IP addressing

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.

The address space of IPv4 is 2^{32} or 4,294,967,296.

Notations

Binary Notation

In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address.

01110101 10010101 00011101 00000010

Dotted-Decimal Notation

To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes.

117.149.29.2

Hexadecimal

To make the IPv4 address more compact addresses can be written in hexadecimal form where each byte is represented by its hexadecimal value.

75 95 1D 02

Convert the IP address whose hexadecimal representation is C22F1582 to dotted decimal notation.

The address is 194.47.21.130

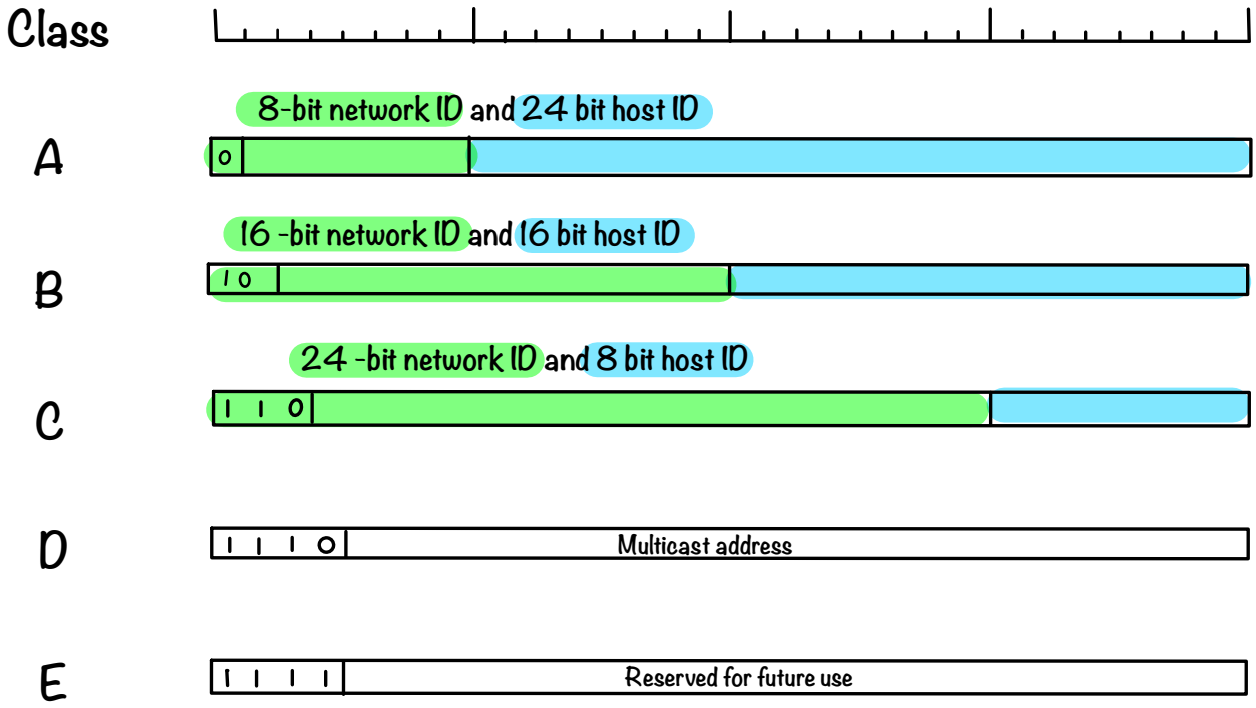
Hexadecimal	Decimal
C2	194
2F	47
15	21
82	130

Why the following IP address are wrong?

111.56.045.78	There must be no leading zero (045).
221.34.7.8.20	There can be no more than four numbersin address.
75.45.301.14	One decimal can not be more than 255.
11100010.23.14.67	Doted decimal must not contain the binary form.

Classful Addressing

In classful addressing, the address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space.



Calculate number of network possible for a class A address:

First byte (8-bits) of address in class A IP represents the network address. Moreover, the starting bit of the byte must be 0.
Hence, the network address should range from 0-127. However, network ID with 0 is reserved for host only address. Similarly 127 is used for loopback address. Hence the network range becomes 1-126. So there are 126 networks possible when using class A of classful addressing.

Calculate number of host possible for a class A address.

Last 3 byte (24-bits) of address in class A IP represents the host address. Hence, there are 2^{24} = 16777216 host possible. However, the IP NetworkID.0.0.0 and NetworkID.255.255.255 is used for network ID and broad cast function respectively. Hence, the number of host is $2^{24}-2$ = 16777214

Calculate number of network possible for a class B address:

First 2 bytes (16 bits) of address in class B IP represents the network address. Moreover, the starting 2 bit have to be 10. So, remaining 14 bit will represent the network ID. Hence there are 2^{14} = 16384 networks possible.

Class	Bits for network	Bits for host	IP range	# network	# host per network
A	8	24	0.0.0.1 - 127.255.255.255	126	16777214
B	16	16	128.0.0.0 - 191.255.255.255	16384	65534
C	24	8	192.0.0.0 - 223.255.255.255	2097152	254
D	NA	NA	224.0.0.0 - 239.255.255.255	NA	NA
E	NA	NA	240.0.0.0- 255.255.255.255	NA	NA

NB:

0.0.0.0 is not a valid IP

0.0.0.1 - 0.255.255.255 is reserved and can not be assigned to any network

Host ID with all zeros represent network ID hence can't be assigned to any host.

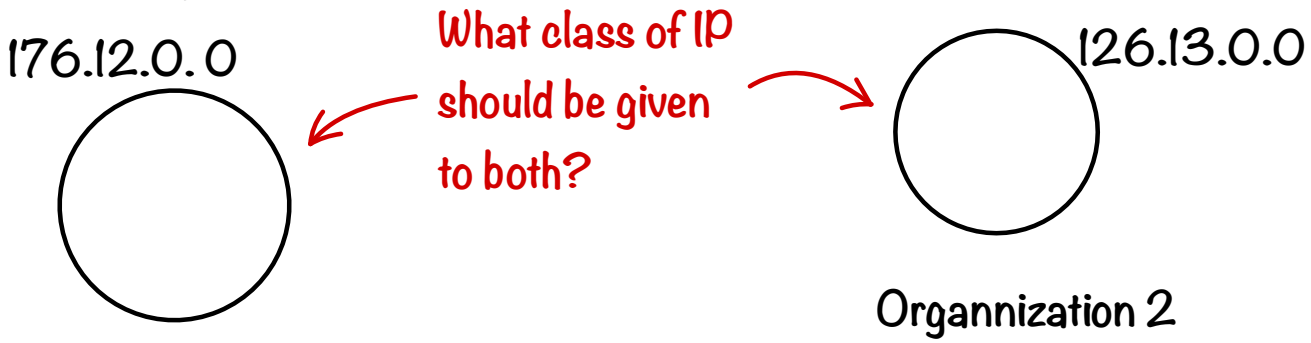
Host ID with all ones is reserved for broadcast hence can't be assigned to any host.

Class D IP are used for broadcast and class E IP are reserved for future use. So we generally don't calculate network ID and host ID for these class.

Suppose that instead of using 16 bits for the network part of a class B address origi- nally, 20 bits had been used. How many class B networks would there have been?

With a 2-bit prefix, there would have been 18 bits left over to indicate the network. Consequently, the number of networks would have been 2^{18} or 262,144. However, all zeros and all ones are special, so only 262,142 are avail- able.

Sub-Net & Super-Net



Organnization 1 having 300 host

Organnization 2 having 500 host

Class C is not be enough to accumulate all hosts.

&

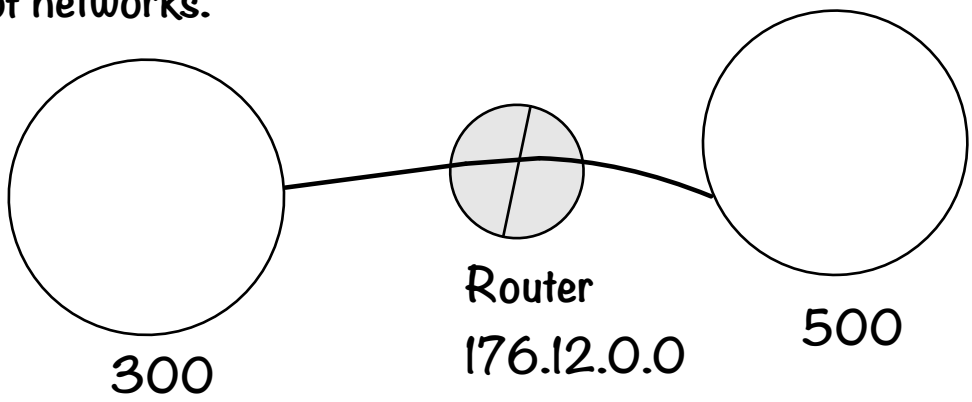
Class B is too much for each

65534
− 500
65034

Not used

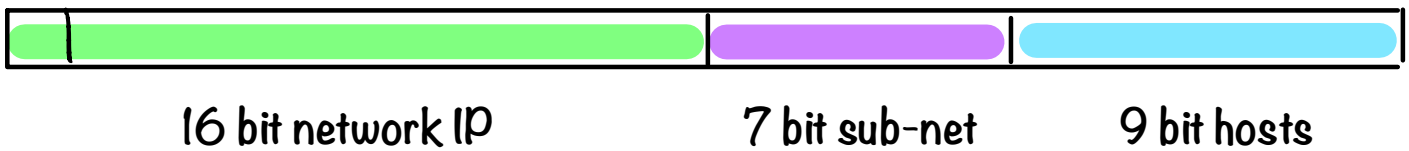
To share a network ID among multiple network the concept of sub-net is used.

Let's assume we need to share the network IP 176.12.0.0 among the above example of networks.



Instead of giving 16 bits to hosts we are going to take some of the bits to represent the sub-net

So 9 bits address that we need to present 500 hosts and 300 hosts hence 16-9 = 7 bits are used for sub-net.



So for the new router and hosts the network address becomes 16+7= 23 bits.

So the network sub-net mask is represented by 32 bit address with first 23 bits set to 1 and other to 0.

11111111 11111111 11111110 00000000

Sub-Net mask

255.255.254.0

176.8.0.0 / 23 Network IP with sub- net also can be shown like this

Classless Inter Domain Routing

Net and sub-net managing for routers become difficult with classful address.

Moreover, the routing table becomes complex to maintain by the network administrator

In, classless addressing IP addresses are contained in prefixes of varying sizes.

The same IP address that one router treats as part of a /22 (a block containing 210 addresses) may be treated by another router as part of a larger /20 (which contains 212 addresses).

CIDR (Classless Inter- Domain Routing)

Given a host IP to be 5.6.230.60/12

Find network IP, first host, last host, broadcast and next sub-net

5 6 230 60

0000 0101 0000 0110 1110 0110 0011 1100

12 bit network address

Hence, network address is ↙ Set the host bits to zero

0000 0101 0000 0000 0000 0000 0000 0000

5.0.0.0 / 12

First host will be

Set the last host bit to zero

0000 0101 0000 0000 0000 0000 0000 0001

5.0.0.1 / 12

Last host will be

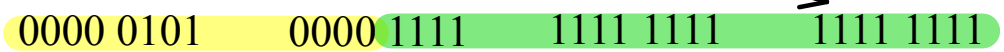
Set all but last bit of host to 1

0000 0101 0000 1111 1111 1111 1111 1110

5.15.255.254 / 12

Broadcast ID

Set all host bit to 1



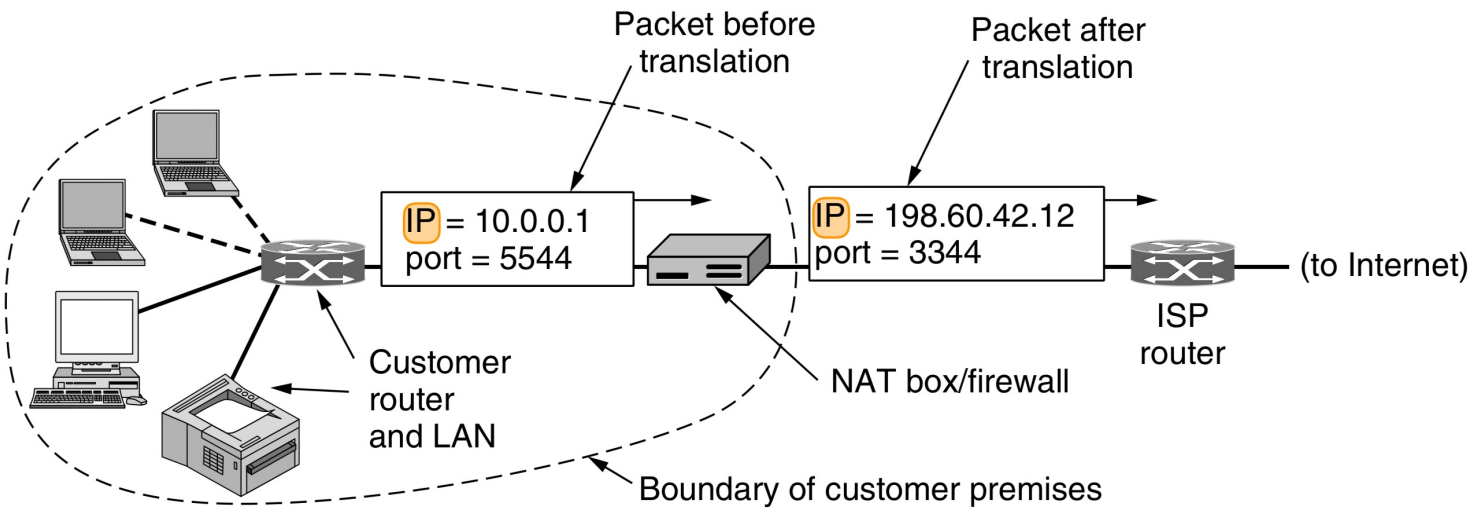
5.15.255.255 / 12

NAT: Network Address Translation

IP addresses are scarce. An ISP might have a /16 address, giving it 65,534 usable host numbers. If it has more customers than that, it has a problem.

The basic idea behind NAT is for the ISP to assign each home or business a single IP address (or at most, a small number of them) for Internet traffic. Within the customer network, every computer gets a unique IP address, which is used for routing intramural traffic. However, just before a packet exits the customer net- work and goes to the ISP, an address translation from the unique internal IP ad- dress to the shared public IP address takes place. This translation makes use of three ranges of IP addresses that have been declared as private. Networks may use them internally as they wish. The only rule is that no packets containing these addresses may appear on the Internet itself. The three reserved ranges are:

10.0.0.0	– 10.255.255.255/8	(16,777,216 hosts)
172.16.0.0	– 172.31.255.255/12	(1,048,576 hosts)
192.168.0.0	– 192.168.255.255/16	(65,536 hosts)



The operation of NAT is shown in figure. Within the customer premises, every machine has a unique address of the form 10.x.y.z. However, before a pack- et leaves the customer premises, it passes through a NAT box that converts the in- ternal IP source address, 10.0.0.1 in the figure, to the customer's true IP address, 198.60.42.12 in this example. The NAT box is often combined in a single device with a firewall, which provides security by carefully controlling what goes into the customer network and what comes out of it.

Port numbers, and socket address

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.

A port number uses 16 bits and so can therefore have a value from 0 to 65535 decimal

Port numbers are divided into ranges as follows:

Port numbers 0-1023 – Well known ports. These are allocated to server services by the Internet Assigned Numbers Authority (IANA). e.g Web servers normally use port 80 and SMTP servers use port 25 (see diagram above).

Ports 1024-49151- Registered Port -These can be registered for services with the IANA and should be treated as semi-reserved. User written programs should not use these ports.

Ports 49152-65535– These are used by client programs and you are free to use these in client programs. When a Web browser connects to a web server the browser will allocate itself a port in this range. Also known as ephemeral ports.

Most popular 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 is a socket?

A socket represents one end of the connection; that allows communication between two different processes on the same or different machines. Unix uses file descriptors to identify each socket.

In Unix, every I/O action is done by writing or reading a file descriptor. A file descriptor is just an integer associated with an open file and it can be a network connection, a text file, a terminal, or something else.

Where is Socket Used?

A Unix Socket is used in a client-server application framework. A server is a process that performs some functions on request from a client. Most of the application-level protocols like FTP, SMTP, and POP3 make use of sockets to establish connection between client and server and then for exchanging data.

Socket Types

There are four types of sockets available to the users. The first two are most commonly used and the last two are rarely used.

Processes are presumed to communicate only between sockets of the same type but there is no restriction that prevents communication between sockets of different types.

Stream Sockets – Delivery in a networked environment is guaranteed. If you send through the stream socket three items "A, B, C", they will arrive in the same order – "A, B, C". These sockets use TCP (Transmission Control Protocol) for data transmission. If delivery is impossible, the sender receives an error indicator. Data records do not have any boundaries.

Datagram Sockets – Delivery in a networked environment is not guaranteed. They're connectionless because you don't need to have an open connection as in Stream Sockets – you build a packet with the destination information and send it out. They use UDP (User Datagram Protocol).

Raw Sockets – These provide users access to the underlying communication protocols, which support socket abstractions. These sockets are normally datagram oriented, though their exact characteristics are dependent on the interface provided by the protocol. Raw sockets are not intended for the general user; they have been provided mainly for those interested in developing new communication protocols, or for gaining access to some of the more cryptic facilities of an existing protocol.

Sequenced Packet Sockets – They are similar to a stream socket, with the exception that record boundaries are preserved. This interface is provided only as a part of the Network Systems (NS) socket abstraction, and is very important in most serious NS applications. Sequenced-packet sockets allow the user to manipulate the Sequence Packet Protocol (SPP) or Internet Datagram Protocol (IDP) headers on a packet or a group of packets, either by writing a prototype header along with whatever data is to be sent, or by specifying a default header to be used with all outgoing data, and allows the user to receive the headers on incoming packets.

What are Socket addresses?

Process to process delivery (transport layer communication) needs two identifiers, one is IP address and the other is port number at each end to make a connection. Socket address is the combinations of IP address and port number as shown in the figure.