk 0	Disk 1	Disk 2	Disk 3
0	3	4	6
1	3	5	7
8	10	12	14
9	11	13	15

Evaluation:

Reliability: 0
There is no duplication of data. Hence, a block once lost cannot be recovered.

Capacity: N*B
The entire space is being used to store data. Since there is no duplication, N disks each having B blocks are fully utilized.

RAID-1 (Mirroring)

More than one copy of each block is stored in a separate disk. Thus, every block has two (or more) copies, lying on different disks.

Disk 0	Disk 1	Disk 2	Disk 3
0	0	1	1
2	2	3	3
4	4	5	5
6	6	7	7

The above figure shows a RAID-1 system with mirroring level 2.

RAID 0 was unable to tolerate any disk failure. But RAID 1 is capable of reliability.

Evaluation:

Assume a RAID system with mirroring level 2.

Reliability: 1 to N/2
1 disk failure can be handled for certain, because blocks of that disk would have duplicates on some other disk. If we are lucky enough and disks 0 and 2 fail, then again this can be handled as the blocks of these disks have duplicates on disks 1 and 3. So, in the best case, N/2 disk failures can be handled.

Capacity: N*B/2
Only half the space is being used to store data. The other half is just a mirror to the already stored data.

RAID-4 (Block-Level Stripping with Dedicated Parity)

Instead of duplicating data, this adopts a parity-based approach.

Disk 0	Disk 1	Disk 2	Disk 3	Disk 4
0	1	2	3	P0
4	5	6	7	P1
8	9	10	11	P2
12	13	14	15	P3

In the figure, we can observe one column (disk) dedicated to parity.

Parity is calculated using a simple XOR function. If the data bits are 0,0,0,1 the parity bit is XOR(0,0,0,1) = 1. If the data bits are 0,1,1,0 the parity bit is XOR(0,1,1,0) = 0. A simple approach is that even number of ones results in parity 0, and an odd number of ones results in parity 1.

C1	C2	C3	C4	Parity
0	0	0	1	1
0	1	1	0	0

Assume that in the above figure, C3 is lost due to some disk failure. Then, we can recompute the data bit stored in C3 by looking at the values of all the other columns and the parity bit. This allows us to recover lost data.

Evaluation:

Reliability: 1
RAID-4 allows recovery of at most 1 disk failure (because of the way parity works). If more than one disk fails, there is no way to recover the data.

Capacity: (N-1)*B
One disk in the system is reserved for storing the parity. Hence, (N-1) disks are made available for data storage, each disk having B blocks.

RAID-5 (Block-Level Stripping with Distributed Parity)

This is a slight modification of the RAID-4 system where the only difference is that the parity rotates among the drives.

Disk 0	Disk 1	Disk 2	Disk 3	Disk 4
0	1	2	3	P0
5	6	7	P1	4
10	11	P2	8	9
15	P3	12	13	14
P4	16	17	18	19

In the figure, we can notice how the parity bit “rotates”.

This was introduced to make the random write performance better.

Evaluation:

Reliability: 1
RAID-5 allows recovery of at most 1 disk failure (because of the way parity works). If more than one disk fails, there is no way to recover the data. This is identical to RAID-4.

Capacity: (N-1)*B
Overall, space equivalent to one disk is utilized in storing the parity. Hence, (N-1) disks are made available for data storage, each disk having B blocks.

What about the other RAID levels?

RAID-2 consists of bit-level stripping using a Hamming Code parity. RAID-3 consists of byte-level striping with dedicated parity. These two are less commonly used.
RAID-6 is a recent advancement that contains a distributed double parity, which involves block-level stripping with 2 parity bits instead of just 1 distributed across all the disks. There are also hybrid RAIDs, which make use of more than one RAID levels nested one after the other, to fulfill specific requirements.

What is RAID and what are the different RAID modes?

Note: Not all StarTech.com devices support each of the RAID modes described below. For more information on the RAID modes that your device supports, refer to the manual or the StarTech.com product page.

Redundant Array of Independent Disks (RAID) is a virtual disk technology that combines multiple physical drives into one unit. RAID can create redundancy, improve performance, or do both.

RAID should not be considered a replacement for backing up your data. If critical data is going onto a RAID array, it should be backed up to another physical drive or logical set of drives.

The following are terms that are normally used in connection with RAID:

Striping: data is split between multiple disks.

Mirroring: data is mirrored between multiple disks.

Parity: also referred to as a checksum. Parity is a calculated value used to mathematically rebuild data.

Different RAID levels exist for different application requirements.

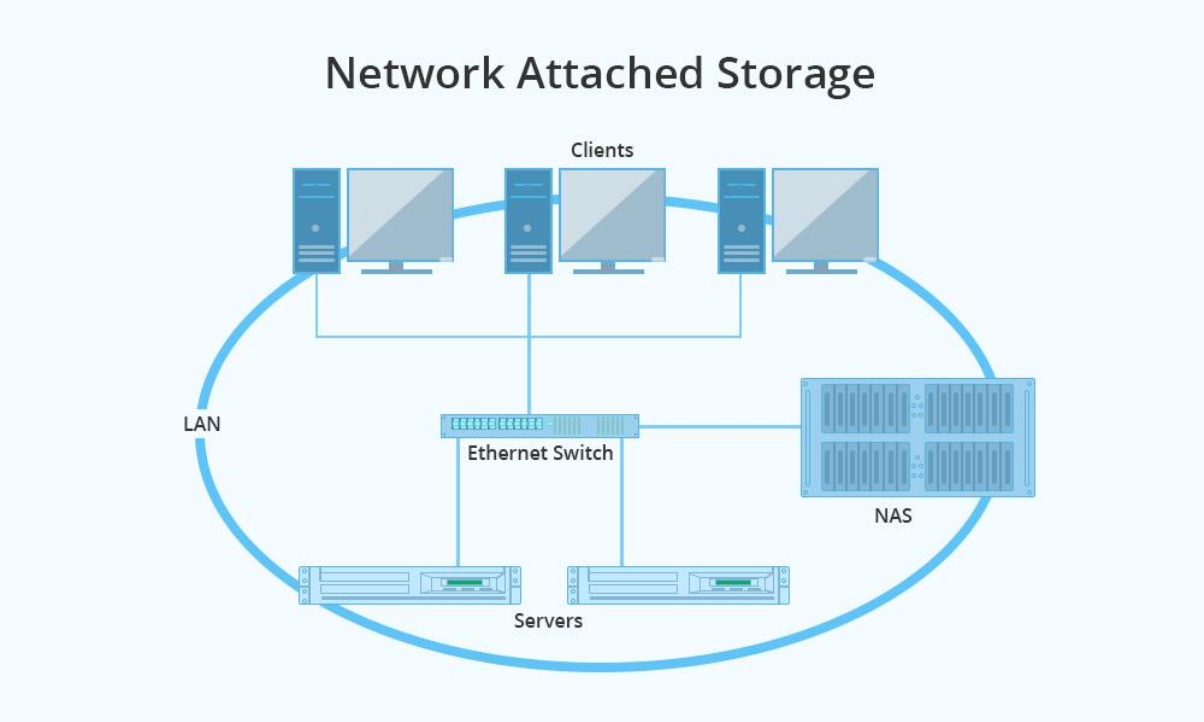
Refer to the following table for the list of RAID modes offered by some StarTech.com products:

RAID mode	Description	Operation	Advantages	Disadvantages	Recovery
RAID 0	Striped disks	Data is split evenly between two or more disks.	Large size and the fastest speed.	No redundancy.	If one or more drives fails, this results in array failure.
RAID 1	Mirrored disks	Two or more drives have identical data on them.	A single drive failure will not result in data loss.	Speed and size is limited by the slowest and smallest disk.	Only one drive is needed for recovery.
RAID 3	Striped set with dedicated parity	Data is split evenly between two or more disks, plus a dedicated drive for parity storage.	High speeds for sequential read/write operations.	Poor performance for multiple simultaneous instructions.	A single drive failure will rebuild.
RAID 5	Striped disks with distributed parity	Data is split evenly between three or more disks. Parity is split between disks.	Large size, fast speed, and redundancy.	The total array size is reduced by parity.	A single drive failure will rebuild.

RAID 10	1+0; Striped set of Mirrored Subset	Four or more drives are made into two mirrors that are striped.	Larger size and higher speed than RAID-1, and more redundancy than RAID-0.	No parity.	Only one drive in a mirrored set can fail.
JBOD	Just a Bunch Of Disks	Any number of drives are accessed independently by the operating system.	Software RAID modes can be used.	Hardware RAID may have better performance.	N/A
Big	Spanning or Concatenation	Data is written on one drive until it is full, and then the next drive(s) until it or they are full.	Creates a very large and simple array.	No redundancy.	N/A
Clone	RAID 1 + Spare	Two drives have identical data, plus one drive is used for rebuilding in case of a primary array failure.	Seamless operation when one drive fails in a RAID-1 array.	Spare drive is not accessible to the user.	Only one drive is needed for recovery.

NAS – the Hard Drive That Is Connected to a Network

NAS is a file-level access storage architecture connected to a network which enables multiple users and heterogeneous client devices to retrieve data from centralized disk capacity. NAS connects directly to an Ethernet switch which is linked to the servers. Users on a local area network (LAN) can access the shared storage from the NAS via a standard Ethernet connection. NAS devices provide infrastructure to consolidate storage in one place and to support tasks, such as archiving and backup, and a cloud tier. Unlike traditional external hard drives, NAS devices generally have some kind of built-in operating system which adds software functions like native media streaming, printer streaming, or remote access.



Pros

Smaller than servers and save more space in the office

NAS devices are much cheaper than servers

NAS devices can be used to host applications with ease of access

NAS devices can also be used to automatically create locally stored backups of your business data

NAS simplifies file sharing and collaboration among multiple users

Cons

NAS is LAN-dependent; if the LAN goes down, so does the NAS

With a NAS, you're limited to applications you can download on the NAS operating system

NAS consumes large amounts of bandwidth which may affect the speed of the computer network

NAS device vendors require users to choose one of their own applications rather than choosing any third-party software

NAS is lack of security over the cloud as someone could pick it up and take it

Server – Security-enhanced Hardware with Built-in Firewall

A server is a high-performance hardware designed to process requests and deliver data to other computers over a local network or Internet. The Internet server is normally configured with additional processing memory and storage capacity to handle massive users and requests.

Pros

Storing large amounts of data clearing space on your PC and giving you more processing power to supercharge your network

Not limited to the alternative applications because servers allow you to install third-party software

More reliable and higher security-enhanced infrastructure with built-in firewall to protect your business data

Cons

You need to do regular maintenance for the server, just in case one of the hard drives kicks the bucket

Server operating systems often require companies to purchase a server license

Servers require more power and are more expensive than NAS devices

Server installations take much longer to implement and require expertise to administrate

NAS vs Server: Which Is Right for You?

NAS vs server topic has been discussed many times in forums. Both NAS devices and servers provide a great way to share files across devices on a network. When selecting between NAS vs server,

you’re supposed to consider the following aspects to decide which one is more suitable for your needs.

Cost

Your budget is the most fundamental factor to consider because a server would be much pricier than a NAS device. Apart from the price of the equipment itself, the server expense may also cover higher power consumption, more cooling fees, as well as the server license charge.

Space

A server is much larger than a NAS device thus the server is not suitable for office applications which are limited in space. In contrast, the NAS devices are portable and easy to move around so that they can be connected to a router or switch in small and medium-sized businesses (SMBs).

Security

NAS processes file-based data and may operate with a global namespace to share data in LANs. NAS devices are susceptible to environmental factors and can be easily picked up and stolen. The servers have higher security-enhanced infrastructure with built-in firewalls to protect your business data.

Scalability

Scalability is a major driver when making your data storage options between NAS vs server. NAS devices are not highly scalable because you're limited to the drive cage of the NAS. In contrast, the server’ network architecture enables admins to scale the network capacity in scale-up or scale-out configurations. Therefore, if you plan to install a bunch of applications and customize almost everything, servers would be the winner.

Best Affordable Servers for Cloud Storage and SMBs

All of the current data trends place a lot of prominence on the IT infrastructure that serves and stores it. Thus the servers implemented to store and backup the data must be capable to scale with growth and continue to provide higher levels of performance. FS provides three enterprise servers listed in the chart below. These small business servers come with high performance and storage flexibility for future growth in a 2RU form factor.

What Is CMD

CMD stands for Command (.CMD). A command is an instruction given to a computer program that tells the program what has to be done. It is an application that is found in most computers with Windows as the Operating System, and it helps in the execution of the commands entered. It is also called Command Prompt or Windows Command Processor.

Why Is Command Prompt Useful

Command prompt has become increasingly popular with people having no background in IT as it helps to automate several tedious, mundane tasks with the help of a few clicks. The interface allows the user to run multiple commands, and the commands can be executed one after the other. This has proved a boon in the world of automation.

Most users find it difficult to learn and cannot use Command prompt as compared to the user-friendly interface that is available on the modern apps, however, Command prompt can still be used in many situations.

How To Open CMD In Windows

Opening Command Prompt in the Windows Operating System is as simple as a few clicks.

Step 1: Go to the Start Menu. This is at the bottom left of the screen. RUN.

Step 2: Type cmd in the search bar and hit Enter. The ones who love shortcuts in Windows can also use Ctrl+R which routes them to RUN, and then they can search for cmd and hit enter. The best thing about these commands in Windows is that they are not case sensitive, which makes it user friendly.

Let us now look at some of the basic and most commonly used CMD commands in the Command Prompt. In the next section, let us see the list of CMD commands with syntax.

Note: It is important to note that these commands are not case sensitive.

Basic CMD Commands

#1) CD- Change Directory

This command allows users to change from one directory to another or move from one folder to another.

Syntax: CD [/D] [drive:][path]

Example: C:>CD Prog

CD- Change Directory

Some of the other parameters of this command are discussed below. This will make this command more useful.

Parameter- cmd device: This parameter gives specific information about the device which will be used for input and output.

Parameter /d: This parameter is used when the user wants to change the current directory and the current drive as well.

#2) Mkdir

This command is used when subdirectories are to be created within the directories.

Syntax: mkdir [<drive>:]<path>

Example: mkdir fantastic (to create a directory name “ fantastic”)

Mkdir 3

#3) REN: Rename

Syntax: ren [<drive>:][<path>]<filename1> <filename2>

Example– ren /?

Rename 4

#4) ASSOC: Fix File Associations

This is one of the most basic and most common commands. It helps to associate (as the name suggests) some file extensions to some programs. For Example- When we click on .doc (extension), the computer is able to decide that it needs to associate it with Microsoft Word. The screenshot below shows an example of how this command works.

Syntax: assoc [.ext[=[fileType]]]

ASSOC: Fix File Associations

Example: – C:\Users\assoc.txt

assoc.txt

#5) FC File compare

The second most common command used is FC, also known as File Compare. This is an interesting feature that allows comparing files that have been changed over time.

Syntax: FC /a [/c] [/l] [/lb<n>] [/n] [/off[line]] [/t] [/u] [/w] [/<nnnn>] [<drive1>:][<path1>]<filename1> [<drive2>:][<path2>]<filename2>

FC/b [<drive1:>][<path1>]<filename1> [<drive2:>][<path2>]<filename2>

Example: FC File 1.txt File 2.txt

FC File compare 7

There are a few other parameters of FC command, explained below-

Parameter- /a: This parameter helps to concise the output when ASCII comparison is done. It shows the first and the last line in the list of differences.

Parameter /c: This parameter ignores the case sensitive aspect of letters.

Parameter /w: This parameter is very useful when files are compared. It eases the process of comparison of files by compressing or removing the white space in the process of comparison. This parameter /w in the FC command disregards the white space, if any, at the beginning and end of the line.

#6) POWERCFG: Power Configuration

This command gives a report of the power settings of the computer. In situations when the power of the computer drains out quickly, this command can help to generate a complete power efficiency. The report is generated within a minute and is extremely useful to detect any warnings which may impact the performance of the system.

Syntax: powercfg /option [arguments] [/?]

Example: powercfg /?

POWERCFG: Power Configuration

Another parameter of this command is /list, /L. This parameter lists all the power sources.

POWERCFG

#7) SHUTDOWN: Turn off Computer

This command is a very resourceful command. By using this command, users can not just shut down computers but also can control the process of the shutdown. This command is popular in situations where shutdown is part of a planned task.

Users can type shutdown/i on the command prompt and choose to either restart or a complete shutdown on the GUI dialogue box that appears. Users have a choice to avoid this GUI dialogue box by typing the shutdown/s command.

Syntax: shutdown [/i | /l | /s | /sg | /r | /g | /a | /p | /h | /e | /o] [/hybrid] [/fw] [/f] [/m \\computer][/t xxx][/d [p|u:]xx:yy [/c "comment"]]

Example: shutdown/i

SHUTDOWN: Turn off Computer

#8) SYSTEMINFO: System Information

This command helps to get system-related information like a network card, Windows OS, or details of the processor. The information provided by this command is easy to comprehend.

Syntax: systeminfo [/s <computer> [/u <domain>\<username> [/p <password>]]] [/fo {TABLE | LIST | CSV}] [/nh]

Example: C:\Users\systeminfo

System Information

#9) SFC: System File Checker

This command helps to detect any malware or virus threat by running a scan on the core system files. In order to run this command, Administrator rights are needed. On the CMD command prompt icon, use the right-click key and select the option RUN as Administrator.

Users need to type SFC/SCANNOW runs a diagnostic check to ensure all files are safe from malware and in case of any threat of malware, these files are repaired using the backup files.

Syntax: SFC [/scannow] [/verifyonly] [/scanfile=<file>] [/verifyfile=<file>] [/offwindir=<offline windows directory> /offbootdir=<offline boot directory>]

Example: C:\Users\SFC

System File Checker

RUN as Administrator

#10) .NET USE: Map Drives

This command is used for mapping a new drive. Users also have an option to use File Explorer and use Map Network Drive Wizard, if a new drive needs to be mapped, however, this command makes the process quick through one string of command.

The command syntax is– Net use (drive name)\\OTHER-COMPUTER\SHARE/persistent.yes . This is considering that \\OTHER-COMPUTER\SHARE is a shared folder on the computer and needs to be mapped to a new drive. It is important to use “persistent” here as it ensures that every time the computer is logged onto, the drive is revamped.

Syntax: Net use (drive name)\\OTHER-COMPUTER\SHARE/persistent.yes

Example: Net use /Persistent: Yes

#11) CHKDSK: Check Disk

This command is a step ahead of the SFC command. It allows the scanning of the complete drive as against the scanning of the core system files done by the SFC command. This command needs to be run as an administrator, and the syntax is CHKDSK/f (drive name). In the below screenshot, we can see that the command could not be executed as Administrator rights were missing.

Syntax: chkdsk [<volume>[[<path>]<filename>]] [/f] [/v] [/r] [/x] [/i] [/c] [/l[:<size>]] [/b]

Example: chkdsk C:

Check Disk13

Some important parameters for this command are explained below-

Parameter /f: This parameter helps to fix any errors on the disk. In order to use this parameter, the disk must be locked.

Parameter /v: This parameter shows the name of all files in all directories as the process of checking the disk progresses.

#12) SCHTASKS: Schedule Task

This command is another option apart from the inbuilt wizard in Windows when a schedule for tasks has to be created. Tasks can be scheduled by using the Schedule Task wizard or simply by using the command SCHTASKS.

The frequency of the tasks can be minute, hourly, daily, or monthly and can be set by the /MO command. If the command execution is successful, the following response can be seen- SUCCESS: The Scheduled Task “name of task” has been created.

Syntax:

schtasks change

schtasks create

schtasks delete

schtasks end

schtasks query

schtasks run

Example- C :\Users\schtasks

SCHTASKS: Schedule Task

This command also has some important parameters which make this command more useful. These have been discussed below-

Parameter /sc: This parameter specifies the schedule a particular task will follow.

Parameter /tn: This parameter describes the name of each task. It is important that every task has a name that is unique and complies with the rules of the file name. The name should not be more than 238 characters.

Parameter /s: This parameter shows details like the name and IP address of a remote computer. The local computer is the default output for this command.

#13) ATTRIB: Change File Attributes

Windows OS allows users to change the attributes of a file. The first step is to find the file and then find the property that needs to be changed. There is a simple command as well available in Windows which can be used to change the attributes of a file. It is – ATTRIB.

Syntax: Attrib [{+|-}r] [{+|-}a] [{+|-}s] [{+|-}h] [{+|-}i] [<drive>:][<path>][<filename>] [/s [/d] [/l]]

ATTRIB: Change File Attributes

Example- C:\Users\Attrib /?

ATTRIB

Some of the other parameters used for ‘attrib’ command are mentioned below-

Parameter {+|-}r: This parameter sets or clears the read-only file attribute. (+) is used for setting the attribute and (-) for clearing the attribute.

Parameter /s: This parameter uses 'attrib' and command-line options to similar files. Similar files can either be in the current directory or in any of the subdirectories.

Apart from the above-mentioned commands, there are a few more popular commands which are commonly used. Some of these commands are listed below-

a) BITSADMIN: This command is useful when uploading or downloading of data is done either within a network or through the Internet. It also helps to keep a check of the file transfer.

Syntax: bitsadmin [/RAWRETURN] [/WRAP | /NOWRAP] command

BITSADMIN

Some of the important parameters of this command are discussed below:

Parameter /list: This parameter is used to list all the jobs.

Parameter- gettype: This parameter shows the GUID or the display name of the job.

b) COLOR: This command helps to make changes to the background and foreground color of the command prompt window.

Syntax: color [[<b>]<f>]

Example: color /?

COLOR

We discuss some more parameters of this command below-

Paramater <b>: This parameter is used to change the background color. When this parameter is used in the format 'color b1'– it changes the background color to blue.

color b1

Parameter <f>: This parameter is used to change the background color. When this parameter is used in the format 'color fc', it changes the foreground color to red.

color fc'

c) COMP: This command allows the user to make a comparison between two files and capture differences.

Syntax: comp [<data1>] [<data2>] [/d] [/a] [/l] [/n=<number>] [/c]

d) FIND/FINDSTR: This command allows users to search ASCII files for any strings.

Syntax- findstr [/b] [/e] [/l | /r] [/s] [/i] [/x] [/v] [/n] [/m] [/o] [/p] [/f:<file>] [/c:<string>] [/g:<file>] [/d:<dirlist>] [/a:<colorattribute>] [/off[line]] <strings> [<drive>:][<path>]<filename>[…]

e) PROMPT: Using this command, the command prompt can be changed to another drive from C:\>.

Syntax: prompt [<text>]

Example- prompt –$g In this example, the command will display an arrow (–>) type.

PROMPT

f) TITLE: This command is used to make alterations to the title of the command prompt window.

Syntax: title [<string>]

Example: title /?

Parameter <string>: This parameter helps to set the title of the command prompt. It specifies the text which shows as the title of the command prompt.

title

g) REGEDIT: This command is extremely popular when keys are edited in the Windows registry. This command should be used very carefully.

Syntax:

reg add

reg compare

reg copy

reg delete

reg export

reg import

reg load

reg query

reg restore

reg save

reg unload

h) ROBOCOPY: This command is used to copy files or directories from a particular location to a different location. It can also be used to copy an entire drive.

Syntax: robocopy <source> <destination> [<file>[…]] [<options>]

Now, let us also discuss some CMD commands for Network.

CMD Network Commands

#14) IPCONFIG: IP Configuration

This command is extremely useful when troubleshooting for the network is required. When we type IPCONFIG in the command prompt, we get detailed information like IP address, Subnet Mask, Default Gateway IP, and current domain about the network. These details are important in the troubleshooting process of the router or any other connectivity issue.

Syntax: ipconfig [/allcompartments] [/all] [/renew [<adapter>]] [/release [<adapter>]] [/renew6[<adapter>]] [/release6 [<adapter>]] [/flushdns] [/displaydns] [/registerdns] [/showclassid <adapter>] [/setclassid <adapter> [<classID>]]

Example-C:\Users\IPCONFIG

IPCONFIG

IPCONFIG 23

#15) Network Statistics NETSTAT

This command ensures the prevention of any virus attack on the computer. We need to type “NETSTAT” in the command prompt and we get details of all the TCP connections which are currently active.

Syntax: NETSTAT [-a] [-b] [-e] [-n] [-o] [-p <Protocol>] [-r] [-s] [<interval>]

Example: C:\Users\Netstat (shows active connections)

Network Statistics NETSTAT

#16) TRACERT: TRACEROUTE

TRACERT is a really interesting command offered by Windows. It is especially meant for users who want to look at the routing of Internet traffic from their own browser to any remote system like a Google server. As the name suggests, it traces the route of the packets which are sent to a remote address which can be a website or even a server.

The information this command provides includes:

Number of hops (number of intermediate or connecting servers) before the destination was reached.

Time taken to reach each of these hops.

Name of the hops and the IP address of the hops.

This command wonderfully displays the route and hops of any Internet request and how these change when the location to access the web changes. It also helps to detect glitches in a router or a switch on a local network.

Syntax: TRACERT [/d] [/h <maximumhops>] [/j <hostlist>] [/w <timeout>] [/R] [/S <srcaddr>] [/4][/6] <targetname>

Example: C:\Users\ Username>TRACERT google.com

TRACE ROUTE 11

#17) PING: Send Test Packets

This command is extremely useful, especially for IT Professionals. It helps the analyst run checks if the computer is able to access and connect to another computer or another network. It also helps to detect if there are any issues with the connection.

This command also tracks the time for sending packets and this time is calculated in milliseconds, which is quick enough to detect any network glitches. In the below screenshot, the required details can be entered in the format specified to get the information.

Syntax: PING [/t] [/a] [/n <count>] [/l <size>] [/f] [/I <TTL>] [/v <TOS>] [/r <count>] [/s <count>] [{/j <hostlist> | /k <hostlist>}] [/w <timeout>] [/R] [/S <Srcaddr>] [/4] [/6] <targetname>

Example: C:\Users\username\ PING[-t]

Send Test Packets

Some of the parameters used for this command are mentioned below:

Parameter /t: This parameter is used to send Ping requests to a specific destination until there is an interruption.

Parameter /n<count>: This parameter states the count of echo requests sent. The default count is 4.

#18) PathPing

This command serves the same purpose as that of TRACERT but yields more information. It provides a detailed analysis of the route that a packet sent to a particular destination takes. It also provides information for loss of packet at each hop it takes.

Syntax: pathping [/n] [/h <maximumhops>] [/g <hostlist>] [/p <Period>] [/q <numqueries> [/w <timeout>] [/i <IPaddress>] [/4 <IPv4>] [/6 <IPv6>][<targetname>]

Example: C:\ Users\pathping www.google.com

PathPing

#19) GETMAC Media Access Control

Media Access Control is a unique address that is assigned by the manufacturing company to all the devices which meet the standards of IEE 802. This MAC address also helps users to keep control of devices that are allowed to connect to the network. It is possible to see multiple MAC addresses, and this is because there could be multiple network related adapters on the network.

Syntax: getmac[.exe][/s <computer> [/u <domain\<user> [/p <password>]]][/fo {table | list | csv}][/nh][/v]

Example: C:\Userss\getmac /?

Media Access Control

#20) NSLOOKUP- Name Server Lookup

This command helps the users to find the records pertaining to the name server of any domain name.

Syntax: nslookup [exit | finger | help | ls | lserver | root | server | set | view] [options]

Example: C:\Users\Username>nslookup

NSLOOKUP

#21) NETSH- NETWORK SHELL

This command is a network command which is used for gathering details of network adapters available on the system. It helps to check and set up the network adapters.

Syntax: netsh [-a <Aliasfile>][-c <Context>][-r <Remotecomputer>][-u [<domainname>\<username>][-p <Password> | [{<NetshCommand> | -f <scriptfile>}]

Example: C:\Users\netsh dump \?

NETSH- NETWORK SHELL

Parameter /?: This parameter shows the list of commands.

Parameter dump: This parameter displays a configuration script.

Parameter dump

Parameter netsh

#22) ARP

Arp command allows the user to show, delete, and make additions to ARP information of the devices on the network.

Syntax: arp [/a [<inetaddr>] [/n <ifaceaddr>]] [/g [<inetaddr>] [-n <ifaceaddr>]] [/d <inetaddr> [<ifaceaddr>]] [/s <inetaddr> <etheraddr> [<ifaceaddr>]]

ARP

Example: C:\Users\arp –a

inetaddr

#23) NBTSTAT

This command helps to show all the current protocol statistics and current TCP/IP connections (NETBIOS over TCP/IP). It uses NBT to resolve issues related to NETBIOS name resolution.

Syntax: nbtstat [/a <remotename>] [/A <IPaddress>] [/c] [/n] [/r] [/R] [/RR] [/s] [/S] [<interval>]

Example: C:\Users\nbtstat

NBTSTAT

#24) Finger

This command helps to gather information about the user. This can include information related to the last login, last read time for emails, etc.

Syntax: finger [-l] [<user>] [@<host>] […]

Finger

Example: finger @ host: This parameter specifies the server on the remote system from which user information is required.

finger @ host

#25) Hostname

This command shows the hostname of the computer.

Syntax: hostname

Example: C:\Users\hostname

Hostname

#26) Net

This command allows the user to see and find out details of the network settings and update and solve network related issues.

Syntax: net [accounts | computer | config | continue | file | group | help | helpmsg | localgroup | name | pause | print | send | session | share | start | statistics | stop | time | use | user | view]

Example: C:\Users\net [accounts]

Net

#27) Route

This command is used to check and make changes to the route table of the computer.

Syntax: route [-f] [-p] [-4|-6] command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]

Route

Example: C:\Users\route. PRINT

PRINT

#28) WHOIS

This command is useful when users want to find the domain name or the IP address. It searches the WHOIS database for relevant objects.

Syntax: whois [-h HOST] [-p PORT] [-aCFHlLMmrRSVx] [-g SOURCE:FIRST-LAST]

[-i ATTR] [-S SOURCE] [-T TYPE] object

Example: whois [-h]

Note: This command could not be executed due to admin restrictions.

Parameter whois –v: This parameter is used to print the whois information for the domain name.

Usage: whois.exe[-v]domainname [whois.server]

Interestingly, there are some useful tricks of command prompt which helps to enhance the experience of using Windows CMD commands and will prove to be time-saving as well.

Let us share some of the useful tricks below-

CMD Command Tricks

#1) Command History

This trick helps users to recall commands which have been used in the past but they are not able to recall.

Trick: doskey/history

Command History

#2) Run multiple commands

This trick is very efficient and time-saving when more than one command needs to be run back to back. All we need to do is to use “&&” between the two commands.

Example: assoc.txt && IPCONFIG

Run multiple commands 44

#3) Function keys and their usage

We have discussed an extensive list of commands available in the command prompt. Now, you must be thinking if you need to remember all of them? The answer is No.

We have been talking about the user-friendliness of Command Prompt in Windows and trust me, in case one forgets these commands, it is easy to retrieve the list of commands.

Follow the below-mentioned steps-

Step 1: Open the Command Prompt by clicking on the Start Menu and typing cmd. Alternatively, one can also use a shortcut- Ctrl+R (key), and on the Run dialogue box, type cmd, and press Enter.

Step 2: In order to retrieve the list of commands- Type Help and press Enter. This will help to list down all the commands in alphabetic order, and the commands can be found by scrolling up and down. The list may vary depending upon the version of Windows used.

Below is a list of the function keys which can help to enhance the experience with CMD commands.

CMD commands

#4) Send output to clipboard

This trick is very useful and efficient when the result or output of command needs to be saved. This trick saves a lot of time by saving the output of the command to the Windows clipboard as against the traditional copy and paste method.

Trick: Assoc.txt| clip

#5) Abort Command

This trick helps to stop the execution of command if the Enter key has been pressed by mistake.

Trick: CTRL+C

Command Prompt is a part of all systems with Windows NT based operating system. The list of commands which are available in the command prompt is long however these commands and their availability may be different on different versions of Windows Operating Systems like Windows 7, Windows 8, etc.

There are advanced versions of Command prompt in Windows which are called PowerShell and are now a part of the latest versions of Windows. PowerShell serves the purpose of a booster to the running of commands in Command Prompt. It is believed that in the newer versions of Windows, Windows PowerShell may substitute command prompt.

Below are some of the frequently asked questions about Windows Command Prompt.

Frequently Asked Questions

Q #1) How can we change the name of CMD?

Answer: In order to change the name of CMD, the following steps are to be followed-

Step1: Use the Start icon and click to select Settings.

Step2: Select the “System”.

Step3: Select “Rename PC” which can be seen under the tab “About”.

Step4: Enter the new name and select Next.

Step5: It is important to restart the system so that the settings can be applied. Select Restart Now.

Q #2) Where can we find CMD.exe?

Answer: The following path is to be followed to locate CMD.exe- C:\\Windows\System32 folder.

Q #3) Why do we use CMD?

Answer: CMD allows users to perform all the functions which are done using the graphical interface in Windows. CMD can be used to copy, rename, or delete files. It even allows users to run applications and alter settings.

Q #4) How can we fix Windows system32 cmd exe?

Answer: Select Windows+ R key to open Run Dialogue box and type msconfig. A dialogue box called System Configuration will pop up. Use the “StartUp” tab. Check if C:\WINDOWS\system32\cmd.exe is listed. If it is found to be listed, uncheck the box and select Apply. The system needs to be restarted for the changes to take effect.

Q #5) How many CMD commands are there?

Answer: In Windows, there are as many as 280 commands which can be accessed through the Command Prompt. They help the users to automate various tasks of a repeated nature and also help in solving some of the problems with the Windows Operating System.

cmd command	Description
Basics:	
call	calls a batch file from another one
cd	change directory
cls	clear screen
cmd	start command prompt
color	change console color
date	show/set date
dir	list directory content
echo	text output
exit	exits the command prompt or a batch file
find	find files
hostname	display host name

pause	pauses the execution of a batch file and shows a message
runas	start a program as another user
shutdown	shutdown the computer
sort	sort the screen output
start	start an own window to execute a program or command
taskkill	terminate a process or a application
tasklist	display applications and related tasks
time	display/edit the system time
timeout	wait any time
title	set title for prompt
ver	display operating system version
w32tm	setting time synchronisation/time server/time zone
Network:	
ftp	transfer files to a FTP server
ftype	display file type and mapping
getmac	display MAC address

ipconfig	display IP network settings
netsh	configure/control/display network components
netstat	display TCP/IP connections and status
nslookup	query the DNS
pathping	test the connection to a specific IP address
ping	pings the network
route	display network routing table, add static routes
systeminfo	displays computer-specific properties and configurations
telnet	establish Telnet connection
tftp	transfer files to a TFTP server
tracert	trace routes similar to patchping
Files:	
attrib	display file attributes
comp	compare file contents
compact	display/change file compression
copy / xcopy	copy files

diskcomp	compare content of two floppy disks
diskcopy	copy floppy disc to another one
erase / del	delete one or more files
expand	extract files
fc	copare files and display the differences
mkdir	create a new directory
move	move/rename files
rename	rename files
replace	replace files
rmdir / rd	delete directory
tree	display folder structure graphically
type	display content of text files
Media:	
chkdsk	check volumes
chkntfs	display/change volume check at startup
defrag	defragment media

diskpart	volume management
driverquery	display installed devices and their properties
format	format volumes
label	change volume name
mode	configure interfaces/devices
mountvol	assign/delete drive mountpoints
verify	monitoring whether volumes are written correctly
vol	show volume description and serial numbers of the HDDs
Miscellaneous:	
for	for loop
gpresult	display group policies
gpupdate	update group policies
perfmon	start performance monitor
prompt	change command prompt
reg	add/read/import/export registry entries

Linux Commands:

Command	Description
cat [filename]	Display file's contents to the standard output device (usually your monitor).
cd /directorypath	Change to directory.
chmod [options] mode filename	Change a file's permissions.
chown [options] filename	Change who owns a file.
clear	Clear a command line screen/window for a fresh start.
cp [options] source destination	Copy files and directories.
date [options]	Display or set the system date and time.
df [options]	Display used and available disk space.
du [options]	Show how much space each file takes up.
file [options] filename	Determine what type of data is within a file.
find [pathname] [expression]	Search for files matching a provided pattern.
grep [options] pattern [filesname]	Search files or output for a particular pattern.
kill [options] pid	Stop a process. If the process refuses to stop, use kill -9 pid.
less [options] [filename]	View the contents of a file one page at a time.

ln [options] source [destination]	Create a shortcut.
locate filename	Search a copy of your filesystem for the specified filename.
lpr [options]	Send a print job.
ls [options]	List directory contents.
man [command]	Display the help information for the specified command.
mkdir [options] directory	Create a new directory.
mv [options] source destination	Rename or move file(s) or directories.
passwd [name [password]]	Change the password or allow (for the system administrator) to change any password.
ps [options]	Display a snapshot of the currently running processes.
pwd	Display the pathname for the current directory.
rm [options] directory	Remove (delete) file(s) and/or directories.
rmdir [options] directory	Delete empty directories.
ssh [options] user@machine	Remotely log in to another Linux machine, over the network. Leave an ssh session by typing exit.
su [options] [user [arguments]]	Switch to another user account.
tail [options] [filename]	Display the last n lines of a file (the default is 10).
tar [options] filename	Store and extract files from a tarfile (.tar) or tarball (.tar.gz or .tgz).
top	Displays the resources being used on your system. Press q to exit.

touch filename	Create an empty file with the specified name.
who [options]	Display who is logged on.

Directory Structure

In the FHS, all files and directories appear under the root directory / , even if they are stored on different physical or virtual devices. Some of these directories only exist on a particular system if certain subsystems, such as the X Window System, are installed.

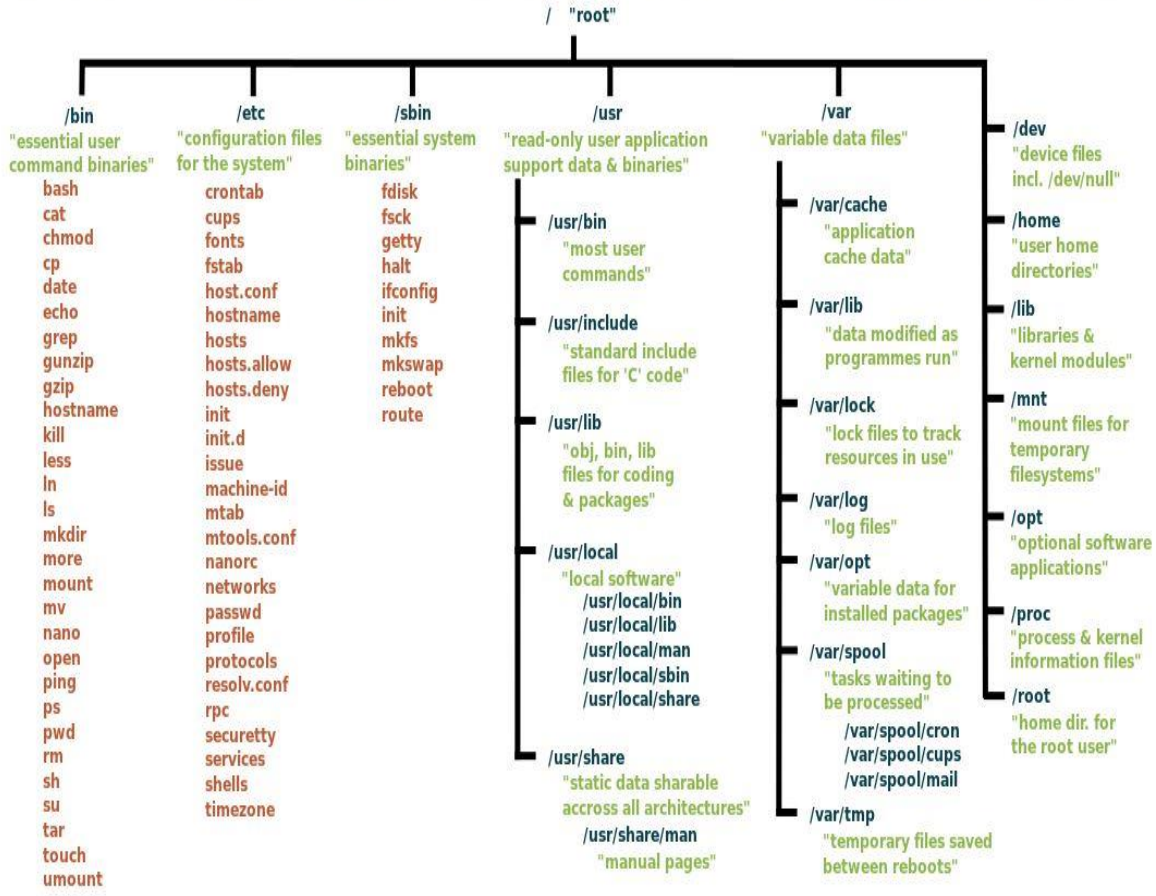
Most of these directories exist in all Unix-like operating systems and are generally used in much the same way; however, the descriptions here are those used specifically for the FHS, and are not considered authoritative for platforms other than Linux.

Directory	Description
/	*Primary hierarchy* root and root directory of the entire file system hierarchy.
/bin	Essential command binaries that need to be available in single user mode; for all users, *e.g.*, cat, ls, cp.
/boot	Boot loader files, *e.g.*, kernels, initrd.
/dev	Device files, *e.g.*, /dev/null , /dev/disk0 , /dev/sda1 , /dev/tty , /dev/random.
/etc	Host-specific system-wide configuration files. There has been controversy over the meaning of the name itself. In early versions of the UNIX Implementation Document from Bell labs, /etc is referred to as the *etcetera directory*, as this directory historically held everything that did not belong elsewhere (however, the FHS restricts /etc to static configuration files and may not contain binaries). Since the publication of early documentation, the directory name has been re-explained in various ways. Recent interpretations include acronyms such as "Editable Text Configuration" or "Extended Tool Chest."
/etc/opt	Configuration files for add-on packages that are stored in /opt .
/etc/sgml	Configuration files, such as catalogs, for software that processes SGML.
/etc/X11	Configuration files for the X Window System, version 11.
/etc/xml	Configuration files, such as catalogs, for software that processes XML.
/home	Users' home directories, containing saved files, personal settings, etc.
/lib	Libraries essential for the binaries in /bin and /sbin .

/lib<qual>	Alternative format essential libraries. Such directories are optional, but if they exist, they have some requirements.
/media	Mount points for removable media such as CD-ROMs (appeared in FHS-2.3 in 2004).
/mnt	Temporarily mounted filesystems.
/opt	Optional application software packages.
/proc	Virtual filesystem providing process and kernel information as files. In Linux, corresponds to a procfs mount. Generally automatically generated and populated by the system, on the fly.
/root	Home directory for the root user.
/run	Run-time variable data: Information about the running system since last boot, *e.g.*, currently logged-in users and running daemons. Files under this directory must be either removed or truncated at the beginning of the boot process, but this is not necessary on systems that provide this directory as a temporary filesystem (tmpfs).
/sbin	Essential system binaries, *e.g.*, fsck, init, route.
/srv	Site-specific data served by this system, such as data and scripts for web servers, data offered by FTP servers, and repositories for version control systems (appeared in FHS-2.3 in 2004).
/sys	Contains information about devices, drivers, and some kernel features.
/tmp	Temporary files (see also /var/tmp). Often not preserved between system reboots, and may be severely size restricted.
/usr	*Secondary hierarchy* for read-only user data; contains the majority of (multi-)user utilities and applications.
/usr/bin	Non-essential command binaries (not needed in single user mode); for all users.
/usr/include	Standard include files.
/usr/lib	Libraries for the binaries in /usr/bin and /usr/sbin.
/usr/lib<qual>	Alternative format libraries, *e.g.* /usr/lib32 for 32-bit libraries on a 64-bit machine (optional).
/usr/local	*Tertiary hierarchy* for local data, specific to this host. Typically has further subdirectories, *e.g.*, bin , lib , share .
/usr/sbin	Non-essential system binaries, *e.g.*, daemons for various network-services.
/usr/share	Architecture-independent (shared) data.
/usr/src	Source code, *e.g.*, the kernel source code with its header files.
/usr/X11R6	X Window System, Version 11, Release 6 (up to FHS-2.3, optional).
/var	Variable files—files whose content is expected to continually change during normal operation of the system—such as logs, spool files, and temporary e-mail files.
/var/cache	Application cache data. Such data are locally generated as a result of time-consuming I/O or calculation. The application must be able to regenerate or restore the data. The cached files can be deleted without loss of data.
/var/lib	State information. Persistent data modified by programs as they run, *e.g.*, databases, packaging system metadata, etc.
/var/lock	Lock files. Files keeping track of resources currently in use.

/var/log	Log files. Various logs.
/var/mail	Mailbox files. In some distributions, these files may be located in the deprecated /var/spool/mail .
/var/opt	Variable data from add-on packages that are stored in /opt .
/var/run	Run-time variable data. This directory contains system information data describing the system since it was booted. In FHS 3.0, /var/run is replaced by /run ; a system should either continue to provide a /var/run directory, or provide a symbolic link from /var/run to /run , for backwards compatibility.
/var/spool	Spool for tasks waiting to be processed, *e.g.*, print queues and outgoing mail queue.
/var/spool/mail	Deprecated location for users' mailboxes.
/var/tmp	Temporary files to be preserved between reboots.

In a pictorial manner, here is what the filesystem looks like. Some of these directories have standard files as well - /bin, /etc and /sbin specifically.



HOW-TO

How to Find your Windows 10 Product Key

By Andre Da Costa

Last Updated on October 12, 2021

Microsoft has made every effort to make Windows 10 licensing convenient. That said, there are times where product **activation might not work** according to plan. Whether you want to perform a new install or **transfer your Windows 10 license to a new computer**, your product key is an important asset you need to have. Depending on how you acquired Windows 10, you might not have a Windows 10 product key; in some cases, you do, here is how you find it.

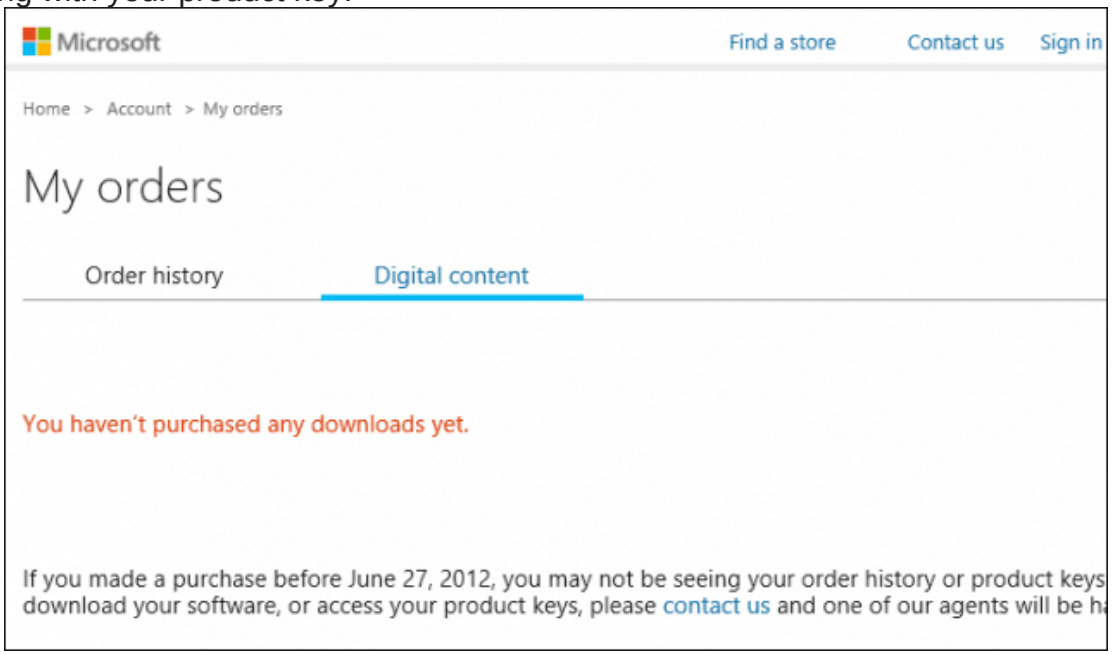
Locate Your Windows 10 Product Key

First, let's start with a purchased Windows product key or license as it is officially known. Windows 10 is licensed as a digital download or a full packaged product you can purchase at a physical store. Both Microsoft and Amazon.com are the **only** authorized online merchants from whom you can purchase a digital copy of Windows 10. Any other retailer selling you just a product key is likely not genuine; so, make sure you purchase a license only from Amazon or Microsoft if you decide to go the digital download route.

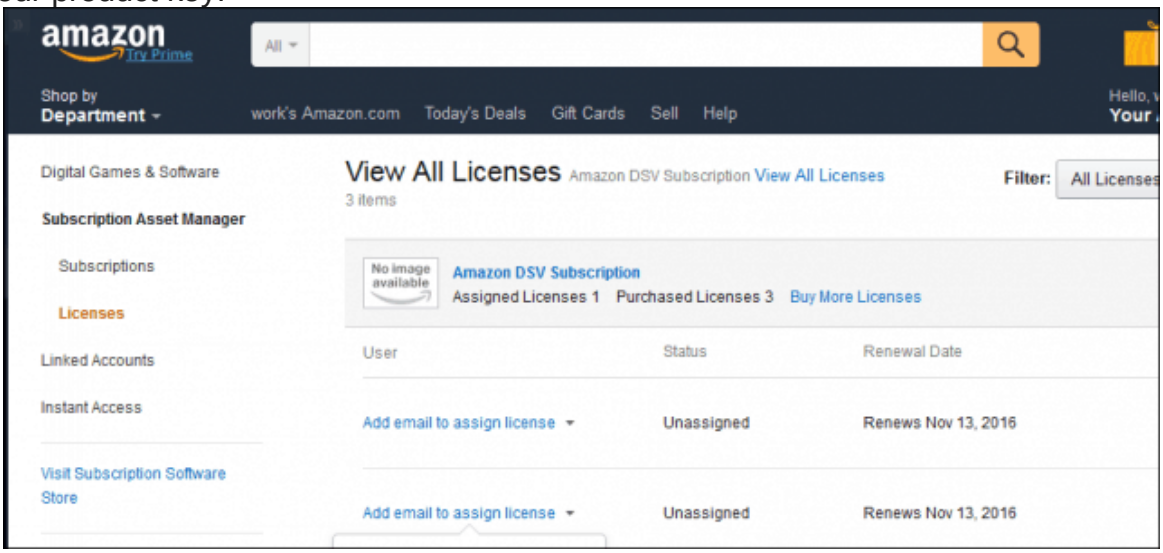
Another tip, if you **buy a license from Amazon, use this link**. Some have tried to save a few bucks by purchasing a license from the Amazon marketplace, only to find the license is an MSDN key and not valid.

When you purchase your **Windows 10 license from the Microsoft Store**, a copy of the product key is stored in your Microsoft Account. Microsoft will also send you a copy of the product key in a confirmation email. If you don't see the confirmation email, check your junk mail folder.

If you still don't find it, log into the **Microsoft Store** > Downloads > Product Keys > Subscription page. Then click the Digital Content tab to see your previous purchases along with your product key.



Amazon customers can visit the **Your Games and Software Library** section to find your product key.



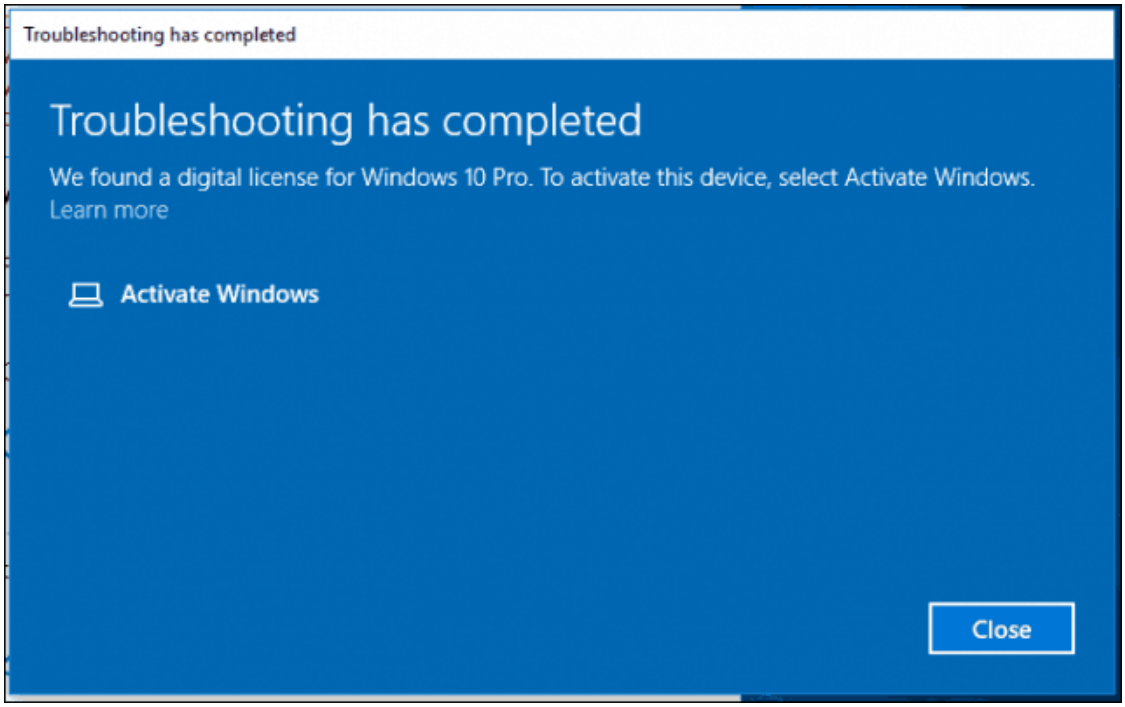
Windows 10 Pro Pack key

When you purchase a Windows 10 Pro Pack using the **Easy Upgrade** option in Windows 10 Home, you don't receive a product key. Instead, the **digital license is attached to your Microsoft Account**, used to make the purchase. If you decide to transfer the Windows 10 Pro Pack to another computer, you can use the **Activation Troubleshooter**.

s

Transfer Windows 10 Pro Pack Key to a new Computer

1. Open *Settings* > *Update & security* > *Activation* > *Troubleshooter*.
2. Sign in with your Microsoft Account used to purchase the Pro Pack license.
3. After troubleshooting is completed, Windows 10 will indicate a digital license for Windows 10 Pro has been found.
4. Click *Activate Windows,* then follow the on-screen wizard.



Retail Full Packaged Product

Windows 10 is also available as a **retail full packaged product** you can buy at a store. Inside the Windows 10 product box, you will find your product key on a small business card at the back. Users should make sure they store the product key in a safe place or have a backup copy. I also recommend you **use our trick to take a photo of the key and store it online** for safekeeping.

OEM System Builder License

The Windows 10 product key is normally found outside the package, on the Certificate of Authenticity. If you purchased your PC from a white box vendor, the sticker might be attached to the machine's chassis; so, look at the top or side to find it. Again, snap a photo of the key for safekeeping. After several years, I've found these keys like to rub off with normal wear-and-tear.

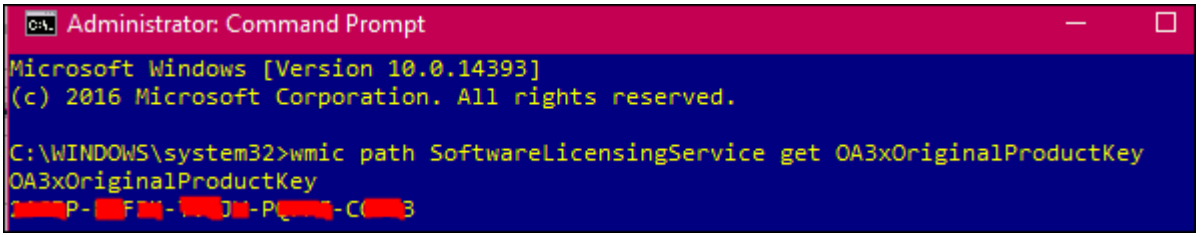
Find Windows 10 Product Key on a New Computer

The product key for new computers that come preinstalled with Windows 10 has the product key stored within the motherboard firmware. Users can retrieve it by issuing a command from the command prompt.

1. Press *Windows key + X*
2. Click *Command Prompt (Admin)*
3. At the command prompt, type:

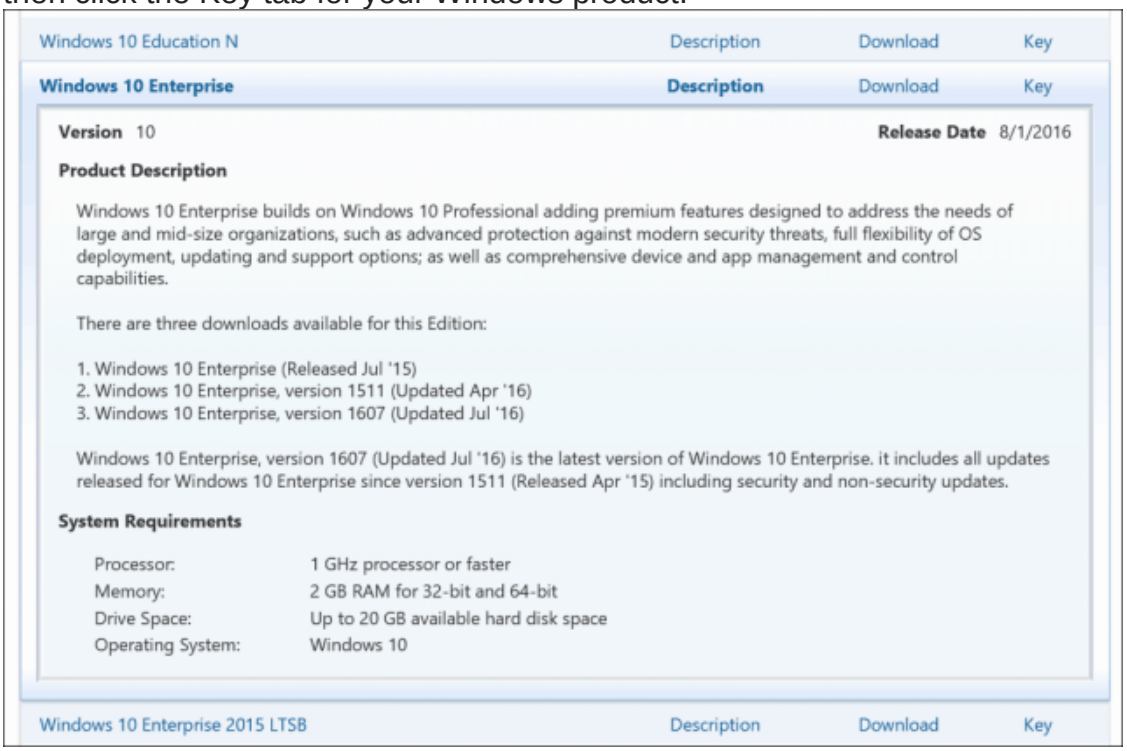
```
wmic path SoftwareLicensingService get OA3xOriginalProductKey
```

This will reveal the product key.



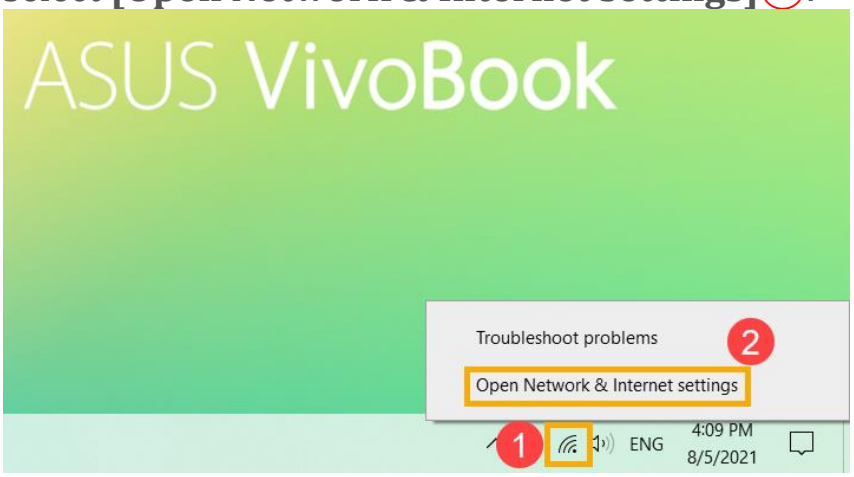
Volume License Product Key Activation

If you're using Windows 10 in a business environment, editions such as Windows 10 Pro, Enterprise, and Education don't use normal product keys. Instead, Domain Administrators set up special KMS (Key Management Service) servers that manage activation across the business network. This eliminates the need for computers to connect to Microsoft for activation. System Administrators responsible for deploying Windows 10 in an organization can find the product key from the **Volume License Service Center portal**; click the *Licenses* tab, then click the Key tab for your Windows product.

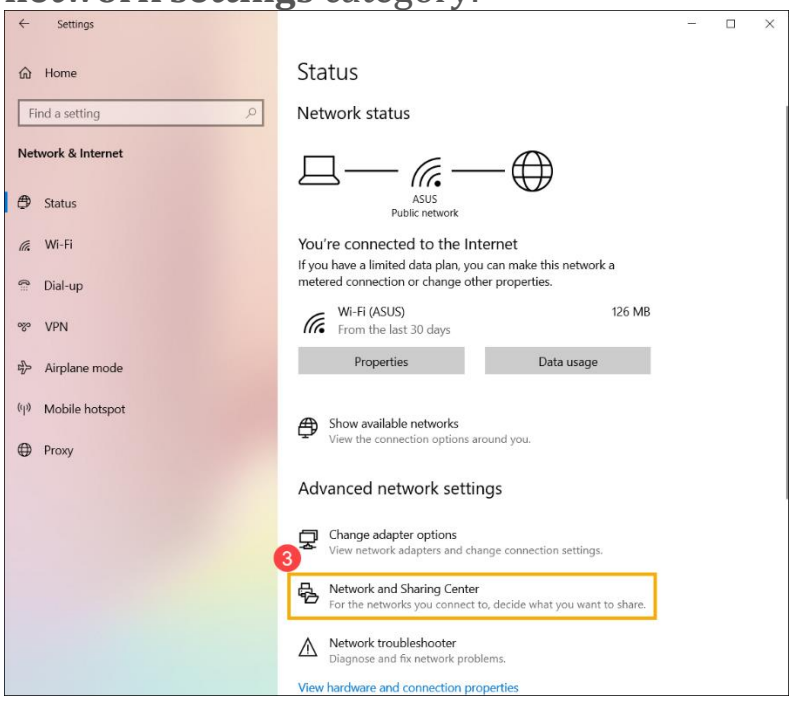


Method 1: Check the Wi-Fi password via Network & Internet settings

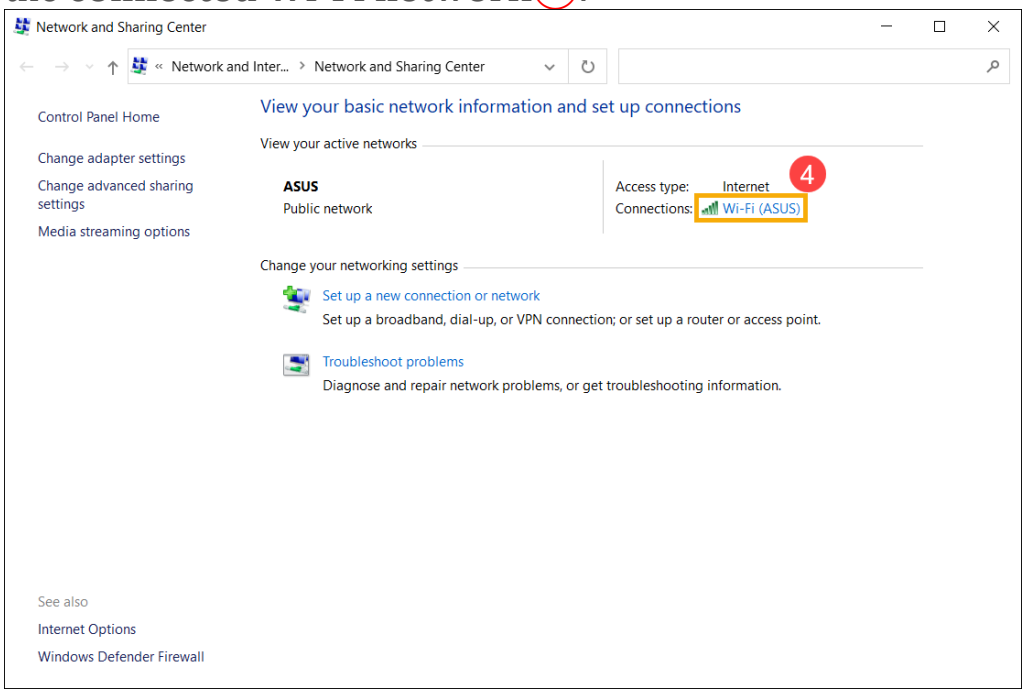
1. Please connect to Wi-Fi that you want to check the password, then right-click the **[Network]** icon ① on the taskbar and select **[Open Network & Internet settings]** ②.



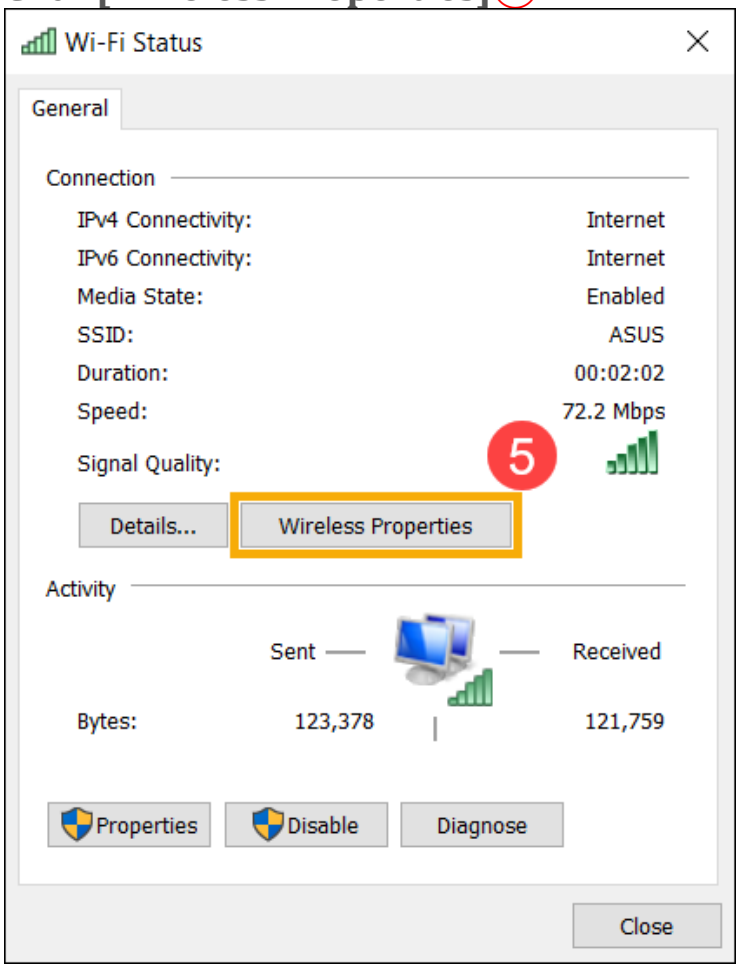
2. Select **[Network and Sharing Center]** ③ in the **Advanced network settings** category.



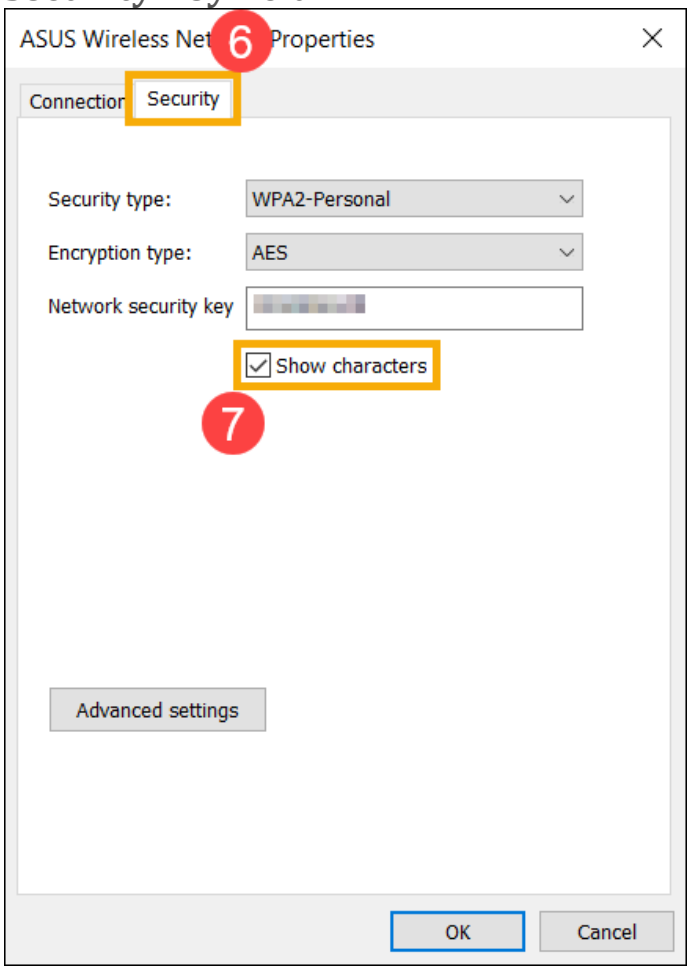
3. After entering the Network and Sharing Center window, click the **connected Wi-Fi network**④.



4. Click **[Wireless Properties]**⑤.

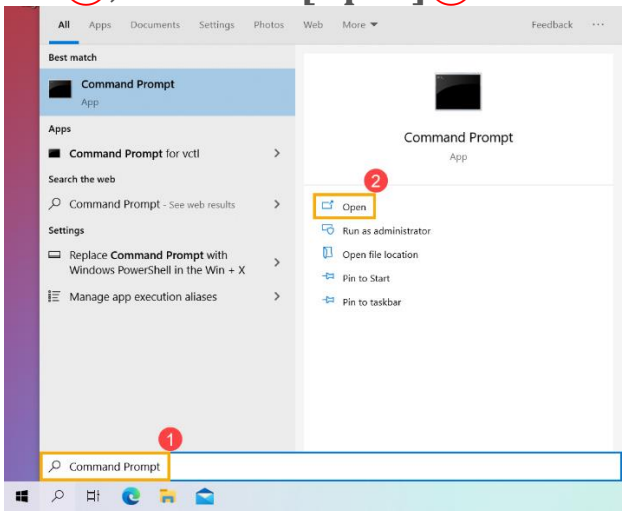


5. Select the **[Security]** tab⑥, and then check the box to **[Show characters]**⑦, you will find the Wi-Fi password in the **Network security key** field.

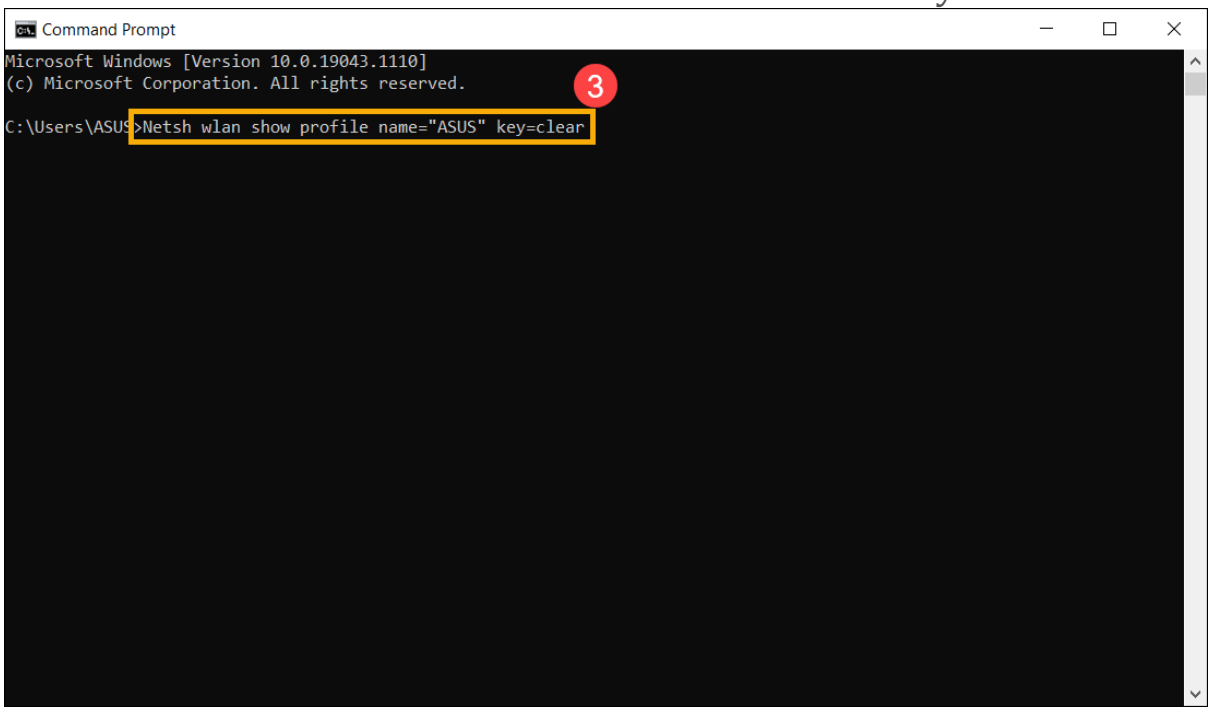


Method 2: Check the Wi-Fi password via Command Prompt

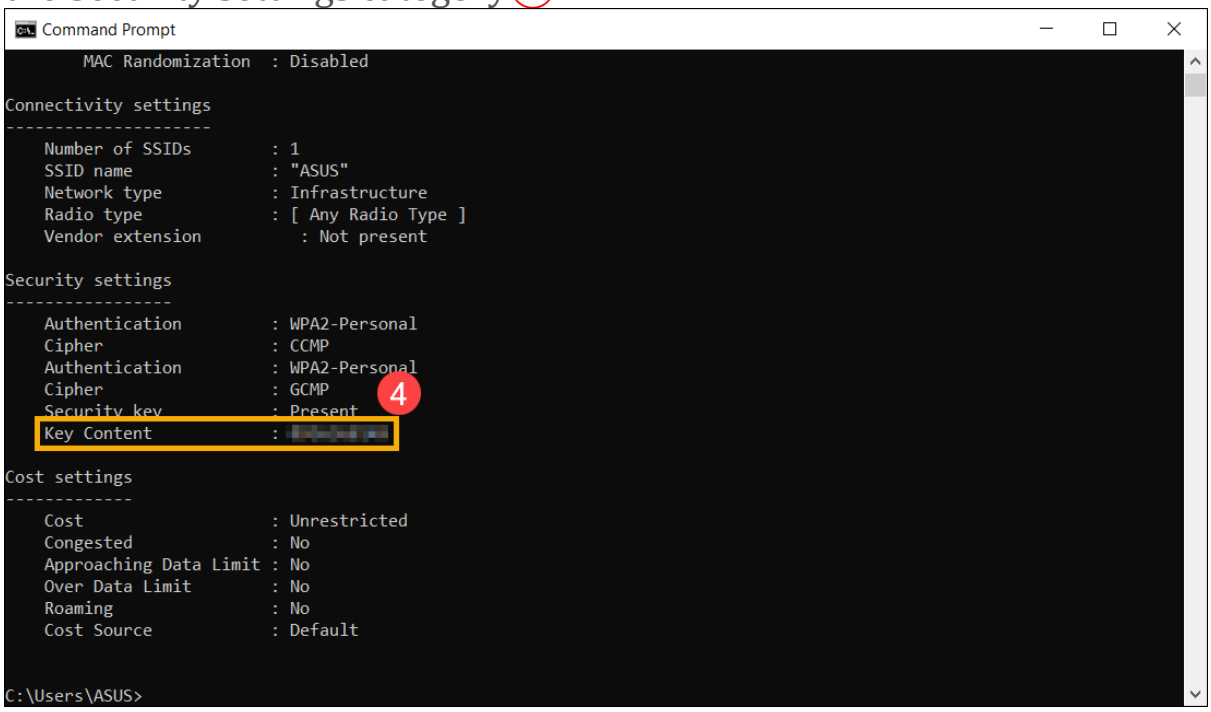
1. Type and search **[Command Prompt]** in the Windows search bar①, then click **[Open]**②.



2. In the Command Prompt window, type the command **[Netsh wlan show profile name=”Wi-F name” key=clear]**③, and then press Enter key.
   For example: Netsh wlan show profile name=”ASUS” key=clear, ASUS is a Wi-Fi name that has been connected currently.



3. You can find the Wi-Fi password in the **[Key Content]** field in the Security settings category④.



4. If you want to check all Wi-Fi passwords the computer has ever connected, you can use the following command. Press Enter key

after typing this command, you will find the passwords for each Wi-Fi.

[for /f "skip=9 tokens=1,2 delims=:" %i in ('netsh wlan show profiles') do @echo %j | findstr -i -v echo | netsh wlan show profiles %j key=clear]