Module 4 – Part 2

Vipin Das
SAINTGITS College of Engineering

IP addresses and its usage

IP V4 addresses uses 32 bit address.

A part of it is used to represent network part and other part for hosts.

Simple IP address can reveal about host and network .

There are basically two schemes which determine how many bits are reserved for network and for host.

Format of an IP Address

Classful addressing

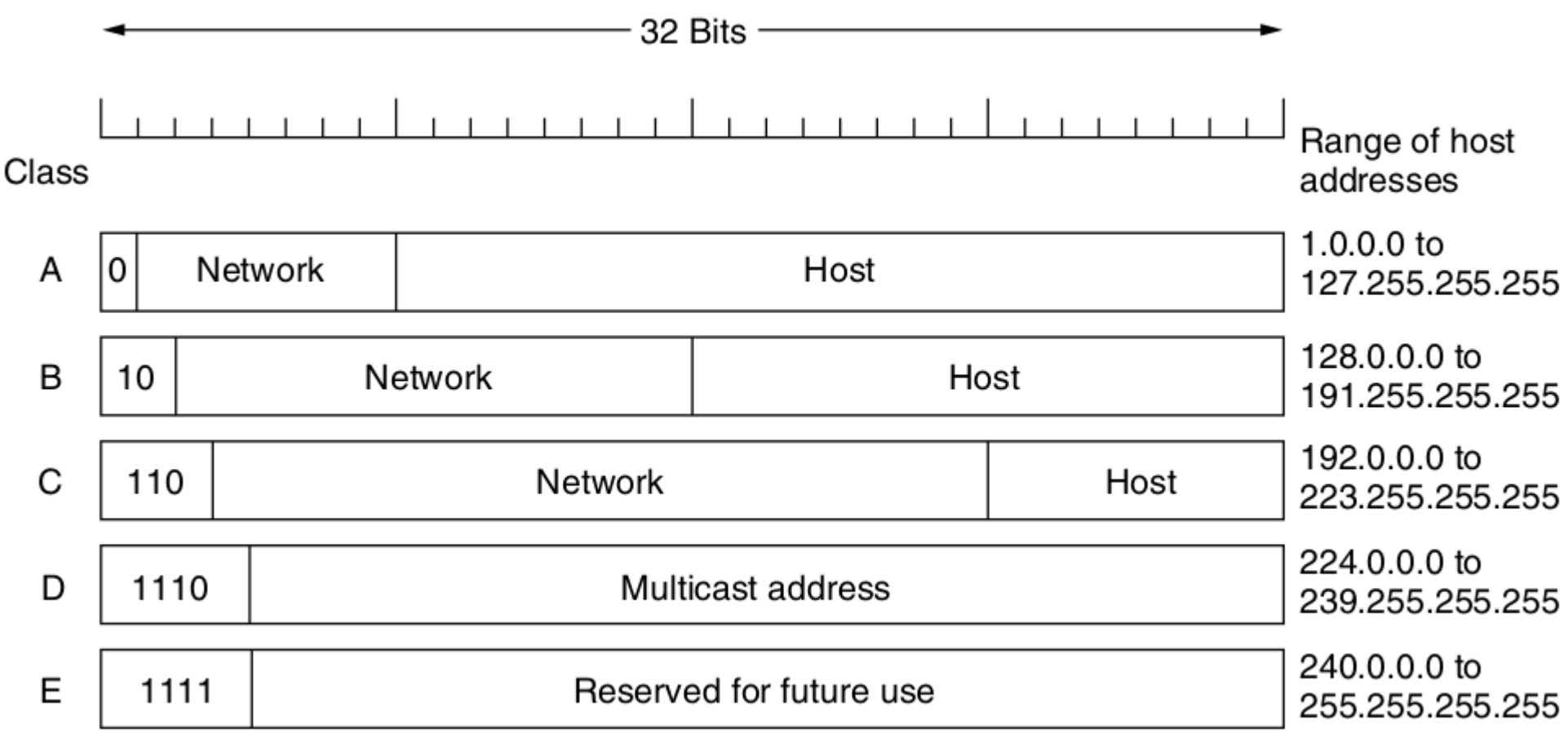
In classful addressing a predefined set of bits are reserved for network part and another for host part.

There are 5 major types and each are given class names.

Follows a hierarchial order.

Although the concept is simple ,organizations had difficulty in choosing correct classes.

Either they will waste a large number of IP addresses or they will not find sufficient IP addresses.


32 Bits
Class
Range of host addresses
A
0
Network
Host
1.0.0.0 to 127.255.255.255
B
10
Network
Host
128.0.0.0 to 191.255.255.255
C
110
Network
Host
192.0.0.0 to 223.255.255.255
D
1110
Multicast address
224.0.0.0 to 239.255.255.255
E
1111
Reserved for future use
240.0.0.0 to 255.255.255.255

Classless Inter Domain Routing -CIDR

In CIDR there are no fixed arrangement on the number of bits that are used to represent host and network.

A prefix is added along with the IP address which specifies how many higher order bits are reserved for the network part.

The IP address is represented as *a.b.c.d/x* where x represents the network part.

Ex:- 192.168.1.1/18 --> The first 18 bits indicate the network part.Remaining bits could be used to address hosts.

The concept of subnet mask

Subnet represents a group of systems which could be imagined as being isolated from other networks.

The network part address of the systems in the subnet will be same.

A special IP address known as subnet mask will help routers to identify the network part.

More on subnet mask.

The subnet mask IP address will have all 1’s in which the network part is represented.

If the first part of 24 bits is designated for network part the IP address mask is 255.255.255.0

A bitwise AND operator of any IP address and the mask will give the network part ,which will be used by routers to direct the packets.

Dynamic Host Configuration Protocol

When there are a large number of Computers in a network manually assigning IP addresses to each of them is tedious.

Manual assignments could lead to IP clashes also.

DHCP helps to reslove this issue

Every network is supposed to have a DHCP server.

The server is configured with the starting address,range,mask etc.

When a new system joins the network it broadcasts a DHCP discover packet.

It eventually reaches the DHCP server .

The DHCP server gets an IP address from the pool and creates a DHCP Offer reply.

The messages are sent back and forth using the Physical address.

Each IP address is given to a host for a specific period of time.

The host can request renewal before the expiry.

If the DHCP server denies the renewal ,the host should stop using the IP.

Since the IP address is given only for a specific time,the process is also known as IP leasing.

Internet Control Messages

In addition to data transfer network layer defines a few other protocol which helps in setting up various parameters,exchange control information etc.

DHCP is one among them.

These messages are often transmitted without the application/user intervention.

ICMP – Internet Control Message Protocol

ICMP messages carry information from the routers.

The routers send ICMP messages so as to inform the sender about the status of events at the router.

ICMP messages are carried as payload in IP packets.

ICMP messages define a type and code field which have predefined meaning.

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

ARP – Address Resolution Protocol

The IP address that is assigned is temporary in nature.

In an actual scenario the data movement should include the IP address and MAC(Physical) Address also.

There is a need to map IP address to MAC address.

ARP protocol does the work.

The working

A ARP table listing the known MAC and IP addresses is kept in each node.

When the node wants to send a data to the IP *a.b.c.d* it creates a ARP brodcast packet(ARP Query) .

The ARP query has the senders IP,MAC ,required IP and broadcast MAC address.

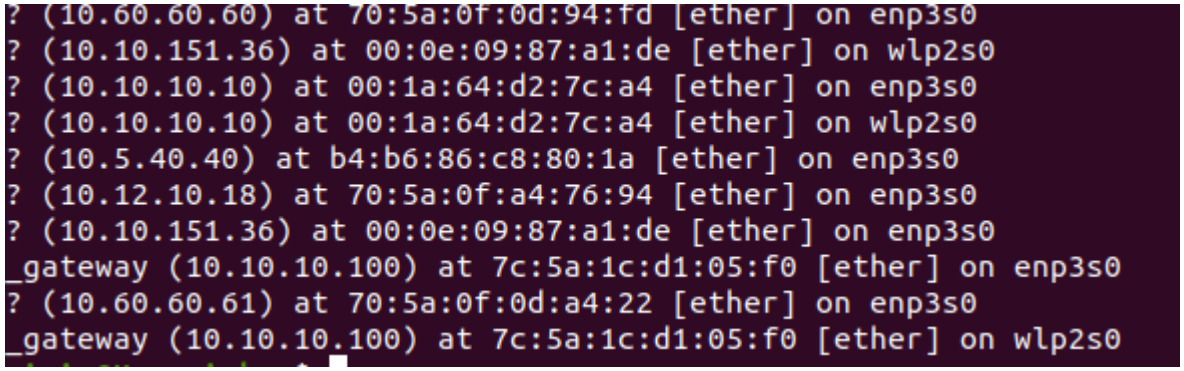
This query passes through all the nodes.

If the IP address of any node matches the required IP, a ARP reply packet is contructed.

The ARP reply is sent as unicast transmission.

All the nodes that receive the ARP query can use the address information in the packet to update their ARP table.

ARP query ends up flashing the MAC and IP combo to all the nodes.



RARP – Reverse Address Resolution protocol

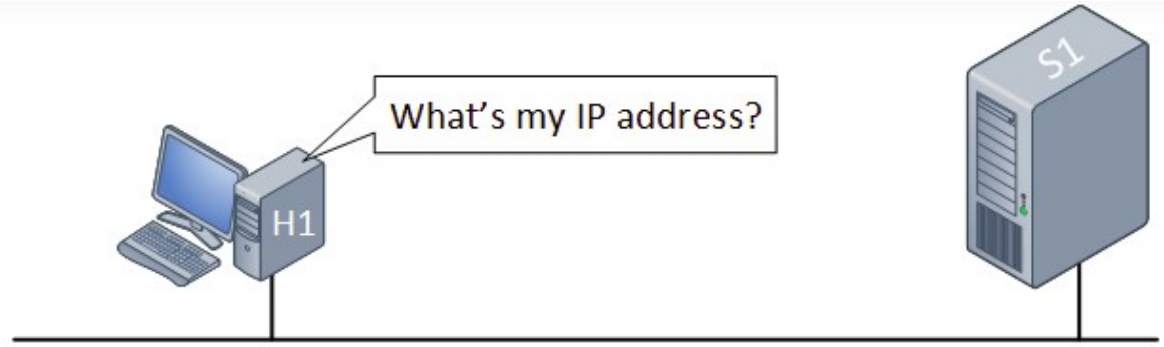
RARP is used by clients which does not store the IP addresses.

RARP was used before DHCP to get the IP addresses.

The client will send a brodcast message with its MAC as content .

The server will reply with an IP address.

The contents at the server are manually entered.

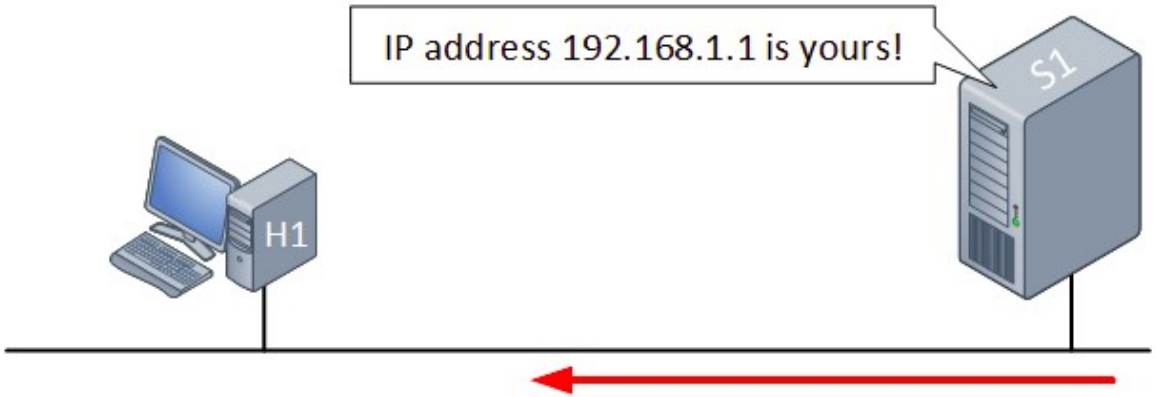


RARP Request:
MAC: aaaa.bbbb.cccc
IP: 0.0.0.0

And the RARP server replies with the RARP reply:

RARP TABLE:

aaaa.bbbb.cccc = 192168.1.1
dddd.eeee.ffff = 192.168.1.2

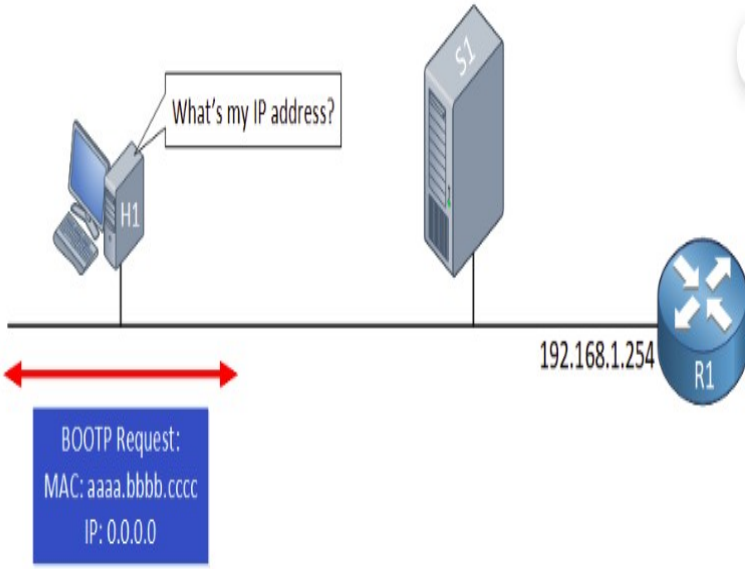


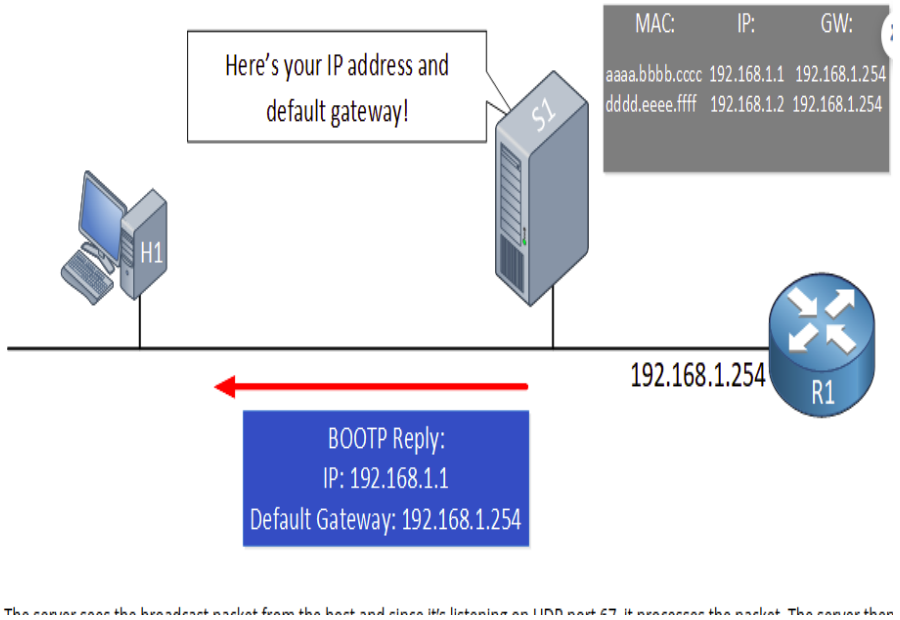
RARP Reply:
MAC: aaaa.bbbb.cccc
IP: 192.168.1.1

BOOTP

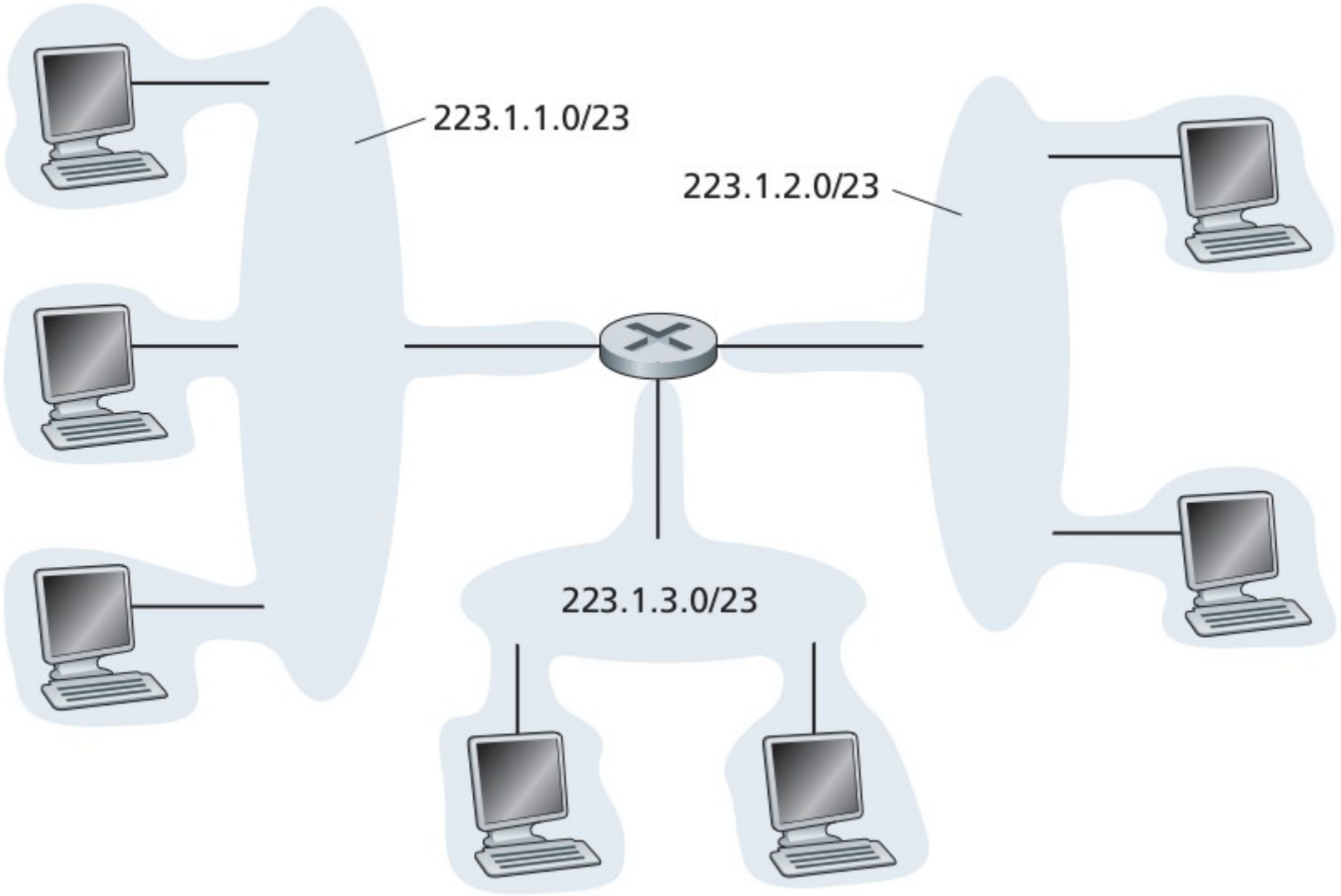
Direct predecessor to DHCP.

The protocol uses a static database of IP and coressponding MAC address.





A subnet



The concept of Autonomous systems

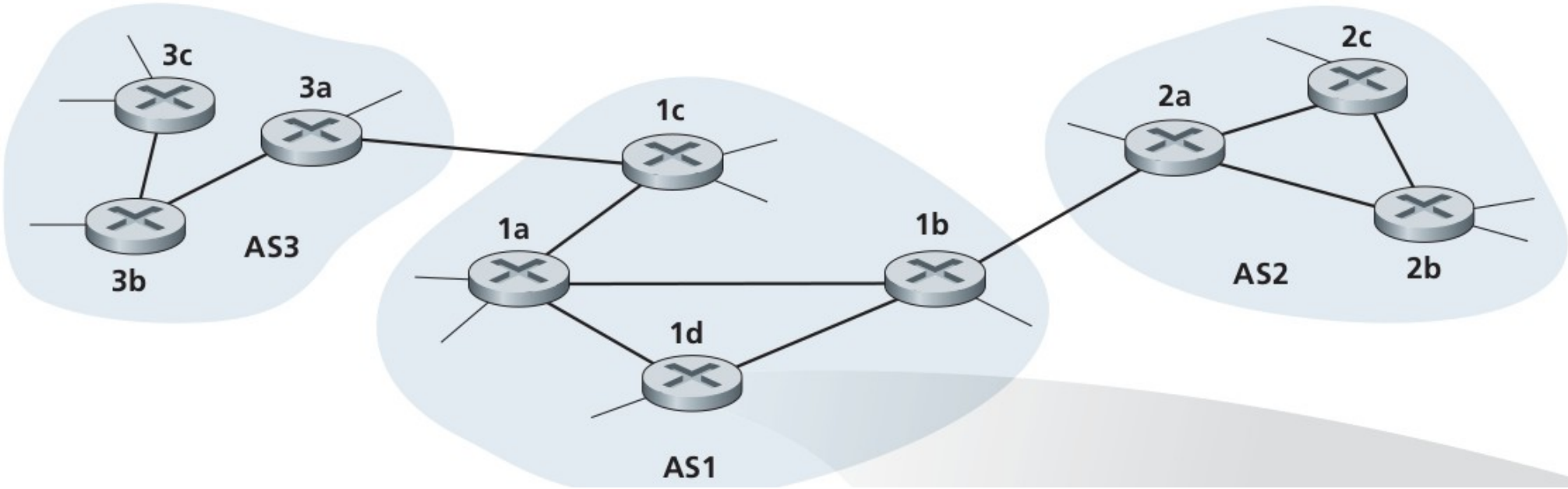
Grouping a set of routers together forms an autonomous system.

An autonomous system will be having a same administrative component.

Under one autonomous system there could be multiple routers and to each router there could be subnets attached.

One autonomous system could be connected to others also.

Autonomous systems (AS) creates a hierarchial order in spreading the routing information and also in maintaining the network.


3c
3a
1c
2c
2a
1a
1b
3b
AS3
AS2
2b
1d
AS1

Routing in the Internet

Data movement in the internet is made possible by moving data across different AS.

This calls for routing mechanisms within the AS and also between different AS.

The protocols that are used to acheive this task makes use of modified versions of distance vector or linkstate algorithms.

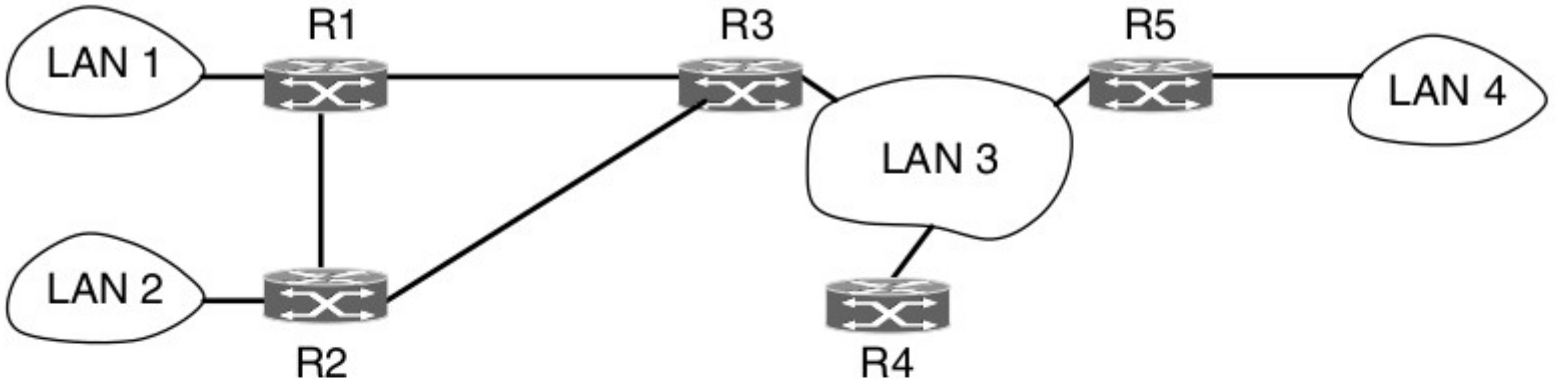
OSPF-Open Shortest Path First

OSPF is an intra AS routing algorithm used in the internet.

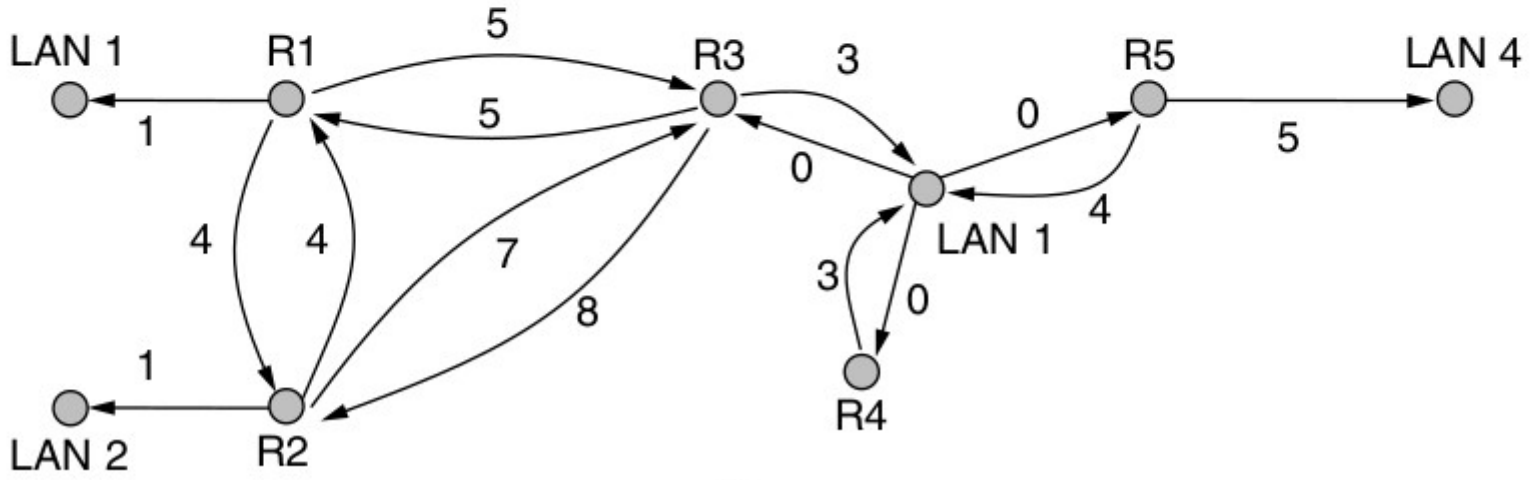
OSPF uses linkstate flooding and makes use of Dijkstras shortest path algorithm.

Routers in the AS create a graph of the entire AS.

At each router shortest path algorithm is performed to find the shortest path.


R1
R3
R5
LAN 1
LAN 4
LAN 3
LAN 2
R2
R4

(a)


LAN 1
R1
5
R3
3
R5
LAN 4
1
5
0
5
4
4
7
LAN 1
4
3
0
8
1
R4
LAN 2
R2

(b)

OSPF allows splitting up of the AS into parts known as *area.*

There could be routers in the AS that are not part of any AS.

Routers that lie completely within one area is known Internal routers.

Every AS has a special backbone area.

All the areas are connected to the routers in backbone area.

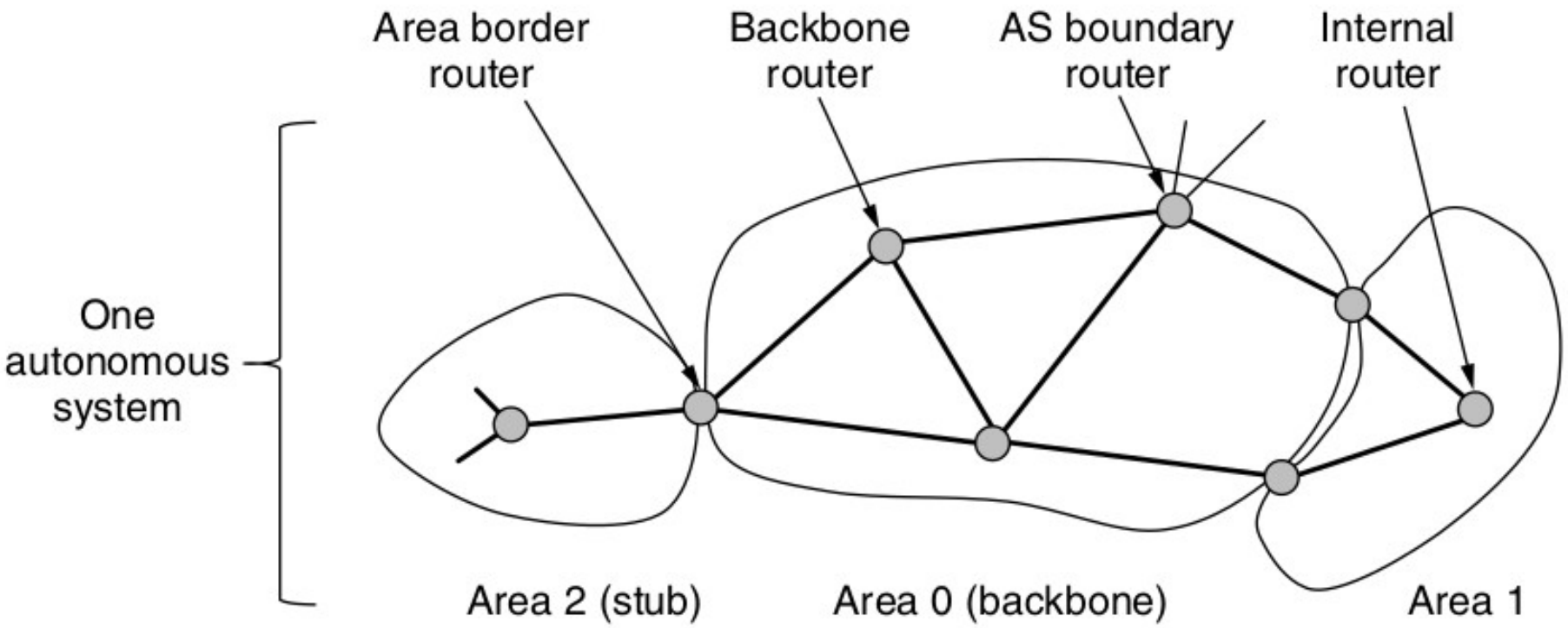
This helps all other routers to find a path to the other through the backbone area.

A router that is connected to two or more area is know as border router.

If there is one border router for an area ,that area is known as stub area.

There are special boundary routers that connect one AS to other .

The arrangement of splitting into area is done so as to make routing decisions hierarchally.


Area border router
Backbone router
AS boundary router
Internal router
One autonomous system
Area 2 (stub)
Area 0 (backbone)
Area 1

OSPF selects a few routers as designated router to which information is exchanged.

OSPF works by using special messages which are send across to fetch and update routing information.

Message type	Description
Hello	Used to discover who the neighbors are
Link state update	Provides the sender's costs to its neighbors
Link state ack	Acknowledges link state update
Database description	Announces which updates the sender has
Link state request	Requests information from the partner

BGP – Border Gateway Protocol

BGP is a inter AS routing protocol.

BGP was proposed as there could be specifications of restricting routing through specific parts of the overall AS.

For ex: Organisations does not want to transfer their data through rival AS.

BGP uses a variation of distance vector routing.

The key selection criteria would not be minimum cost path.

The minimum cost path in some cases would be through a restricted area.

BGP keeps track of full path along with the cost.

A connection between two routers is known as a BGP session.

If the session is between two AS its a e-BGP session. (e-> External)

If the session is within the same AS it is a i-BGP session . (i->Internal)

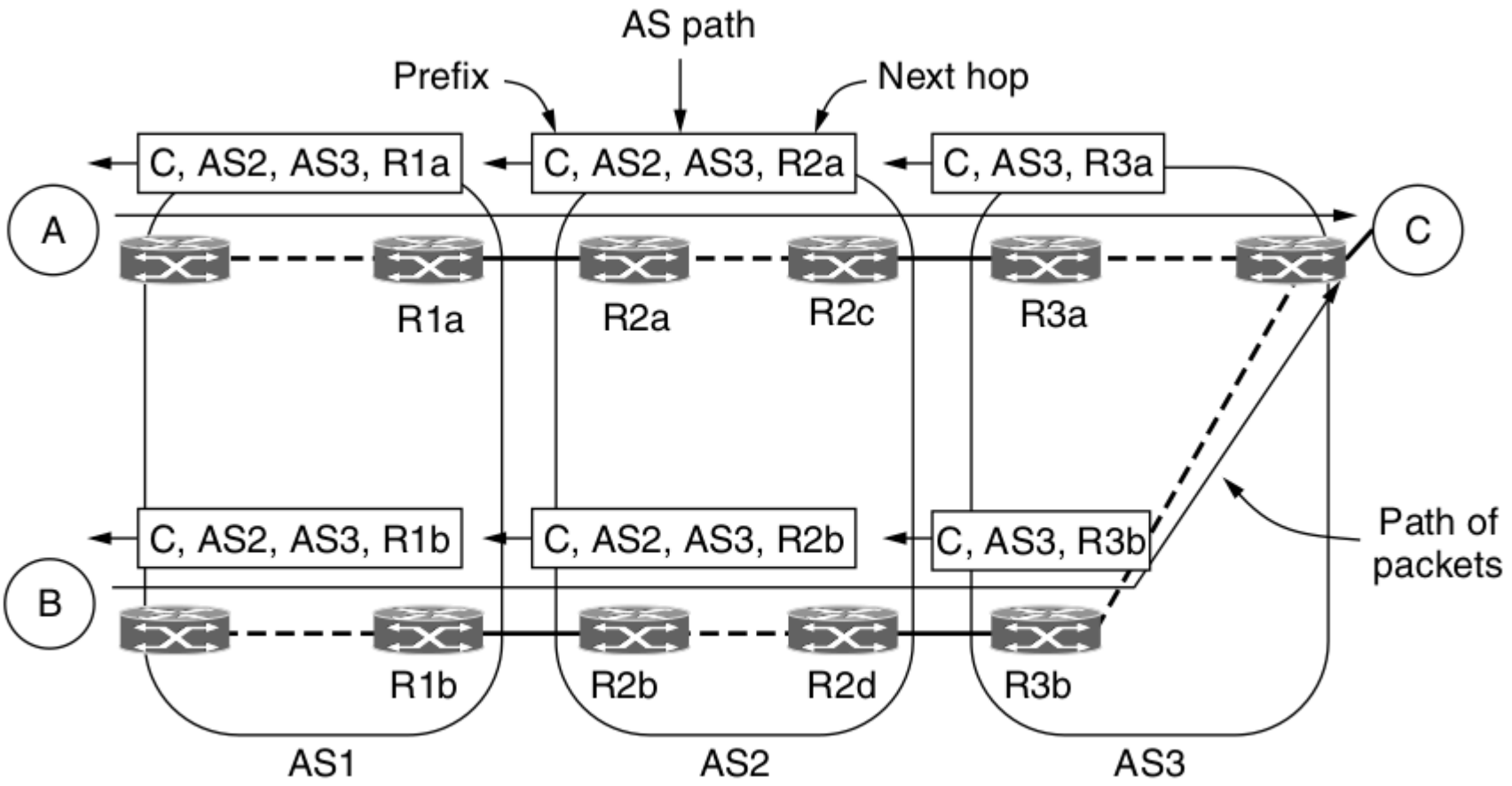
In BGP every AS is identified by a Autonomous System number (ASN).

The destinations are often represented CIDR prefixes.

A route that is learned by one boundary router will be propogated to all other boundary routers.

There could be *transit* routes which are chargeable.

Path advertisement of C to A



Selection of paths

If free paths are available they are chosen.

Another startegy is that path with less AS listed is chosen.

The limitation for such a startegy is that one AS could be so deep that the two AS combined.

Another option is to select the path least cost.

This ensures that data is moved fast and is known as early exit strategy.

Internet Multicast

Every system that needs to receive IP packets should have an IP address.

There could be cases in which the data should be sent to more than one person.

Ex:- Updations,Online conferences etc.

Classful addressing specified class D addresses as multicast addresses.

But even then how to deliver the contents to a set of systems.

IGMP – Internet Group management Protocol.

IGMP specifies methods for the client to join a particular multicast.

The data will be forwarded to those nodes who have subscribed to the services.

A tree structure is created so as to identify the nodes which are part of the transmission.

Within an AS , Protocol Independent Multicast methods will be used to deliver the data.

A reverse path forwarding tree will be created so as to identify the nodes that are part of the transmission.

Network Address Translation *

We have seen that IP addresses are mostly alloted in random.

And IP addresses are required to carry the information to the outside world also.

So if we are browsing ,the data is moving out of our home/office network.

WHAT IP ADDRESS DOES IT CARRY ??

Of all the IP addresses few are available for the access by general public.

Such IP is known as public IP.

EX:- IP address of Google, most websites.

* -> Not specifically mentioned in Syllabus,but good to understand.

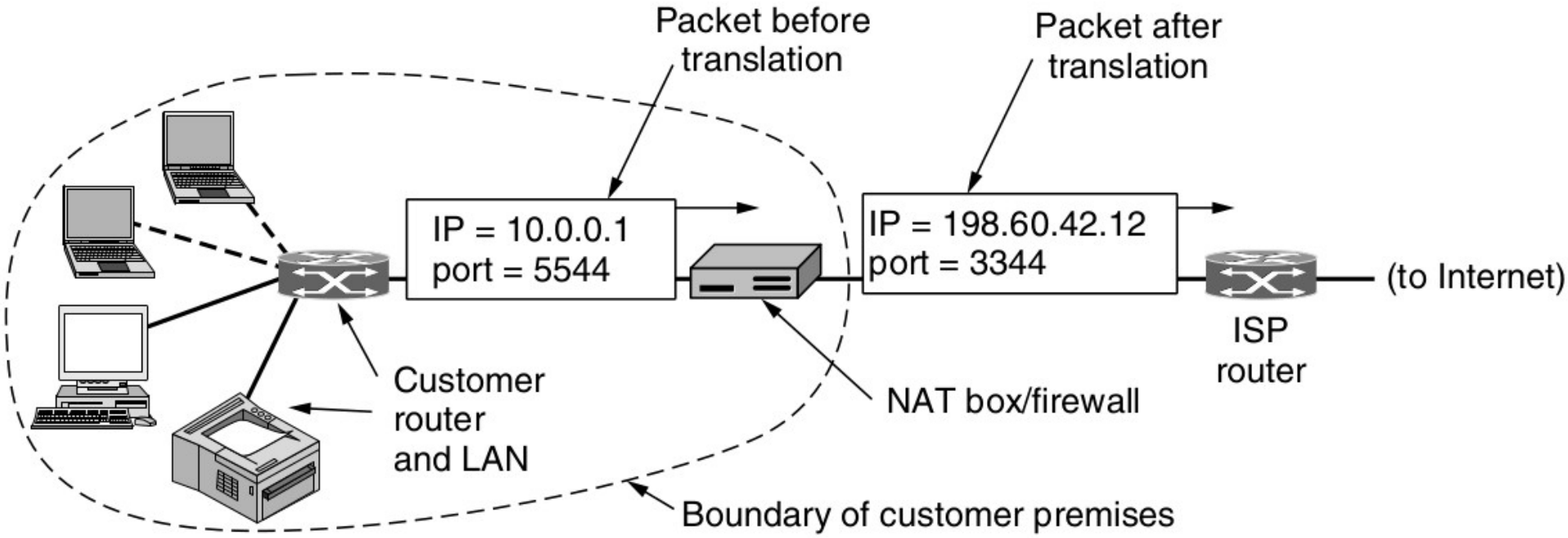
In reality most of the organizations(or ISP) have a public IP.

When we sent data to internet the source IP is changed to the organization IP /ISP IP.

NAT helps in translating the internal private IP.

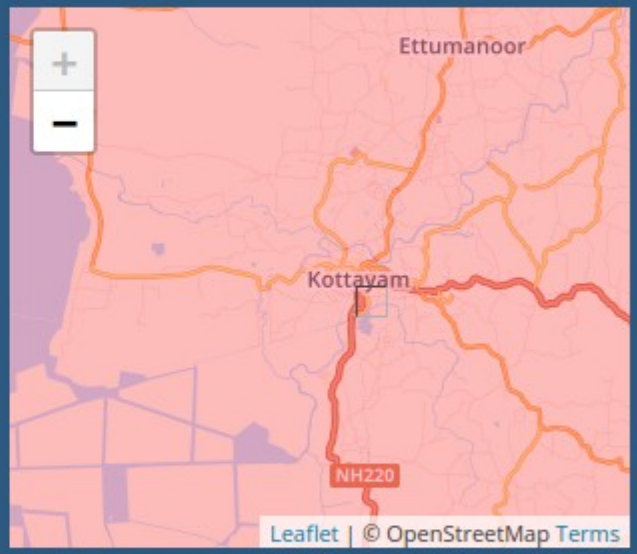
NAT keeps a table of the internal IP,application that sent the data.

This combination is used to direct the data back to the correct application.


Packet before translation
Packet after translation
IP = 10.0.0.1
port = 5544
IP = 198.60.42.12
port = 3344
(to Internet)
ISP router
Customer router and LAN
NAT box/firewall
Boundary of customer premises

IP Details For: 117.254.186.29

Decimal:	1979628061
Hostname:	117.254.186.29
ASN:	9829
ISP:	BSNL
Organization:	BSNL
Services:	None detected
Type:	Broadband
Assignment:	Likely Static IP
Continent:	Asia
Country:	India
State/Region:	Kerala
City:	Kottayam



Latitude:	9.5813 (9° 34′ 52.68″ N)
Longitude:	76.5263 (76° 31′ 34.68″ E)
Postal Code:	686532

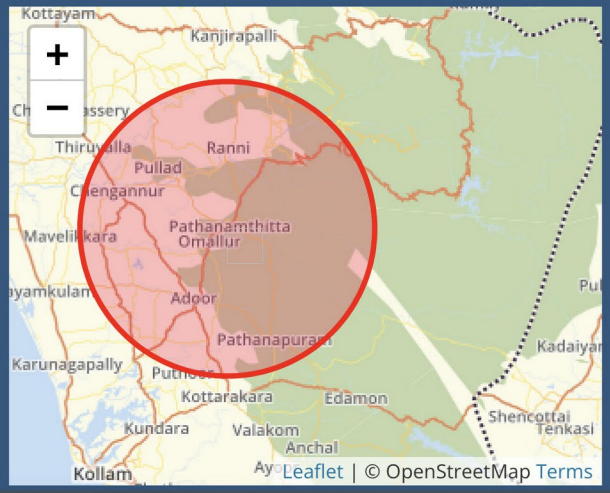
2:41 LTE

WhatIsMyIPAddress.com

Expanded:
2409:4073:2e8e:5688:39fb:6f13:2e7f:7db3

Hostname:
2409:4073:2e8e:5688:39fb:6f13:2e7f:7db3

ASN:	55836
ISP:	Jio
Organization:	Jio
Services:	None detected
Type:	Wireless Broadband
Assignment:	Likely Static IP
Continent:	Asia
Country:	India
State/Region:	Kerala
City:	Pathanamthitta



AA whatismyipaddress.com

--> Content beyond syllabus <--

The use of wireshark tool.

Wireshark is a free tool to capture and analyze network data. [One among a lot !!]

The flag values ,field values etc can be viewed.

There are options to filter data based on protocols.

A set set of capture could be saved .

The save could be analysed using programmming languages like Python to get more insight.

https://www.wireshark.org/

ICMP V6

IPv6 uses the ICMP as defined for IPv4 with a number of changes.

The resulting protocol is called ICMPv6.

ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation or mis-operation.

ICMP uses IP, ICMP packet delivery is unreliable, so hosts can't count on receiving ICMP packets for any network problem.

ICMP v6 Header

Three Fields

Type (8 bits)

Indicates the type of the message.

If the high order bit = 0 (0- 127)→ error message

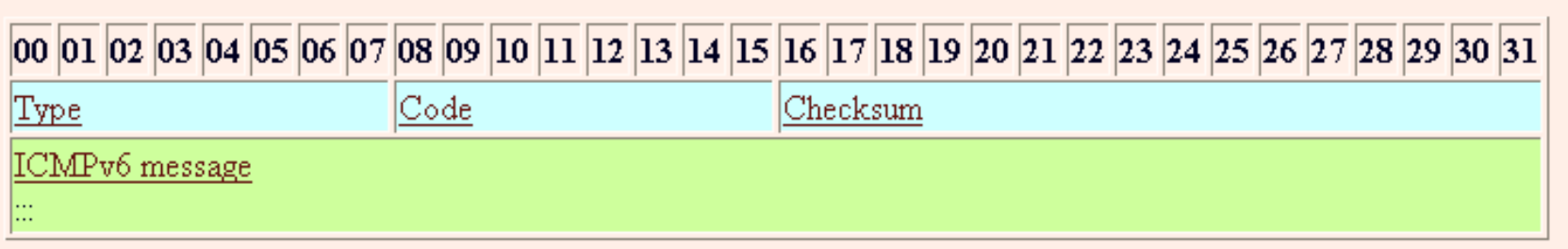
if the high-order bit = 1 (128 – 255) → information message.

Code (8 bits)

content depends on the message type, and it is used to create an additional level of message granularity.

Checksum (16 bits)

Used to detect errors in the ICMP message and in part of the IPv6 message.



ICMP v6 Error messages

Type Value	Message Name	Summary Description of Message Type
1	Destination Unreachable	Indicates that a datagram could not be delivered to its destination. *Code* value provides more information on the nature of the error.
2	Packet Too Big	Sent when a datagram cannot be forwarded because it is too big for the MTU of the next hop in the route. This message is needed in IPv6 and not IPv4 because in IPv4, routers can fragment oversized messages, while in IPv6 they cannot.
3	Time Exceeded	Sent when a datagram has been discarded prior to delivery due to the *Hop Limit* field being reduced to zero.
4	Parameter Problem	Indicates a miscellaneous problem (specified by the *Code* value) in delivering a datagram.

ICMPv6 Informational Messages	**128**	***Echo Request***	Sent by a device to test connectivity to another device on the internetwork.	2463
	129	***Echo Reply***	Sent in reply to an *Echo (Request)* message; used for testing connectivity.	2463
	133	***Router Solicitation***	Prompts a router to send a *Router Advertisement*.	2461
	134	***Router Advertisement***	Sent by routers to tell hosts on the local network the router exists and describe its capabilities.	2461
	135	***Neighbor Solicitation***	Sent by a device to request the layer two address of another device while providing its own as well.	2461
	136	***Neighbor Advertisement***	Provides information about a host to other devices on the network.	2461
	137	***Redirect***	Redirects transmissions from a host to either an immediate neighbor on the network or a router.	2461
	138	***Router Renumbering***	Conveys renumbering information for router renumbering.	2894

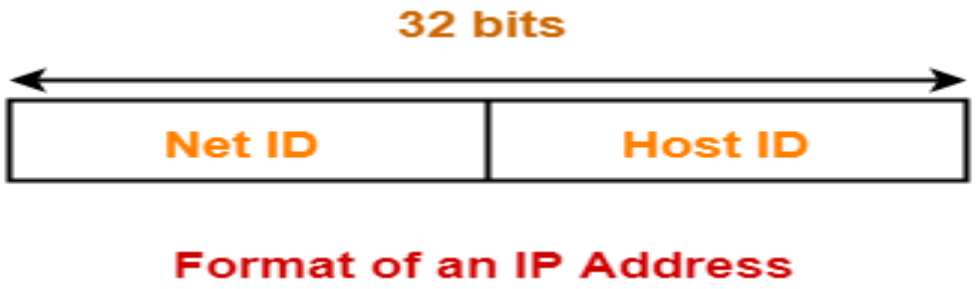
ICMP v6 Combines functionalities of ARP and IGMP protocol.

More on IP V4

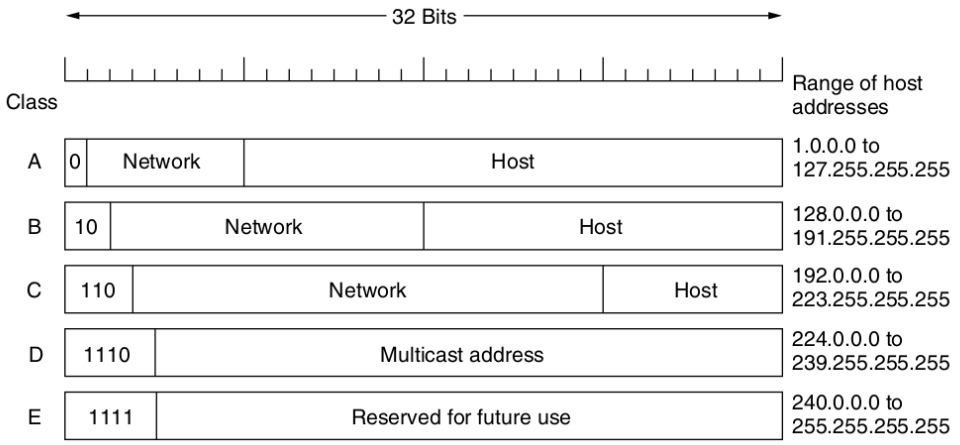
IP V4 allowed two ways in specifying the address.

Classful and CIDR

In both cases a part of the total bits are reserved to represent the network part and rest for the hosts.



Format of an IP Address



Subnet mask

Special IP address in which that bits representing the network part is set as 1 and host part as 0.

For class B -> The mask will be 255.255.0.0

The network part should be contigous.255.0.0255 is an invalid mask.

Given any ip address bitwise ‘and’ operation with the mask will return the network address.

Take ones compliment of mask and perform bitwise AND to get the network part.

	Binary form	Dot-decimal notation
IP address	11000000.00000000.00000010.10000010	192.0.2.130
Subnet mask	11111111.11111111.11111111.00000000	255.255.255.0
Network prefix	11000000.00000000.00000010.00000000	192.0.2.0
Host identifier	00000000.00000000.00000000.10000010	0.0.0.130

Usable IP address

Let us take a class C address. 192.168.10.1

We know that the last 8 bits in class C is meant to represent the host.

Theoritically we can address around 2^8 hosts [8 bits for the host]

But practically **there are two addresses** in any IP range which are not assigned to any host.

In the host part where all bits are Zero --> Start of address

In the host part where all bits are One --> Brodacast in that IP range

So in the above example 192.168.10.0 and 192.168.10.255 are not used for any host.

Maximum no.of hosts in any case is **(2^n)-2** where n is the number of bits used to represent the hosts.

The concept of subnetting

There might occur cases in which we need to have flexibility in the allocation of IP addresses.

We can borrow bits from the host part to create sub networks and the process is known as subnetting.

By doing so we will have more networks but the total number of hosts will come down.

Consider the class C address 200.1.2.0

The default mask for this 255.255.255.0

Lets split this network into two.

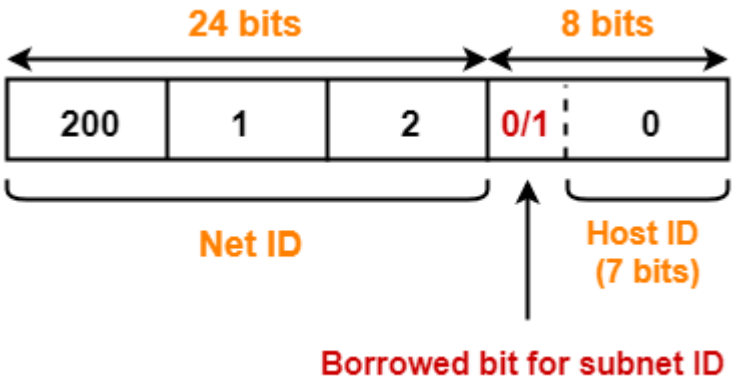
To do that we need to get the number of bits that needs to be taken from the host part.

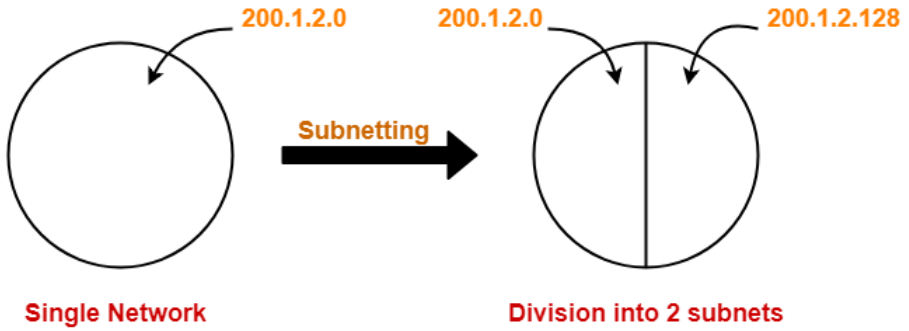
Since 2^1 is 2 we need to borrow one bit.

The starting IP address of the two networks become

a.200.1.2.**0**0000000 = 200.1.2.0

b.200.1.2.**1**0000000=200.1.2.128





More details on the subnet 1

IP Address of the subnet = 200.1.2.0

Total number of IP Addresses = 27 = 128

Total number of hosts that can be configured = 128 – 2 = 126 [Can use 7 bits]

Range of IP Addresses = [200.1.2.00000000, 200.1.2.01111111] = [200.1.2.0, 200.1.2.127]

The addresses 200.1.2.0, 200.1.2.127 are not assigned to any specific host.

Direct Broadcast Address = 200.1.2.01111111 = 200.1.2.127

More details on the subnet 2

IP Address of the subnet = 200.1.2.128

Total number of IP Addresses = 27 = 128

Total number of hosts that can be configured = 128 – 2 = 126

Range of IP Addresses = [200.1.2.10000000, 200.1.2.11111111] = [200.1.2.128, 200.1.2.255]

The addresses 200.1.2.128, 200.1.2.255 are not assigned to any host.

Direct Broadcast Address = 200.1.2.11111111 = 200.1.2.255

Division into 4 subnets

If four subnets needs to be created we have to borrow 2 bits – 2^2=4.

So the IP addresses start at

a. 200.1.2.**00**000000 =200.1.2.0

b.200.1.2.**01**000000=200.1.2.64

c.200.1.2.**10**000000=200.1.2.128

d.200.1.2.**11**000000=200.1.2.192

The address scheme can also be represented as 200.1.2.0/26