NetWhat

What is an IP address?

The IP (Internet Protocol) is the fundamental protocol for communications on the Internet. It specifies the way information is packetized, addressed, transferred, routed, and received by networked devices.

Pocket definition: “An **IP address i**s a network address for your computer so the Internet knows where to send you emails, data and pictures of cats.”

Definition: An **IP address** is a number identifying of a computer or another device on the Internet. It is similar to a mailing address, which identifies where postal mail comes from and where it should be delivered. IP addresses uniquely identify the source and destination of data transmitted with the Internet Protocol.

What is public IP address?

A public IP address is the address that is assigned to a computing device to allow direct access over the Internet. A web server, email server and any server device directly accessible from the Internet are candidate for a public IP address. A public IP address is globally unique, and can only be assigned to a unique device.

What is private IP address?

A private IP address is the address space allocated by InterNIC to allow organizations to create their own private network. There are three IP blocks (1 class A, 1 class B and 1 class C) reserved for a private use. The computers, tablets and smartphones sitting behind your home, and the personal computers within an organizations are usually assigned private IP addresses. A network printer residing in your home is assigned a private address so that only your family can print to your local printer.

When a computer is assigned a private IP address, the local devices see this computer via it's private IP address. However, the devices residing outside of your local network cannot directly communicate via the private IP address, but uses your router's public IP address to communicate. To allow direct access to a local device which is assigned a private IP address, a Network Address Translator (NAT) should be used.

IP Routing

IP Routing describes the process of determining the path for data to follow in order to navigate from one computer or server to another. A packet of data traverses from its source router through a web of routers across many networks until it finally reaches its destination router using a routing algorithm. The routing algorithm takes into account factors such as the size of a packet and its header to determine the most efficient route to the destination. When a packet has reached a router, the source and destination address of the packet are used in conjunction with a routing table (list that contains the routes to a certain network) to determine the next hop address. This process is repeated for the next router using its own routing table until the packet has reached its destination. Because the data is divided into packets, each packet travels independently from each other and is treated as such. As a result, each packet can be sent through a different route to the destination if necessary.

Default Gateway

A gateway is a network node that serves as an access point to another network, often involving not only a change of addressing, but also a different networking technology. More narrowly defined, a router merely forwards packets between networks with different network prefixes. The networking software stack of each computer contains a routing table that specifies which interface is used for transmission and which router on the network is responsible for forwarding to a specific set of addresses. If none of these forwarding rules is appropriate for a given destination address, the default gateway is chosen as the router of last

resort. The default gateway can be specified by the route command to configure the node's routing table and default route.

A default gateway is the node in a computer network using the internet protocol suite that serves as the forwarding host (router) to other networks when no other route specification matches the destination IP address of a packet.

In a home or small office environment, the default gateway is a device, such as a DSL router or cable router, that connects the local network to the Internet. It serves as the default gateway for all network devices.

Netmask

A **netmask** is a 32-bit binary mask (a **mask** is a special value that acts as a data filter. It's called a "mask" because it reveals some parts of digital information, and conceals or alters others) used to divide an IP address into subnets and specify the network's available hosts.

In a netmask, two of the possible addresses, represented as the final byte, are always pre-assigned and unavailable for custom assignment. For example, in 255.255.225.0, "0" is the assigned network address. In 255.255.255.255, the final "255" is the assigned broadcast address. These two values cannot be used for IP address assignment.

Below is an example of a netmask and an example of its binary conversion.

Netmask:	255	255	255	255
Binary:	11111111	11111111	11111111	11111111
Netmask length	8	16	24	32

Counting out the bits in the binary conversion allows you to determine the netmask length. Above is an example of a 32-bit address. However, this address is a broadcast address and does not allow any hosts (computers or other network devices) to connect to it.

Subnet mask

Short for **subnetwork mask**, a **subnet mask** is data used for bitwise operations (A **bitwise operator** may be used in programming for operating on the individual bits of binary values) on a network of IP addresses that is divided into two or more groups. This process, known as **subnetting**, divides an IP network into blocks of logical addresses. Subnetting can improve security and help to balance overall network traffic.

A common example of a subnet mask for class C IP addresses is 255.255.255.0, the default subnet mask for many computers and network routers. When applied to **subnet**, a subnet mask shows the routing prefix.

Broadcast

In computer networking, **broadcasting** is sending data packets to multiple recipients all at once. For instance, a local area network can be configured so that any device on the network can broadcast a message to all the others.

When a networked device wants to broadcast, it transmits a data packet to the network's **broadcast address.** The network hardware, such as routers or switches, does the work of sending the packet to every other device in the group. The group of eligible devices is called a **broadcast domain.**
This type of communication is also called **all-to-all**, because every device can transmit a message simultaneously to every other device. Broadcast networking is supported by IPv4, the network protocol used by most of today's Internet. However, the newer IPv6 protocol deprecates broadcasting in favor of multicasting. Broadcasting is one of the five major techniques for

routing computer network traffic. The others are unicast, multicast, anycast, and geocast.

IPv4 and IPv6 addresses

IPv4 addresses are 32 bits long (four bytes). An example of an IPv4 address is 216.58.216.164, which is the front page of Google.com.

A major advantage of IPv6 is that it uses 128 bits of data to store an address, permitting 2128 unique addresses, or 340,282,366,920,938,463,463,374,607,431,768,211,456. The size of IPv6's address space – 340 duodecillion – is much, much larger than IPv4.

IP address classes

With an IPv4 IP address, there are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used. Each class allows for a range of valid IP addresses, shown in the following table.

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.

Class	Address range	Supports
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or research and development purposes.

TCP

Short for **Transmission Control Protocol**, **TCP** is a standard that dictates how to establish and maintain a connection through which two programs may exchange data. Invented in 1978 and driven by Bob Kahn and Vint Cerf, TCP is a core component in the TCP/IP protocol, which dictates how information is sent over the Internet.

How does it work?

TCP's job is to break down messages or files into smaller pieces (called packets) that are then sent over the Internet. These packets are then received by another TCP layer that then reassembles the data into a complete file or message. TCP is also responsible for error-checking that data stream to ensure the delivery of the data; if an error is found TCP retransmits the packet(s).

UDP

Short for **User Datagram Protocol** and defined in RFC 768, **UDP** is a network communications protocol. Also referred to as UDP/IP, it is an alternative to TCP/IP that sacrifices reliability for speed and simplicity.

Like TCP, UDP transfers packets using IP (Internet Protocol). However, it differs in what data the packets contain, and how the packets are handled by the sender and receiver.

Differences between TCP and UDP

Unlike TCP, UDP does not provide for error checking, or recovery of packets that were lost in transit.

TCP is *connection-oriented*. The protocol requires that a communication session is established, and that the sender and receiver agree about what data was transferred. When TCP packets are received and pass an error check, the receiver responds with an acknowledgement. If TCP packets are corrupted or lost in transit, the receiver does not send an acknowledgement, and the sender eventually re-sends those packets.

UDP is *connectionless*. The receiver can request and listen for UDP packets, but no session is established (there is no "beginning" or "end," data is merely sent and received). If UDP packets are corrupted or lost in transit, the receiver may not be aware of the error. The receiver does not report errors to the sender, or acknowledge that data was received.

OSI

Short for **Open System Interconnection**, **OSI** is a network model developed by ISO in 1978 where peer-to-peer communications are divided into seven layers. Each layer performs a specific task or tasks and builds upon the preceding layer until the communications are complete. Below are each of the seven layers.

1 - Physical layer - responsible for the electrical, mechanical, and timing across the link.

2 - Data link layer (also known as the link layer) - responsible for transmitting data across a link.

3 – Network layer – responsible for routing information through the network and allowing systems to communicate.

4 – Transport layer – responsible for transferring information between endpoints on the network and deals with errors, such as lost or duplicate packets.

5 – Session layer – responsible for managing a session between two applications.

6 – Presentation layer – responsible for the data formatting and display, allowing for compatibility.

7 – Application layer – responsible for user interaction. An example of an OSI application is the FTAM (Short for **file transfer, access, and management, FTAM** is an OSI-compliant standard for file transfers).

DHCP

Short for Dynamic Host Configuration Protocol, DHCP is a protocol used to assign an IP address to a computer or device connected to a network automatically. Routers, switches, or servers that use DHCP to assign addresses to other computers can make setup and management easier for the network administrator.

On a home network, DHCP can be set up by purchasing a home router, wireless router, or switch with NAT/DHCP and connecting each computer to it. If the network has a firewall, ports 67 and 68 need to be open for devices to function properly.

DNS

Short for Domain Name System, a DNS is a service that receives a request containing a domain name hostname and responds with the corresponding IP address. The first DNS was designed and implemented by Paul Mockapetris and Jon Postel in 1983.

How does DNS work?

When a user wants to visit Computer Hope, they can type "https://www.computerhope.com" into the address bar of their browser. Once that domain name is entered, it is looked up on a Domain Name System where it is translated into an IP address (e.g., 216.58.216.164). Using that IP address, your computer can then locate the Computer Hope web page and forward that information to your browser.not every DNS stores every address on the Internet. If a domain name is not found, the server may query other domain servers to obtain its address.

Difference between a domain name system and domain name server

The DNS acronym can be used for "Domain Name System" and "domain name server" and although they share the same acronym they have different meanings. A Domain Name System is the overall system used to make a domain name an IP address as explained above. A domain name server is an individual server that is part of the Domain Name System, which may be comprised of multiple domain name servers.

Port

In computer networking, a port is a communication endpoint. At the software level, within an operating system, a port is a logical construct that identifies a specific process or a type of network service. A port is identified for each transport protocol and address combination by a 16-bit unsigned number, known as the port number. The most common transport protocols that use port numbers are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

A port number is always associated with an IP address of a host and the type of transport protocol used for communication. 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. For this purpose, port numbers lower than 1024 identify the historically most commonly used services and are called the well-known port numbers. Higher-numbered ports are

available for general use by applications and are known as ephemeral ports.

Network behavior

Transport layer protocols, such as the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP), transfer data using protocol data units (PDUs). For TCP, the PDU is a segment, and a datagram for UDP. Both protocols use a header field for recording the source and destination port number. The port numbers are encoded in the transport protocol packet header, and they can be readily interpreted not only by the sending and receiving computers, but also by other components of the networking infrastructure. In particular, firewalls are commonly configured to differentiate between packets based on their source or destination port numbers. Port forwarding is an example application of this.

https://www.computerhope.com/jargon/i/ip.htm
https://www.computerhope.com/jargon/n/netmask.htm
https://www.computerhope.com/jargon/s/subnetma.htm
https://www.iplocation.net/public-vs-private-ip-address#:~:text=A%20public%20IP%20address%20is,be%20accessed%20over%20the%20Internet.&text=Private%20IP%20address%2C%20on%20the,directly%20expose%20to%20the%20Internet.
https://www.computerhope.com/jargon/t/tcp.htm
https://www.computerhope.com/jargon/u/udp.htm
https://www.computerhope.com/jargon/o/osi.htm
https://www.computerhope.com/jargon/d/dhcp.htm
https://www.computerhope.com/jargon/d/dns.htm
https://www.sangoma.com/how-ip-routing-works/#:~:text=IP%20Routing%20describes%20the%20process,router%20using%20a%20routing%20algorithm.
https://en.wikipedia.org/wiki/Default_gateway
https://en.wikipedia.org/wiki/Port_(computer_networking)#:~:text=A%20port%20number%20is%20always,network%20address%20of%20a%20message.