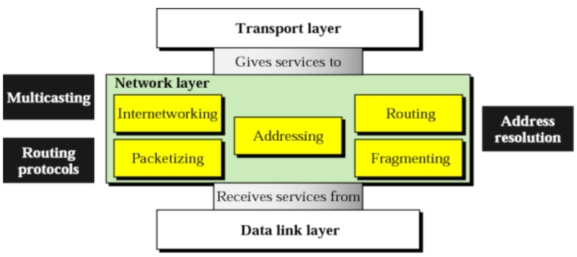
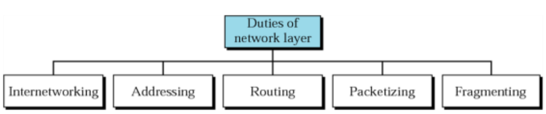
Unit - III
Network Layer

Position of network layer



Position of network layer



Services

- Packetizing:
  - One duty of the network layer is to carry a payload from the source to the destination without changing it or using it.
  - The source host receives the payload from an upper-layer protocol, adds a header that contains the source and destination addresses and some other information that is required by the network-layer protocol (as discussed later) and delivers the packet to the data-link layer.
  - The source is not allowed to change the content of the payload unless it is too large for delivery and needs to be fragmented.

Services

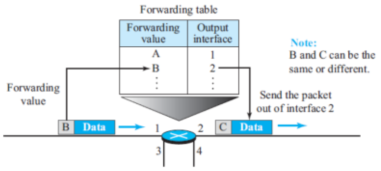
- Packetizing:
  - The destination host receives the network-layer packet from its data-link layer,
  - Decapsulates the packet, and delivers the payload to the corresponding upper-layer protocol.
  - The routers in the path are not allowed to decapsulate the packets they received unless the packets need to be fragmented
  - The routers are not allowed to change source and destination addresses either. They just inspect the addresses for the purpose of forwarding the packet to the next network on the path.

Services

- Routing and Forwarding:
  - The network layer is responsible for routing the packet from its source to the destination.
  - If there is more than one route from the source to the destination, the network layer is responsible for finding the best one among these possible routes.
  - Forwarding can be defined as the action applied by each router when a packet arrives at one of its interfaces.
  - The decision-making table a router normally uses for applying this action is sometimes called the *forwarding table* and sometimes the *routing table*.

Services

- Routing: Routing refers to the network-wide process that determines end-to-end paths that packets take from source to destination.
- Forwarding refers to the router-local action of transferring the packet from an input link interface to the appropriate output link interface.



Topic

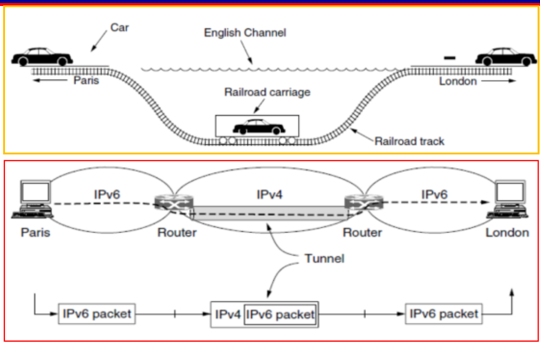
Internetworking

Internetworking

- internetwork or internet: Two or more networks are connected.
- Network may differ.

Item	Some Possibilities
Service offered	Connectionless versus connection oriented
Addressing	Different sizes, flat or hierarchical
Broadcasting	Present or absent (also multicast)
Packet size	Every network has its own maximum
Ordering	Ordered and unordered delivery
Quality of service	Present or absent; many different kinds
Reliability	Different levels of loss
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, packet, byte, or not at all

Internetworking



Tunnelling

Internetworking

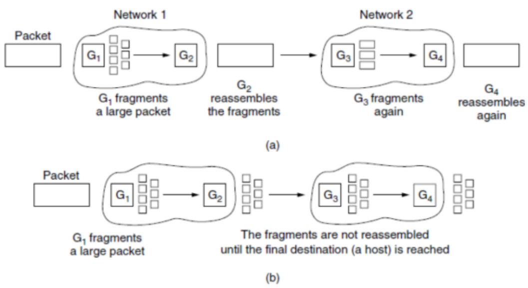


Figure 5-42. (a) Transparent fragmentation. (b) Nontransparent fragmentation.

Internetworking

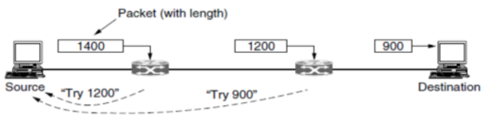
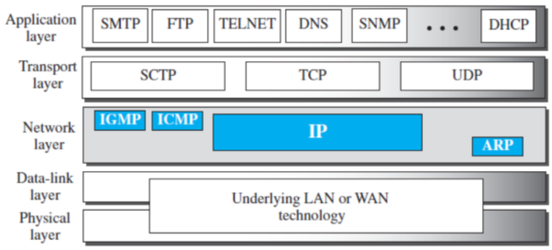


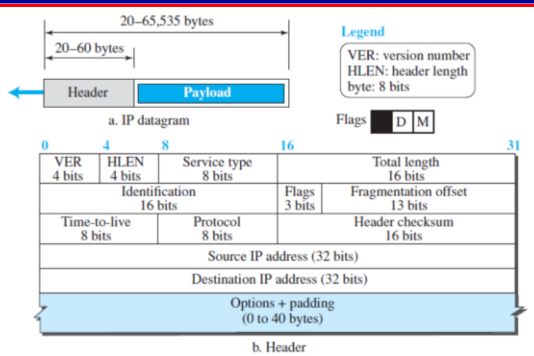
Figure 5-44. Path MTU discovery.

- Each IP packet is sent with its header bits set to indicate that no fragmentation is allowed to be performed.
- If a router receives a packet that is too large, it generates an error packet, returns it to the source, and drops the packet.

Network Layer Protocols



IP Datagram



IP Packet Format

Item	Description
Version	Specifies the version of the IP used. The current version of the IP protocol is 4.
HLEN	The total length of the header is calculated as 4-byte words. The total length is divided by 4 and the value is inserted in the field. The receiver needs to multiply the value of this field by 4 to find the total length..
Type of Service	Contains five subfields that specify the type of precedence, delay, throughput, and reliability desired for that packet. (The Internet does not guarantee this request.)
Total Length	Specifies the length of the datagram including both the header and the data measured in octets
Identification	Contains a unique integer that identifies the datagram. All the fragments contain same identification number.
Flags	The Fragment Flags specify whether the datagram can be fragmented and whether the current fragment is the last one.
Fragment Offset	This offset tells the exact position of the fragment in the original IP Packet.

IP Packet Format

Item	Description
Time to Live	To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross.
Protocol	Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e., the next level Protocol. For example, protocol number of ICMP is 1, TCP is 6 and UDP is 17.
Header Checksum	This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
Source Address	Specifies the Internet address of the sending host
Destination Address	Specifies the Internet address of the receiving host.
Options	This is optional field, which is used if the value of internet header length is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

Topic

Addressing

Learnig Objective

- ***Internet Address***
- ***Classful Addressing***
- ***Subnetting***
- ***Supernetting***
- ***Classless Addressing***
- ***Dynamic Address Configuration***
- ***Network Address Translation***

IP Addressing

Note:

An IP address is a 32-bit address.

Cont …

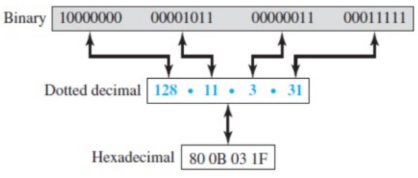
Note:

The IP addresses are unique and universal.

Address Space

- An address space is the total number of addresses used by the protocol.
- If a protocol uses b bits to define an address.
- IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than four billion)

Notation of IPv4



© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Dr. Arpita U3.22

Cont …

Change the following IP addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11111001 10011011 11111011 00001111

Solution

We replace each group of 8 bits with its equivalent decimal number (see Appendix B) and add dots for separation:

a. **129.11.11.239**

b. **249.155.251.15**

© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Dr. Arpita U3.23

Cont …

Change the following IP addresses from dotted-decimal notation to binary notation.

a. 111.56.45.78

b. 75.45.34.78

Solution

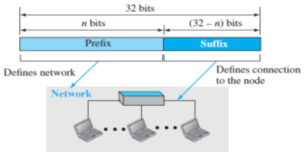
We replace each decimal number with its binary equivalent (see Appendix B):

a. **01101111 00111000 00101101 01001110**

b. **01001011 00101101 00100010 01001110**

© Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi-63 by Dr. Arpita U3.24

Hierarchy in addressing



- A 32-bit IPv4 address is also hierarchical, but divided only into two parts.
- The first part of the address, called the prefix, defines the network.
- the second part of the address, called the suffix, defines the node

Cont …

Note:

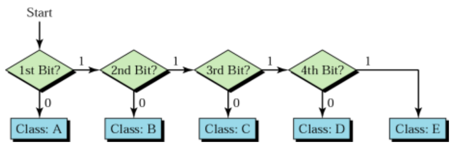
In classful addressing, the address space is divided into five classes: A, B, C, D, and E.

Cont …

Binary Notation

	First byte	Second byte	Third byte	Fourth byte
Class A	**0**			
Class B	**10**			
Class C	**110**			
Class D	**1110**			
Class E	**1111**			

Cont …



 U3.28

Cont …

Find the class of each address:

a. **0**0000001 00001011 00001011 11101111

b. **1111**0011 10011011 11111011 00001111

Solution

See the procedure in Figure 19.11.

a. **The first bit is 0; this is a class A address.**
b. **The first 4 bits are 1s; this is a class E address.**

 U3.29

Finding the class in decimal notation

	First byte	Second byte	Third byte	Fourth byte
Class A	**0 to 127**			
Class B	**128 to 191**			
Class C	**192 to 223**			
Class D	**224 to 239**			
Class E	**240 to 255**			

 U3.30

Cont …

Find the class of each address:

a. **227**.12.14.87

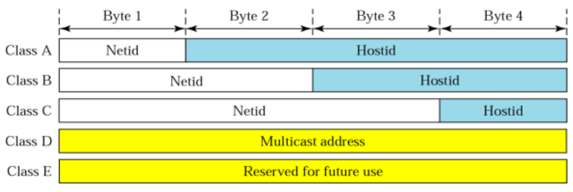
b. **252**.5.15.111

c. **134**.11.78.56

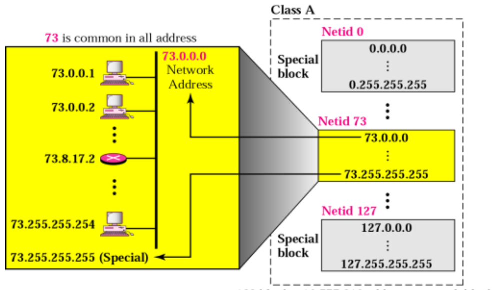
Solution

a. **The first byte is 227 (between 224 and 239); the class is D.**
b. **The first byte is 252 (between 240 and 255); the class is E.**
c. **The first byte is 134 (between 128 and 191); the class is B.**

Netid and Hostid



Blocks in class A



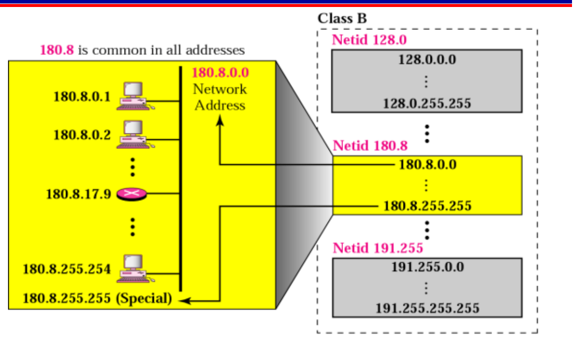
128 blocks: 16,777,216 addresses in each block

Cont …

Note:

Millions of class A addresses are wasted.

Blocks in class B



16384 blocks: 65536 addresses in each block

Cont …

Note:

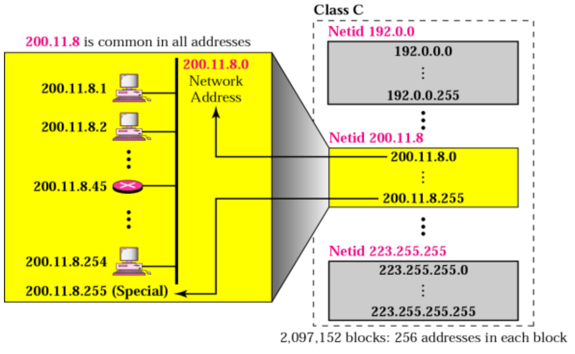
Many class B addresses are wasted.

Cont …

Note:

The number of addresses in class C is smaller than the needs of most organizations.

Blocks in class C



Cont …

Note:

In classful addressing, the network address is the one that is assigned to the organization.

Classes of IPv4 address

Address Class	1st Octet range in decimal	1st Octet bits (Blue Dots do not change)	Network (N) and Host (H) Portion	Default mask (Decimal)	Number of possible networks and hosts per network
A	0-127	00000000 - 01111111	N.H.H.H	255.0.0.0	128 Nets (2^7) 16,777,214 hosts (2^{24}-2)
B	128-191	10000000 - 10111111	N.N.H.H	255.255.0.0	16,384 Nets (2^{14}) 65,534 hosts (2^{16}-2)
C	192-223	11000000 - 11011111	N.N.N.H	255.255.255.0	2,09,150 Nets (2^{21}) 254 hosts (2^8-2)
D	224-239	11100000 - 11101111	NA (Multicast)	-	-
E	240-255	11110000 - 11111111	NA (Experimental)	-	-

nesoacademy.org

 U3.40

Cont …

Given the address 23.56.7.91, find the network address.

Solution

The class is A. Only the first byte defines the netid. We can find the network address by replacing the hostid bytes (56.7.91) with 0s. Therefore, the network address is 23.0.0.0.

 U3.41

Cont …

Given the address 132.6.17.85, find the network address.

Solution

The class is B. The first 2 bytes defines the netid. We can find the network address by replacing the hostid bytes (17.85) with 0s. Therefore, the network address is 132.6.0.0.

 U3.42

Cont …

Given the network address 17.0.0.0, find the class.

Solution

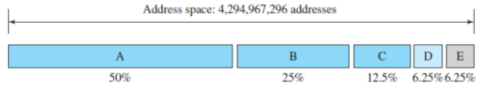
The class is A because the netid is only 1 byte.

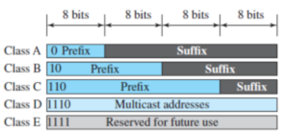
Cont …

Note:

A network address is different from a netid. A network address has both netid and hostid.

Occupation of the address space

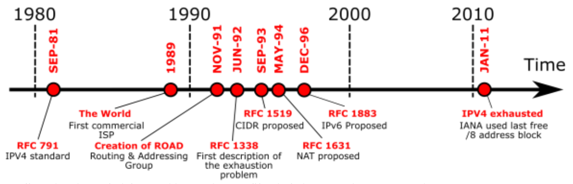




Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

- Class D is not divided into prefix and suffix. It is used for multicast addresses.
- Class D, Class E is not divided into prefix and suffix and is used as reserve.

Address Depletion



https://en.wikipedia.org/wiki/IPv4_address_exhaustion#/media/File:IPv4_exhaustion_time_line-en.svg

- The IP address space is managed globally by the Internet Assigned Numbers Authority and by five Regional Internet Registries (RIRs) responsible in their designated territories for assignment to end users and local Internet registries, such as Internet service providers.

Address Depletion

- The class A can be assigned to only 128 organizations in the world, but each organization needs to have a single network (seen by the rest of the world) with 16,777,216 nodes (computers in this single network).
- Class B addresses were designed for midsize organizations, but many of the addresses in this class also remained unused.
- In Class C, the number of addresses that can be used in each network (256) was so small that most companies were not comfortable using a block in this address

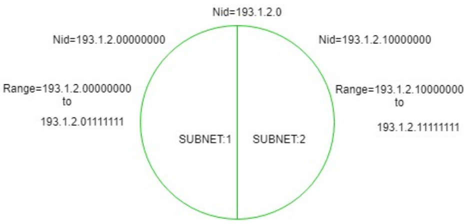
Address Depletion

- Class D addresses were designed for multicasting.
  - Each addresses is used to define one group of hosts.
  - The internet authority wrongly predicted the no. of groups
- Class E addresses were almost never used, wasting the whole class.

Subnetting

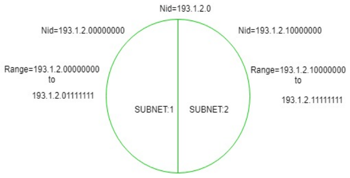
- To alleviate address depletion, two strategies were proposed and, to some extent, implemented:
  - ✓ Subnetting
  - ✓ Supernetting.
- In subnetting, a class A or class B block is divided into several subnets.
- Each subnet has a larger prefix length than the original network.

Subnetting



- It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.

Subnetting



For Subnet-1:
The first bit which is chosen from the host id part is zero

The range of subnet-1
193.1.2.0 to 193.1.2.127

For Subnet-2:
The first bit which is chosen from the host id part is one

The range of subnet-2
193.1.2.128 to 193.1.2.255

Supernetting

- Supernetting is the opposite of Subnetting.
- In subnetting, a single big network is divided into multiple smaller subnetworks.
- In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.
- Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry.

Supernetting

- Combining these networks into one network
  192.168.0.0
  192.168.1.0
  192.168.2.0
  192.168.3.0
- Write all the IP Addresses in binary and Find matching bits from left to right

11000000.10101000.00000000.00000000
11000000.10101000.00000001.00000000
11000000.10101000.00000010.00000000
11000000.10101000.00000011.00000000

Supernetting

11000000.10101000.00000000.00000000
11000000.10101000.00000001.00000000
11000000.10101000.00000010.00000000
11000000.10101000.00000011.00000000

- Rewrite the matching numbers and add the remaining zeros, because you are converting network bits into host bits.

11000000.10101000.00000000.00000000

192.168.0.0

Supernetting

- Find the new subnet mask. Put “1s” in the matching networking part, and all zeros in the host part.

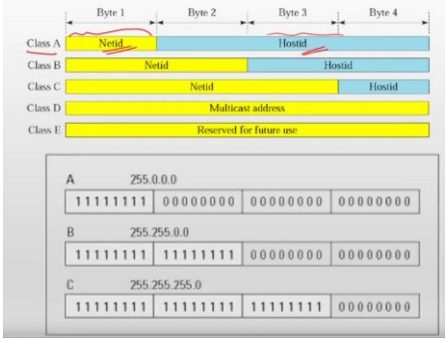
  11111111.11111111.11111100.00000000
- New subnet mask 255.255.252.0

Supernetting

S. NO	Subnetting	Supernetting
1.	Subnetting is the procedure to divide the network into sub-networks.	While supernetting is the procedure of combine the small networks.
2.	In subnetting, Network id's bits are increased.	While in supernetting, Host ID's bits are increased.
3.	In subnetting, The mask bits are moved towards right.	While In supernetting, The mask bits are moved towards left.
4.	Subnetting is implemented via Variable-length subnet masking.	While supernetting is implemented via Classless interdomain routing.
5.	In subnetting, Address depletion is reduced or removed.	While It is used for simplify routing process.

https://www.geeksforgeeks.org/difference-between-subnetting-and-supernetting/?ref=rp

Subnet Mask



Masking

8.20.15.1 = 00001000.00010100.00001111.00000001

255.0.0.0 = 11111111.00000000.00000000.00000000

- Any address bits which have corresponding mask bits set to 1 represent the network ID
- Any address bits that have corresponding mask bits set to 0 represent the node ID

8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000

And 00001000. 00000000.00000000.00000000

Net ID

Masking

- ANDing can be used to determine what subnetwork the address belongs to, as well as what other addresses belong to the same subnet.

A's Subnet mask	11111111	11111111	11111111	00000000
A's IP address	00001010	00000001	10010111	00001010
B's IP address	00001010	00000001	10010111	00000011

A's Subnet mask	11111111	11111111	11111111	00000000
A's IP address	00001010	00000001	10010111	00001010
C's IP address	01000000	11100011	10100000	00010111

- After getting Network Id, A's and B's Network bits are compared, if they match, they are in the same network.
- Otherwise, if bits are different means two network ids are of different network. As in case A's and C's.

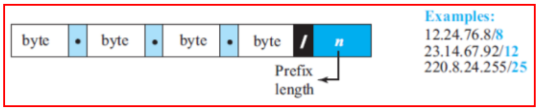
https://www.youtube.com/watch?v=yLeuGOOrUvo

Classless addressing

- Subnetting and supernetting in classful addressing did not really solve the address depletion problem.
- A short-term solution was also devised to use the same address space but to change the distribution of addresses to provide a fair share to each organization.
- The class privilege was removed from the distribution to compensate for the address depletion is called Classless Addressing
- In classless addressing, variable-length blocks are used that belong to no classes.

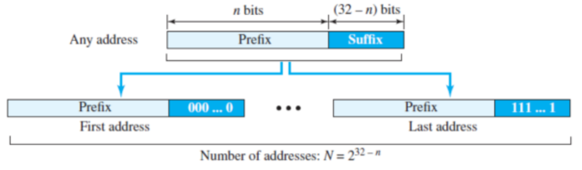
Classless addressing

- In classless addressing, the whole address space is divided into variable length blocks. The prefix in an address defines the block (network); the suffix defines the node (device).
- The notation is informally referred to as slash notation and formally as classless interdomain routing or CIDR (pronounced cider) strategy.



Classless addressing

- The number of addresses in the block is found as $N = 2^{32-n}$.
- To find the first address, we keep the n leftmost bits and set the (32 − n) rightmost bits all to 0s.
- To find the last address, we keep the n leftmost bits and set the (32 − n) rightmost bits all to 1s.



Classless addressing

- A classless address is given as 167.199.170.82/27. We can find the above three pieces of information as follows.

<u>The first address, Last Address and Total no of Blocks</u>

Address:	167.199.170.82/27	10100111 11000111 10101010 01010010
First address:	167.199.170.82/27	10100111 11000111 10101010 01000000
Last Address:	167.199.170.82/27	10100111 11000111 10101010 01011111

Total no of blocks= 2^{32-n}

$= 2^{32-27}$

$= 2^{5} = 32$

Classless addressing

- Another way to find the first and last addresses in the block is to use the address mask.
- To extract the information in a block, using the three bit-wise operations NOT, AND, and OR.
  - The number of addresses in the block N = NOT (mask) + 1.
  - The first address in the block = (Any address in the block) AND (mask).
  - The last address in the block = (Any address in the block) OR [(NOT (mask)].

Classless addressing

- A classless address is given as 167.199.170.82/27. We can find the three information using address mask.
- Address mask for 167.199.170.82/27: 255.255.255.224
  - Number of addresses in the block: N = NOT (mask) + 1= =0.0.0.31 + 1 = 32 addresses
  - First address: First = (address) AND (mask) = 167.199.170.82
  - Last address: Last = (address) OR (NOT mask) = 167.199.170.255

Classless addressing

- Block Allocation:
  - All the IP Addresses in the CIDR block must be contiguous.
  - The size of the block must be presentable as power of 2.
  - First IP Address of the block must be divisible by the size of the block.

Special Addresses

- This-host Address:
  - The only address in the block 0.0.0.0/32 is called the this-host address.
  - It is used whenever a host needs to send an IP datagram but it does not know its own address to use as the source address.
- Limited-broadcast Address:
  - The only address in the block 255.255.255.255/32 is called the limited-broadcast address.
  - It is used whenever a router or a host needs to send a datagram to all devices in a network

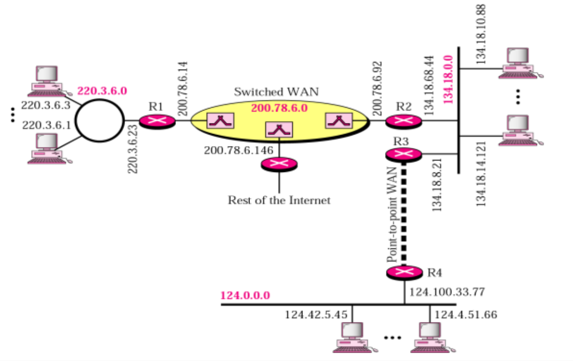
Special Addresses

- Loopback Address:
  - The block 127.0.0.0/8 is called the loopback address.
  - A packet with one of the addresses in this block as the destination address never leaves the host.
- Private Addresses:
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 169.254.0.0/16
- Multicast Addresses:
  - The block 224.0.0.0/4 is reserved for multicast addresses

Special Addresses

S. NO	Classful Routing	Classless Routing
1.	In classful routing, VLMS(Variable Length Subnet Mask) is not supported.	While in classless routing, VLMS(Variable Length Subnet Mask) is supported.
2.	Classful routing does not import subnet mask.	Whereas it imports subnet mask.
3.	In classful routing, address is divided into three parts which are: Network, Subnet and Host.	While in classless routing, address is divided into two parts which are: Subnet and Host.
4.	In classful routing, regular or periodic updates are used.	Whereas in this, triggered updates are used.
5.	In classful routing, CIDR(Classless Inter-Domain Routing) is not supported.	While in classless routing, CIDR(Classless Inter-Domain Routing) is supported.

Sample internet



Routing

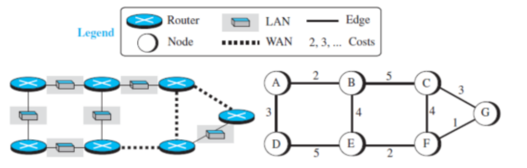
- The routing can be possible if a router has a forwarding table to forward a packet to the appropriate next node on its way to the final destination or destinations.
- To make the forwarding tables of the router, the Internet needs routing protocols that will be active all the time in the background and update the forwarding tables.
- Unicast routing: If a datagram is destined for only one destination (one-to-one delivery)
- Multicast routing: If the datagram is destined for several destinations (one-to-many delivery)

Routing

- The routing algorithms can be classified as follows:
  - Adaptive Algorithms:
    - ✓These are the algorithms that change their routing decisions whenever network topology or traffic load changes.
    - ✓Also known as dynamic routing, these make use of dynamic information such as current topology, load, delay, etc. to select routes.
  - Non-Adaptive Algorithms
    - ✓These are the algorithms that do not change their routing decisions once they have been selected.
    - ✓This is also known as static routing as a route to be taken is computed in advance.

Routing

- To find the best route, an internet can be modeled as a graph.
- In routing, however, the cost of an edge has a different interpretation in different routing protocols



a. An internet b. The weighted graph

Routing Table

- Static Routing Table:
  - Contains information entered manually.
  - When a table is created, it cannot update automatically.
  - A static routing table can be used in a small internet that does not change very often
- Dynamic Routing Table
  - Updated periodically by using one of the dynamic routing protocols such as RIP, OSPF, or BGP
  - Whenever there is a change in the Internet, such as a shutdown of a router or breaking of a link, the dynamic routing protocols update all the tables in the routers (and eventually in the host) automatically.

Routing Table

Mask	Network address	Next-hop address	Interface	Flags	Reference count	Use
....	....	....	....	....	....	....

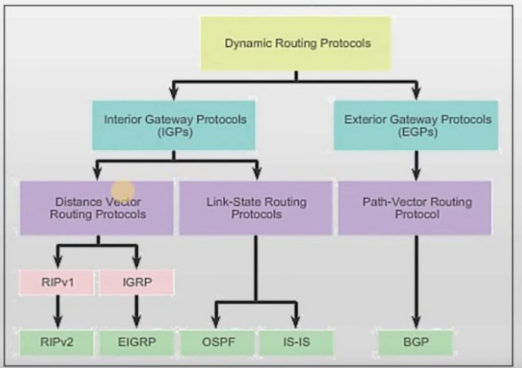
- Mask: This field defines the mask applied for the entry
- Network address: This field defines the network address to which the packet is finally delivered.
- Next-hop address: This field defines the address of the next-hop router to which the packet is delivered
- Interface: This field shows the name of the interface.

Routing Table

Mask	Network address	Next-hop address	Interface	Flags	Reference count	Use
....	....	....	....	....	....	....

- Flags: This field defines up to five flags. Flags are on/off switches that signify either presence or absence. The five flags are U (up), G (gateway), H (host-specific),D (added by redirection), and M (modified by redirection).
- Reference count: This field gives the number of users of this route at the moment.
- Use: This field shows the number of packets transmitted through this router for the corresponding destination.

Types of routing protocols



Unicast Routing

- Autonomous System (AS):
  - Group of networks and routers under the authority of a single administration.
- Routing inside an autonomous system is referred to as intradomain routing.
- Routing between autonomous systems is referred to as interdomain routing.

Routing

- Least-Cost Routing:
  - When an internet is modeled as a weighted graph, one of the ways to interpret the best route from the source router to the destination router is to find the least cost between the two.
  - The source router chooses a route to the destination router in such a way that the total cost for the route is the least cost among all possible routes.

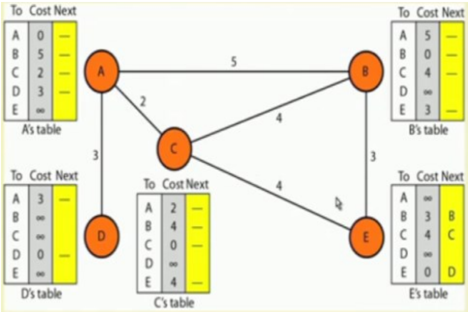
Unicast Routing: Distance Vector Routing

- In distance vector routing, the least-cost route between any two nodes is the route with minimum distance.
- Each node maintains a vector (table) of minimum distances to every node.
- The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).
- It follows the Bellman-Ford Algorithm to find the optimal route.

Unicast Routing: Distance Vector Routing

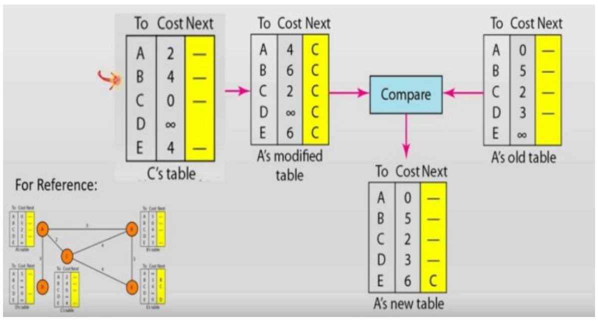
- Initialization
  - Each node can know only the distance between itself and its immediate neighbors those directly connected to it.
- Sharing
  - In distance vector routing, each node shares its routing table with its immediate neighbors periodically and when there is a change.
- Updating
  - The receiving node needs to add the cost between itself and the sending node to each value in the second column.

Unicast Routing: Distance Vector Routing



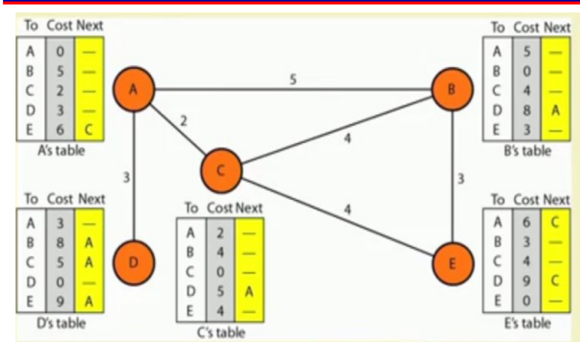
Initialisation

Unicast Routing: Distance Vector Routing



Updation

Unicast Routing: Distance Vector Routing

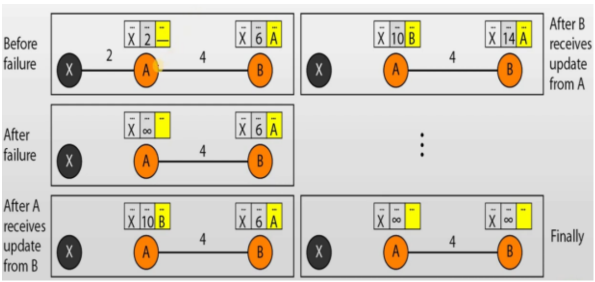


Unicast Routing: Distance Vector Routing

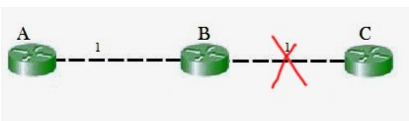
- The Routing Information Protocol (RIP) is an intradomain routing protocol used inside an autonomous system.
- It is a very simple protocol based on distance vector routing
- The metric used by RIP is very simple; the distance is defined as the number of links (networks) to reach the destination (Hop Count).
- Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.

Problem with DVR

- 2 node instability problem



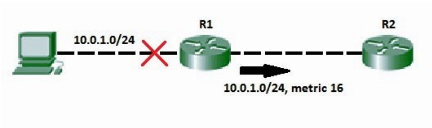
Unicast Routing: Distance Vector Routing



- A will then receive updates from B later and update its cost to 4
- They will then go on feeding each other bad information toward infinity which is called as Count to Infinity problem.

Unicast Routing: Distance Vector Routing

- Solution of Count to Infinity
  - Route Poisoning
    - ✓Route poisoning refers to the practice of advertising a route, but with a special metric value called Infinity.
    - ✓When a route fails, distance vector protocols spread the bad news about a route failure by poisoning the route.
    - ✓The main disadvantage of poison reverse is that it can significantly increase the size of routing announcements



 U3.88

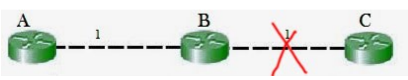
Unicast Routing: Distance Vector Routing

- Solution of Count to Infinity
  - Route Poisoning
    - ✓Route poisoning refers to the practice of advertising a route, but with a special metric value called Infinity.
    - ✓When a route fails, distance vector protocols spread the bad news about a route failure by poisoning the route.
    - ✓The main disadvantage of poison reverse is that it can significantly increase the size of routing announcements

 U3.89

Unicast Routing: Distance Vector Routing

- Solution of Count to Infinity
  - Split Horizon
    - ✓Preventing a router from advertising a route back to the interface from which it was updated.



    - ✓If the link between B and C goes down, B will update its routing table with the value of 16(infinity)
    - ✓Node A does not advertise its route for C (namely A to B to C) back to B because A was updated its route to C only from B. *(Split Horizon)*

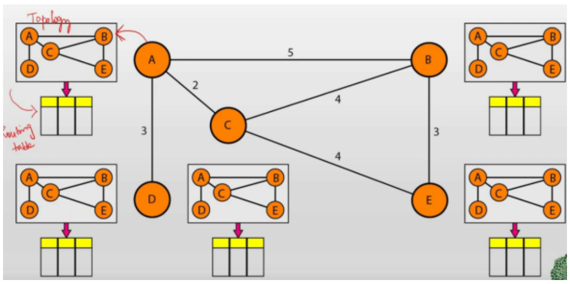
https://www.youtube.com/watch?v=eNbNDVE8tGc

 U3.90

Unicast Routing: Link State Routing

- Distance vector routing was used in the ARPANET until 1979.
- The primary problem was that the algorithm often took too long to converge after the network topology changed.
- It was replaced by an entirely new algorithm, now called link state routing.
- Variants of link state routing called IS-IS (Intermediate System to Intermediate System) and OSPF (Open Shortest Path First) are the routing algorithms that are most widely used inside large networks and the Internet today.

Link State Routing



Unicast Routing: Link State Routing

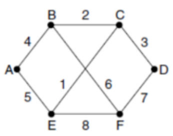
- Each router must do the following Steps to make it work
  - Creation of Link State Packet (LSP)
  - Flooding of Link State packet
  - Formation of shortest path tree
  - Computing the Routing table from shortest path tree

Creation of link state packet

- LSP are created with huge amout of data.
- It's important data are
  - ✓Node identity
  - ✓List of Links
  - ✓Sequence Number
  - ✓Age
- Created on 2 occasion
  - ✓There is a change in topology of domain
  - ✓On a periodic basis

Unicast Routing: Link State Routing

- Building Link State Packets
  - ✓Once the information needed for the exchange has been collected, the next step is for each router to build a packet containing all the data.
  - ✓The packet starts with the identity of the sender, followed by a sequence number and age and a list of neighbors and costs.



Link State Packets

A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

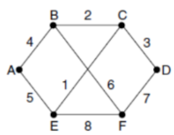
Flooding

- Distributing the Link State Packets
  - ✓Flooding is used to distribute the link state packets to all routers.
  - ✓Each packet contains a sequence number that is incremented for each new packet sent.
  - ✓When a new link state packet comes in, it is checked against the list of packets already seen.
    - If it is new, it is forwarded on all lines except the one it arrived on.
    - If it is a duplicate, it is discarded.
    - If a packet with a sequence number lower than the highest one seen so far ever arrives, it is rejected.

Unicast Routing: Link State Routing

- Formation of shortest path
  - ✓ After advertising the LSP (Link State Packets) and receiving the response from the all nodes, a link state database is created.

LSDB=Link State Database

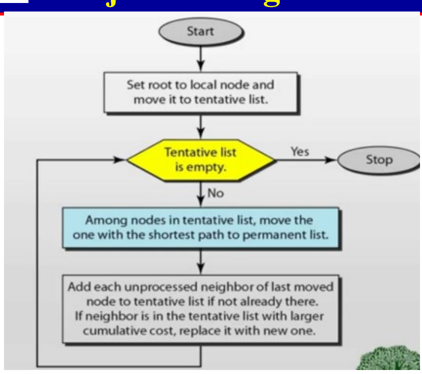


	A	B	C	D	E	F
A	0	4	inf	inf	5	inf
B	4	0	2	inf	inf	6
C	inf	2	0	3	1	inf
D	inf	inf	3	0	inf	7
E	5	inf	1	inf	0	8
F	inf	6		7	8	0

Unicast Routing: Link State Routing

- Computing the New Routes
  - ✓ Once a router has accumulated a full set of link state packets, it can construct the entire network graph, i.e. Link State Database because every link is represented.
  - ✓ Dijkstra's algorithm can be run locally to construct the shortest paths to all possible destinations.
  - ✓ The results of this algorithm tell the router which link to use to reach each destination.
  - ✓ This information is installed in the routing tables, and normal operation is resumed.

Dijkstra's algorithm



Unicast Routing: Link State Routing

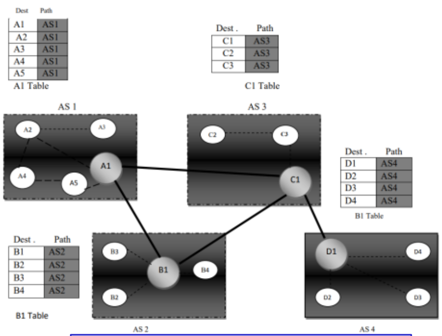
Distance Vector Routing	Link State Routing
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkastra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

https://www.geeksforgeeks.org/difference-between-distance-vector-routing-and-link-state-routing/

Unicast Routing: Path Vector Routing

- The principle of path vector routing is similar to that of distance vector routing.
- It assumes that there is one node in each Autonomous System (AS) that acts on behalf of the entire autonomous system is called Speaker node .
- The speaker node in an AS creates a routing cable and advertises to the speaker node in the neighboring ASs .
- A speaker node advertises the path, not the metrics of the nodes, in its autonomous system or other autonomous systems.

Unicast Routing: Path Vector Routing



Initial routing tables in path vector routine

Unicast Routing: Path Vector Routing

- A speaker in an autonomous system shares its table with immediate neighbours.
  - Node A1 share its table with nodes B1 and C1
  - Node C1 share its table with nodes A1,B1 and D1
  - Node B1 share its table with nodes A1 and C1
  - Node D1 share its table with node C1
- If router A1 receives a packet for nodes A3 , it knows that the path is in AS1.
- The path from a source to all destinations is also determined by the best spanning tree.
- If there is more than one route to a destination, the source can choose the route that meets its policy best

IPv6

- ***IPv6 Addresses***
- ***Categories of Addresses***
- ***IPv6 Packet Format***
- ***Fragmentation***
- ***ICMPv6***
- ***Transition***

Why Do We need a New IP Structure

- Address Space is not sufficient
- Need real time service support
- Mobile applications are unmanageable
- IPv4 was less secure

IPv6

- Larger address space
- Globally unique
- Use of prefix instead of address classes
- Built in authentication and encryption
- Compatibility with IPv4
- Auto Configuration of network interfaces

IPv6 address

128 bit address – represented in 8 hexadecimal number

1111110111101100 ••• 1111111111111111

FDEC : BA98 : 7654 : 3210 : ADBF : BBFF : 2922 : FFFF

Abbreviated address

Unabbreviated

FDEC : BA98 : 0074 : 3210 : 000F : BBFF : 0000 : FFFF

FDEC : BA98 : 74 : 3210 : F : BBFF : 0 : FFFF

Abbreviated

Abbreviated address with consecutive zeros

Abbreviated

FDEC : 0 : 0 : 0 : 0 : BBFF : 0 : FFFF

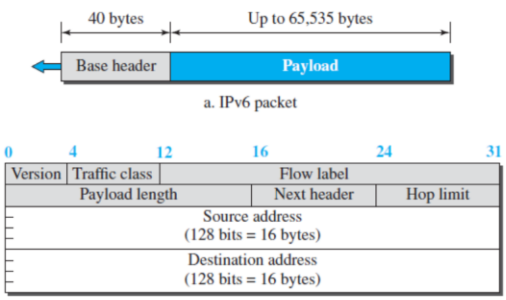
FDEC : : BBFF : 0 : FFFF

More Abbreviated

CIDR address

FDEC : 0 : 0 : 0 : 0 : BBFF : 0 : FFFF/60

Format of an IPv6 datagram

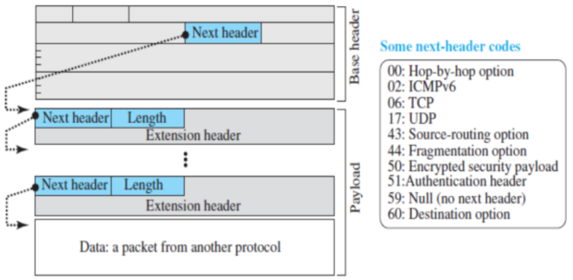


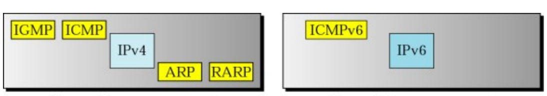
b. Base header

Format of an IPv6 datagram

Version	The 4-bit version field defines the version number of the IP. For IPv6, the value is 6
Traffic class	It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded.
Flow label	It is designed to provide special handling for a particular flow of data. Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real-time service.
Payload length	Defines the length of the IP datagram excluding the header
Next header	The next header is an 8-bit field defining the type of the first extension header (if present)
Hop limit	Time to Live field

Format of an IPv6 datagram





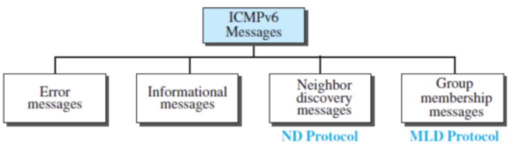
Network layer in version 4

Network layer in version 6

IPV6 Protocol

4. The identification, flag, and offset fields are eliminated from the base header in IPv6. They are included in the fragmentation extension header.
5. The TTL field is called hop limit in IPv6.
6. The protocol field is replaced by the next header field.
7. The header checksum is eliminated because the checksum is provided by upper layer protocols; it is therefore not needed at this level.
8. The option fields in IPv4 are implemented as extension headers in IPv6.

ICMPv6



ICMPv6

- Error-Reporting Messages
  - Four types of errors are handled
    - ✓Destination Unreachable
      - When a router cannot forward a datagram or a host cannot deliver the content of the datagram to the upper layer protocol
    - ✓Packet Too Big
      - IPv6 does not fragment at the router, if a router receives a datagram that is larger than the maximum transmission unit (MTU)
    - ✓Time Exceeded
      - Time-to-live value becomes zero
    - ✓Parameter Problems
      - Any ambiguous or missing value in any field,

ICMPv6

- Informational Messages
  - Echo-Request Message
  - Echo-Reply Message
  - The echo-request and echo-reply messages are designed to check whether two devices on the Internet can communicate with each other.

ICMPv6

- Neighbor-Discovery Messages
  - Two new protocols
    - ✓Neighbor-Discovery (ND) protocol
    - ✓Inverse-Neighbor-Discovery (IND) protocol
  - These two protocols are used by nodes (hosts or routers) on the same link (network) for three main purposes.
    - ✓Hosts use the ND protocol to find routers in the neighborhood that will forward packets for them.
    - ✓Nodes use the ND protocol to find the link-layer addresses of neighbors (nodes attached to the same network).
    - ✓Nodes use the IND protocol to find the IPv6 addresses of neighbors.

ICMPv6

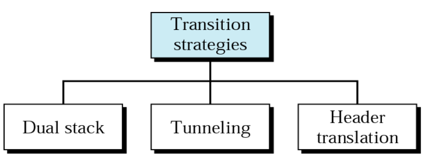
- Neighbor-Discovery Messages
  - Router-Solicitation Message
    - ✓A host uses the router-solicitation message to find a router in the network that can forward an IPv6 datagram for the host.
  - Router-Advertisement Message
    - ✓The router-advertisement message is sent by a router in response to a router solicitation message.
  - Neighbor-Solicitation Message
    - ✓This message is sent when a host or router has a message to send to a neighbor.
    - ✓The sender knows the IP address of the receiver but needs the data-link address of the receiver.

ICMPv6

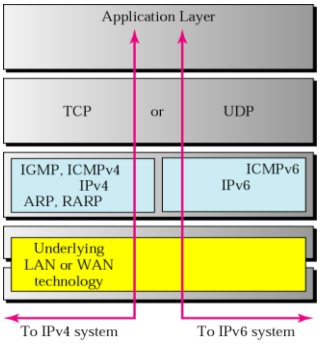
- Neighbor-Discovery Messages
  - Neighbor-Advertisement Message
    - ✓The neighbor-advertisement message is sent in response to the neighbor-solicitation message.
  - Inverse-Neighbor-Solicitation Message
    - ✓The inverse-neighbor-solicitation message is sent by a node that knows the link-layer address of a neighbor, but not the neighbor's IP address.
    - ✓The message is encapsulated in an IPv6 datagram using an all-node multicast address.
  - Inverse-Neighbor-Advertisement Message
    - ✓The inverse-neighbor-advertisement message is sent in response to the inverse-neighbor discovery message

ICMPv6

- Group Membership Messages
  - This is used when multicast delivery handling
    - ✓Membership-Query Message
      - A membership-query message is sent by a router to find active group members in the network.
    - ✓Membership-Report Message

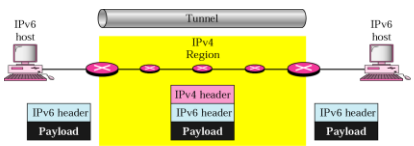


Dual Stack



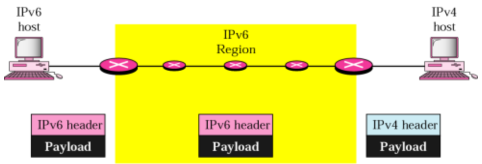
 U3.124

Tunneling



 U3.125

Header translation



 U3.126

Autoconfiguration

- One of the interesting features of IPv6 addressing is the autoconfiguration of hosts.
- In IPv6, DHCP protocol can still be used to allocate an IPv6 address to a host, but a host can also configure itself.
- When a host in IPv6 joins a network, it can configure itself using the following process:
  - The host first creates a link local address for itself.
  - The host then tests to see if this link local address is unique and not used by other hosts.
  - If the uniqueness of the link local address is passed, the host stores this address as its link local address

Mobile IP

- IP protocol that allows mobile computers to be connected to the Internet at any location where the connection is possible.
- The problem of locating a mobile host in a mobile domain is now imminent as the IP address assigned can no longer be restricted to a region.
- Every site that wants to allow its users to roam has to create a helper at the site called a home agent.

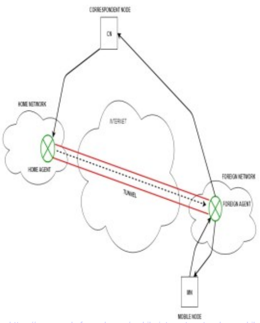
Mobile IP

- Terminologies:
  - Mobile Node (MN) : Communication device that the user carries
  - Home Network: Network to which the mobile node originally belongs as per its assigned IP address.
  - Home Agent (HA): Router in-home network to which the mobile node was originally connected
  - Home Address: permanent IP address assigned to the mobile node
  - Foreign Network: Current network to which the mobile node is visiting.
  - Foreign Agent (FA): router in a foreign network to which the mobile node is currently connected.

Mobile IP

- Terminologies:
  - Correspondent Node (CN): Device on the internet communicating to the mobile node.
  - Care-of Address (COA): Temporary address used by a mobile node while it is moving away from its home network.
    - ✓Foreign agent COA: The COA could be located at the FA
    - ✓Co-located COA: if the MN temporarily acquired an additional IP address which acts as COA

Mobile IP



https://www.geeksforgeeks.org/mobile-internet-protocol-or-mobile-ip/

- The correspondent node sends the data to the mobile node.
- Data packets contain the correspondent node's address (Source) and home address (Destination).
- Packets reach the home agent.
- But now mobile node is not in the home network, it has moved into the foreign network.
- The foreign agent sends the care-of-address to the home agent to which all the packets should be sent.
- A tunnel will be established between the home agent and the foreign agent by the process of tunneling.
- Foreign agent, receives the data packets, decapsulates them, and sends them to the mobile node.
- The mobile node reply in response to the foreign agent and FA sends reply directly to the CN

Mobile IP

- Agent Discovery:
  - Agents advertise their presence by periodically broadcasting their agent advertisement messages.
  - The mobile node receiving the agent advertisement messages observes whether the message is from its own home agent and determines whether it is in the home network or foreign network.
- Agent Registration:
  - Mobile node after discovering the foreign agent sends a registration request (RREQ) to the foreign agent.
  - The foreign agent, in turn, sends the registration request to the home agent with the care-of-address.

Mobile IP

- Tunneling:
  - It establishes a virtual pipe for the packets available between a tunnel entry and an endpoint.
  - Home agent encapsulates the data packets into new packets in which the source address is the home address and destination is the care-of-address.

 U3.133

IP Multicasting

- In multicast communication, the destination of the packet defines one group, but that group may have more than one member on the internet.
- The multicast routing decision at each router depends not only on the destination of the packet, but also on the source of the packet.

a. Packet sent out of two interfaces   b. Packet sent out of one interface

 U3.134

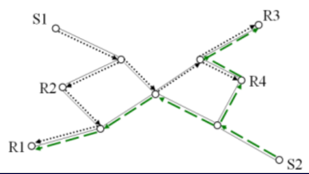
IP Multicasting

- Two Approaches
  - Source-Based Tree Approach
    - ✓Each router needs to create a separate tree for each source-group combination.
    - ✓if there are m groups and n sources on the internet, a router needs to create (m × n) routing trees
    - ✓In each tree, the corresponding source is the root, the members of the group are the leaves, and the router itself is somewhere on the tree.

 U3.135

IP Multicasting

- Two Approaches
  - Source-Based Tree Approach
    - ✓Each tree can therefore be defined by the sender id and the group id, or (S,G).
    - ✓All the trees are shortest path trees with the root in the multicast router closest to the sender
    - ✓Some of the trees in a group might well overlap

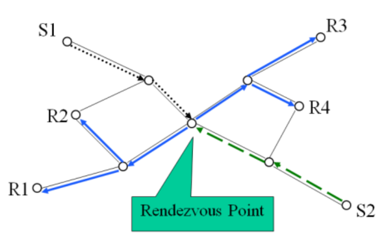


IP Multicasting

- Two Approaches
  - Group-Shared Tree Approach
    - ✓The group-shared tree approach is more efficient from the router performance perspective.
    - ✓Only one tree is built for each group.
    - ✓The tree has its root in a designated router called rendezvous point (RP) or core router.
    - ✓All senders in a group forward their multicast datagrams to the RP encapsulated in unicast datagrams.
    - ✓The RP decapsulates the unicast and forwards the multicast datagrams along the tree.
    - ✓ Since there are many senders in a group G, a group-shared tree is denoted (*,G)

IP Multicasting

- Two Approaches
  - Group-Shared Tree Approach



Recommended reading

1. Tanenbaum , A computer Networks: Prentice Hall
2. Stallings , High speed Networks :Printice Hall
3. Comer D. Computer Networks: Printice hall
4. Kurose, J and ross , Computer Networking : Addison Wesley