Chapter 4 IP

kumo
shinma

IP internet layers protocol

What does IP stand for?

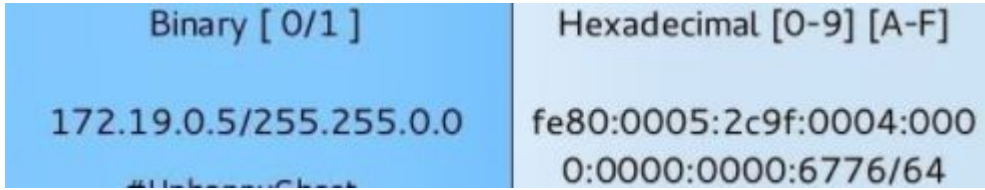
- Internet Protocol

ICMS

- Internet Control Message Protocol

Although there is IPv6, this chapter will be based on IPv4

- An IP address is a long binary number, made of ones and zeros. An IPv4 address is 32 binary digits (or bits) long. An IPv6 is 128 bits long, allowing many more IP addresses to be used.



What is an IP address?

IP Address

- Internet Protocol Address

IP refers to a unique number that gets linked to all online activity

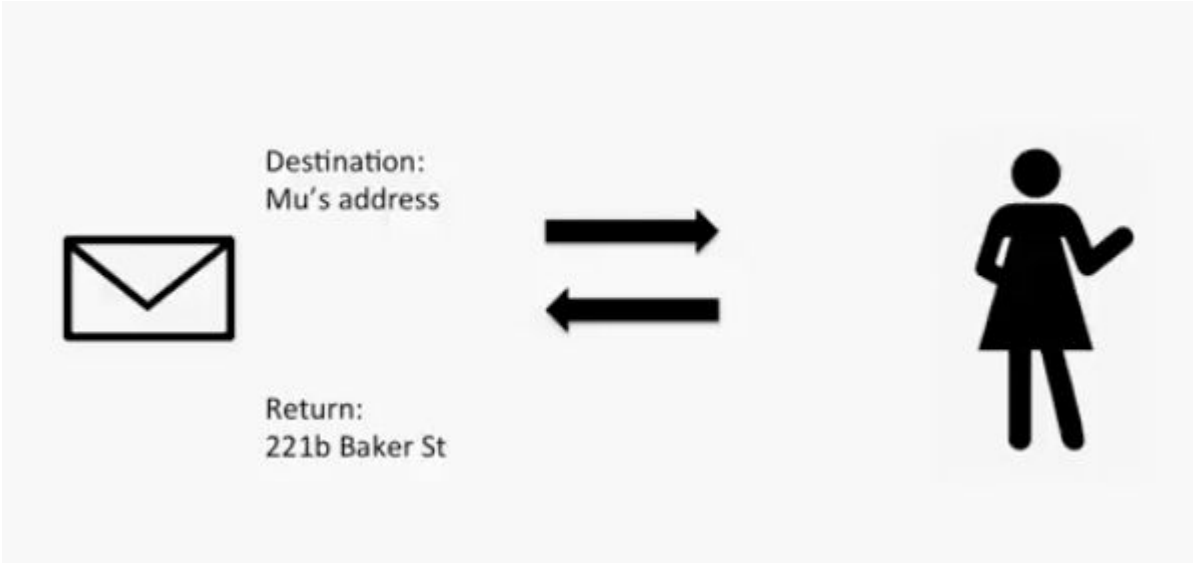
In simple terms “Where you live on the internet”

Simplest Example I could think of

You send a letter to someone.

You add the destination and the return address (your house)

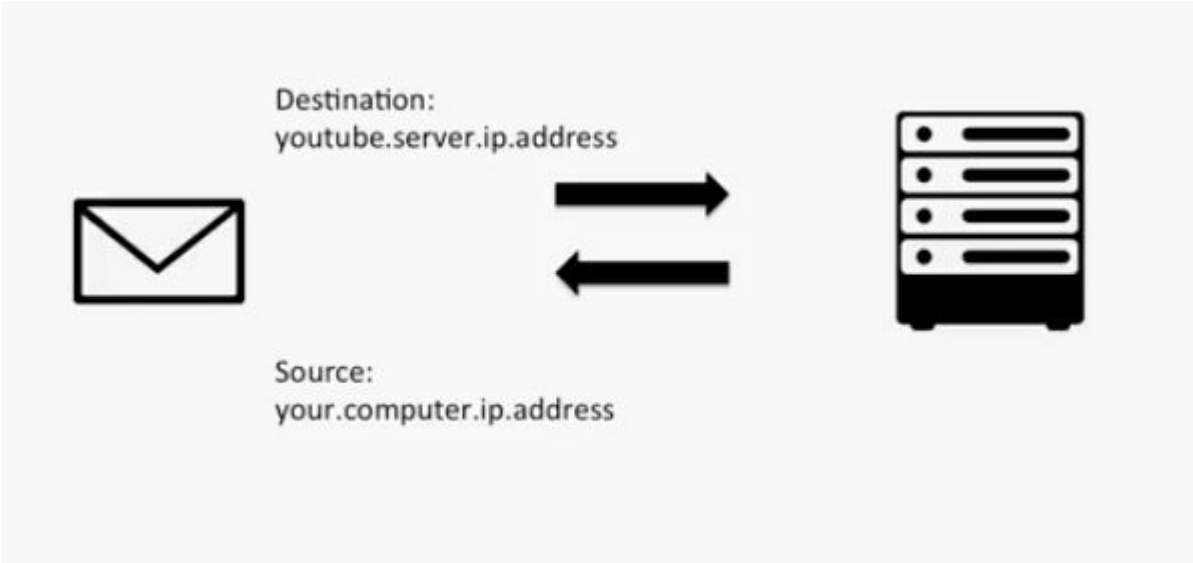
You expect a reply.



Simplest Example I could think of

Exactly the same.

Except it's a server instead of a person ;)



Host and node

Host = A network host is a computer or other device connected to a computer network. A network host may offer information resources, services, and applications to users or other nodes on the network. A network host is a network node that is assigned a network layer host address.

Nodes = In data communication, a physical network node may either be a data communication equipment (DCE) such as a modem, hub, bridge or switch; or a data terminal equipment (DTE) such as a digital telephone handset, a printer or a host computer, for example a router, a workstation or a server.

IP Packet

IP packets contains

- Header
  - Control
  - Packet Information
  - Source IP Address
  - Destination IP Address
- Data segment

Requests / Calls Information

↓

Packages IP packet

↓

Goes through the LAN

↓

Router puts IP packets to their destination network

↓

Router Switch routes IP packet

↓

Network interface picks up IP packet

↓

Firewall into the Bandwidth

↓

Into the WWW

7 OSI layers

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP	**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**	JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	**Routers** IP/IPX/ICMP		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**		

PACKET FILTERING

Network Layer and Data link layer

- **Datalink Layer** allows the reliable transfer of data through the physical layer, sending data frames with the necessary synchronization and performs error checking and signal loss. This allows you to bring up, to the top level, the physical medium such as a transmission line free of bit errors;

- **Network Layer** enables the upper levels to be independent of the mechanisms and transmission technologies used to connect and takes into charge the delivery and the destination of the packets;

So why do we need two?

Imagine you're going on a trip!

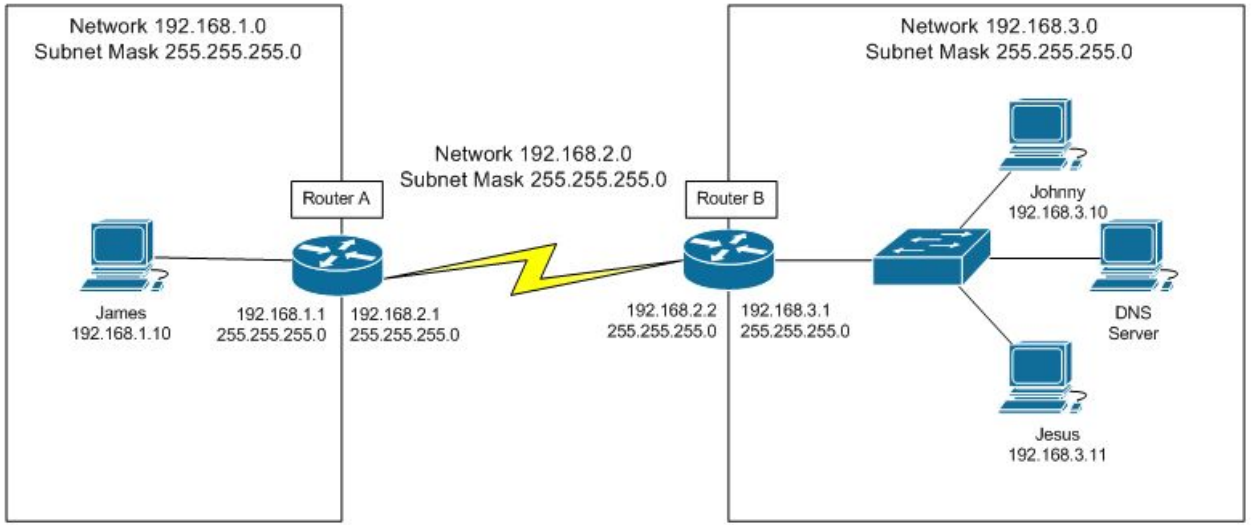
- You decided that you'll take a bus, train and plane to get to your destination.
- You go to the store and tell the your destination and your return destination.
- The store clerk gives you your tickets and a guide which gives you the exact times for the bus, train and flight.
- You have to use different tickets for each transportation because they all belong to different companies
- You go on your trip! (There may be accidents)

Tickets and directions is the Header of the packet

Guide is your network layer. Your destination and final destination is the data link. (You need everything)

IP Routing

The process of moving a packet of data from source to destination. Routing is usually performed by a dedicated device called a router. Routing is a key feature of the Internet because it enables messages to pass from one computer to another and eventually reach the target machine.

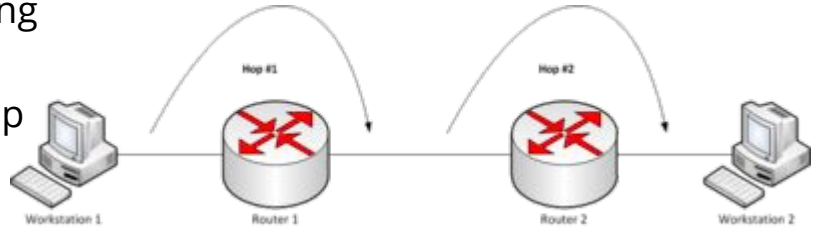


Hopping

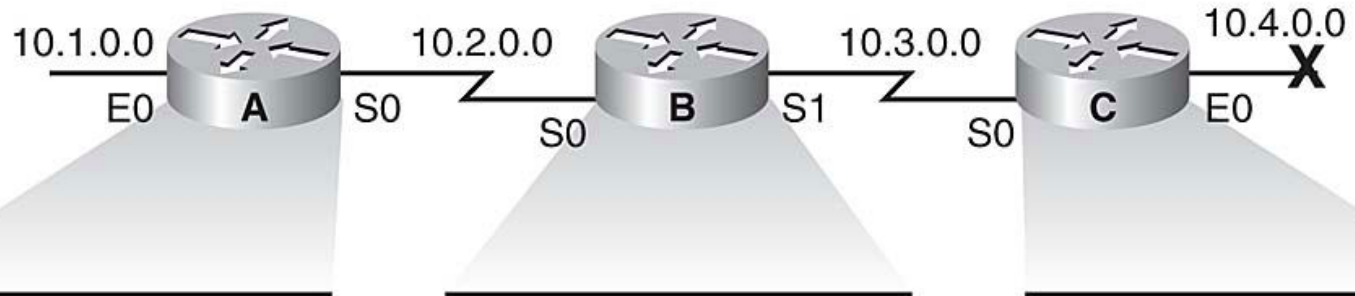
In computer networking, a hop is one portion of the path between source and destination. Data packets pass through bridges, routers and gateways as they travel between source and destination

The hop count refers to the number of intermediate devices (like routers) through which data must pass between source and destination

Hop-by-hop routing forms the basis of today's IP networks. Hop-by-hop routing means that routing decisions are made at each router independently and locally. For each incoming packet at a router, its destination address (maybe some other fields in its IP header, too) is used to get the next hop by consulting the router's routing table.



Routing table



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	Down
10.2.0.0	S0	1
10.1.0.0	S0	2

IP 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.

Different classes supports different number of hosts.

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 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.

Broadcast address

A broadcast address is a logical address at which all devices connected to a multiple-access communications network are enabled to receive datagrams. A message sent to a broadcast address is typically received by all network-attached hosts, rather than by a specific host.

CIDR VLSM

CIDR (Classless Inter-Domain Routing, sometimes called supernetting) is a way to allow more flexible allocation of Internet Protocol (IP) addresses than was possible with the original system of IP address classes. As a result, the number of available Internet addresses was greatly increased, which along with widespread use of network address translation (NAT), has significantly extended the useful life of IPv4.

A Variable Length Subnet Mask (VLSM) is a numerical masking sequence, or IP address subset, based on overall network requirements. A VLSM allows a network administrator to use long masks for networks with few hosts and short masks for networks with multiple hosts. A VLSM is used with a VLSM router and must have routing protocol support.

A VLSM is also known as a classless Internet Protocol (IP) address.

Subnet Mask

- Subnet
  - Sub network or smaller network within a larger network
- Subnet Mask
  - Subnet mask is a 32 bit number that divides the IP address into network address and host address
  - Usually 255.255.???.???
- Subnetting
  - Breaks up networks into smaller parts
  - Decides local and remote traffic

Trying to subnet : 158.173.70.134/29

Subnetting

128	192	224	240	248	252	254	255
128	64	32	16	8	4	2	1

Subnets

Binary bits

00000000	00000000	00000000	00000000	Total of 32 bits
8	16	24	32	

158.173.70.134/29 ← Find the / number and find where it belongs

Trying to subnet : 158.173.70.134/29

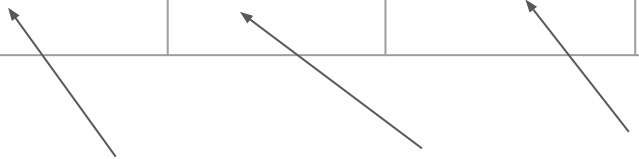
Subnetting

128	192	224	240	248	252	254	255
128	64	32	16	8	4	2	1

Subnets

Binary bits

00000000	00000000	00000000	00000000	Total of 32 bits
8	16	24	32	



29 is higher than 8 . Higher than 16 and 24

Trying to subnet : 158.173.70.134/29

Subnetting

128	192	224	240	248	252	254	255
128	64	32	16	8	4	2	1

Subnets

Binary bits

00000000	00000000	00000000	00000000	Total of 32 bits
8	16	24	32	

29 is lower than 32.
Therefore 32-29 = 3

2^3 = 8. 8's subnet id is 248

Therefore the subnet mask is 255.255.255.248

Trying to subnet : 158.173.70.134/29

Subnetting

128	192	224	240	248	252	254	255
128	64	32	16	8	4	2	1

Subnets

Binary bits

00000000	00000000	00000000	00000000	Total of 32 bits
8	16	24	32	

Subnet Mask: 255.255.255.248
Network IP:
First host IP:
Last host IP:
Broadcast IP: