Advanced Computer Network

EDITION : 2019

Sub Code : 22520

MSBTE I SCHEME PATTERN
T. Y. DIPLOMA SEM V (ELECTIVE)
COMP ENGG./IT PROGRAM GROUP
(CO/CM/IF/CW)

- CHAPTERWISE SOLVED MSBTE QUESTIONS SUMMER 2015 to WINTER 2018

INCLUDES-I SCHEME PATTERN
SAMPLE PAPERS

TECHNICAL PUBLICATIONS
An Up-Thrust for Knowledge

Iresh A. Dhotre
Vilas S. Bagad

As per Revised Syllabus of

MSBTE - I SCHEME

Advanced Computer Network

T. Y. Diploma (Semester - V) Elective
Computer Engineering / IT Program Group (CO/CM/IF/CW)

Iresh A. Dhotre

M.E. (Information Technology)
Ex-Faculty, Sinhgad Collage of Engineering
Pune

Vilas S. Bagad

M.E. (E&TC), Microwaves
M.M.S.(Information systems)
Faculty, Institute of Telecommunication Management
Ex-Faculty, Sinhgad Collage of Engineering,
Pune

TECHNICAL PUBLICATIONS
An Up-Thrust for Knowledge

Website : www.technicalpublications.org
https://www.facebook.com/technicalpublications

Advanced Computer Network

T.Y. Diploma (Semester - V) Elective
Computer Engineering / IT Program Group (CO/CM/IF/CW)

First Edition : June 2019

Published by :
TECHNICAL PUBLICATIONS
Amit Residency, Office No.1, 412, Shaniwar Peth, Pune - 411030, M.S. INDIA
Ph.: +91-020-24495496/97, Telefax : +91-020-24495497
Email : sales@technicalpublications.org Website : www.technicalpublications.org

ISBN 978-93-89180-25-1

MSBTE I

PREFACE

The importance of **Advanced Computer Network** is well known in various engineering fields. Overwhelming respondse to our books on various subjects inspired us to write this book. The book is structured to cover the key aspects of the subject **Advanced Computer Network.**

The book uses plain, lucid language to explain fundamentals of this subject. The book provides logical method of explaining various complicated concepts and stepwise methods to explain the important topics. Each chapter is well supported with necessary illustrations, practical examples and solved problems. All chapters in this book are arranged in a proper sequence that permits each topic to build upon earlier studies. All care has been taken to make students comfortable in understanding the basic concepts of this subject.

Representative questions have been added at the end of each section to help the students in picking important points from that section.

The book not only covers the entire scope of the subject but explains the philosophy of the subject. This makes the understanding of this subject more clear and makes it more interesting. The book will be very useful not only to the students but also to the subject teachers. The students have to omit nothing and possibly have to cover nothing more.

We wish to express our profound thanks to all those who helped in making this book a reality. Much needed moral support and encouragement is provided on numerous occasions by our whole family. We wish to thank the **Publisher** and the entire team of **Technical Publications** who have taken immense pain to get this book in time with quality printing.

Any suggestion for the improvement of the book will be acknowledged and well appreciated.

Authors
D. A. Dhotre
V. S. Bagad

Dedicated to God.

SYLLABUS

Advanced Computer Network (22520)

Teaching Scheme			Credit (L + T + P)	Examination Scheme											
				Theory						Practical					
				Paper Hrs.	ESE		PA		Total		ESE		PA		Total	
L	T	P			Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min
3	-	2	5	3	70	28	30*	00	100	40	25#	10	25	10	50	20

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub - topics
Unit - I **Network Layer and Protocols**	1a. Explain significance of the given field in the packet format of Internet Protocol. 1b. Implement IP addressing for the given network. 1c. Explain significance of the given field in packet format of ICMPv4. 1d. Explain the given inefficiency in Mobile IP.	1.1 **IP Addressing :** Address Space, Notations, Classfull addressing, Classless addressing, Network Address Translation (NAT). 1.2 **Internet Protocol (IP) :** Datagram Format, Fragmentation, Options. 1.3 **ICMPv4 :** Messages, Debugging Tools, ICMP Checksum. 1.4 **Mobile IP :** Addressing, Agents, Three Phases, Inefficiency in Mobile IP. 1.5 **Vitrual Private Network :** VPN Technology.
Unit - II **Next Generation IP**	2a. Map the given IPv4 address to 1Pv6 address. 2b. Describe function of the given step in the stateless auto configuration process. 2c. Outline the given strategy of Transition from 1Pv4 to 1Pv6. 2d. Explain significance of the given field in Datagram format of 1Pv6.	2.1 **IPv6 Addressing :** Representation, address space, address space allocation, Autoconfiguration, Renumbering. 2.2 **Transition from IPv4 to IPv6 :** Dual Stack, Tunneling, Header Translation. 2.3 **IPv6 Protocol :** Packet format, Extension Header.

Unit - III **Unicast and Multicast Routing Protocols**	3a. Choose relevant routing Protocol for the given network situation. 3b. Compare Dynamic Routing and Static Routing on the given aspect. 3c. Calculate shortest paths from a single source vertex to all the other vertices in the given weighted digraph. 3d. Explain functioning of the given multicast routing protocol.	3.1 **Introduction :** Inter-domain, Intra-domain Routing. 3.2 **Routing Algorithms :** Distance Vector Routing, Bellman-Ford algorithm, Link State Routing, Path Vector Routing. 3.3 **Unicast Routing Protocols :** Internet Structure, Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol Version 4 (BGP4). 3.4 **Introduction :** Unicast, Multicast and Broadcast. 3.5 **Intradomain Multicast Protocols:** Multicast Distance Vector (DVMRP), Multicast Link State (MOSPF), Protocol Independent Multicast (PIM).
Unit - IV **Transport Layer Protocols**	4a. Explain significance of the given field in UDP Packet format. 4b. Describe the given State Transition of TCP. 4c. Explain significance of the given field in TCP Packet format. 4d. Describe the given field in the packet format of SCTP. 4e. Explain the functioning of the given Protocol with Flow and Error control by taking an example.	4.1 **User Datagram Protocol :** User Datagram, UDP Services, UDP Applications. 4.2 **Transmission Control Protocol :** TCP Services, TCP features, Segment, A TCP Connection, State Transition Diagram, Windows in TCP, Flow Control, Error Control, TCP Congestion Control, TCP Timers, Options. 4.3 **SCTP :** SCTP Services, SCTP Features, Packet Format, An SCTP Association, Flow Control, Error Control.
Unit - V **Application Layer protocols**	5a. Explain function of the given application layer protocol. 5b. Explain function of the given FTP command. 5c. Explain working of the given components in the Architecture of Electronic Mail. 5d. Explain process of resolving the space, given host name into IP address using DNS. 5e. Explain working of the given Remote Login Protocol.	5.1 World Wide Web and HTTP. 5.2 File Transfer : FTP and TFTP. 5.3 Electronic Mail : Architecture Web-Based Mail, Email Security, SMTP, POP, IMAP and MIME, SNMP. 5.4 DNS-Concept of Domain name space, DNS operation. 5.5 DHCP - Static and Dynamic Allocation, DHCP operation. 5.6 Remote Login : TELNET and SSH.

TABLE OF CONTENTS

Unit - I

Unit - II

Unit - III

Unit - IV

Unit - V

UNIT - I

1 NETWORK LAYER AND PROTOCOLS

1.1 IP Addressing

- An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.
- An IP address serves two principal functions : host or network interface identification and location addressing.

1.1.1 Address Space & Notation

- IP corresponds to the network layer in the OSI reference model and provides a connectionless best effort delivery service to the transport layer. An Internet Protocol (IP) address has a fixed length of 32 bits.
- IPv4 addresses are unique. Two devices on the internet can never have the same address at the same time.
- The address structure was originally defined to have a two level hierarchy : Network ID and host ID. The **network ID** identifies the network the host is connected to. The **host ID** identifies the network connection to the host rather than the actual host.

Address Space

- An address space is the total number of addresses used by the protocol. If a protocol uses N bits to define an address, the address space is 2^N because each bit can have two different values and N bits can have 2^N values.
- IPv4 uses 32-bit addresses, which means that the address space is
  2^{32} or 4, 294, 967, 296.
- IP addresses are usually written in **dotted decimal** notation so that they can be communicated conveniently by people. The address is broken into four bytes with each byte being represented by a decimal number and separated by a dot.
- For example, an IP address of
  10000000 10000111 01000100 00000100 is written as 128.135.68.4 in dotted-decimal notation.
  The address 193.32.216.9 in binary notation is
  11000001 00100000 11011000 00001001
- An IP address is a numeric identifier assigned to each machine on an IP network. IP address is a software address, not a hardware address, which is hard-coded in the machine or NIC. An IP address is made up of 32 bits of information. These bits are divided into four parts containing 8 bit each.
- There are three method for depicting an IP address.

1. Dotted-decimal as in 131.57.30.57
2. Binary, as, 10000010.00111001.00011110.00111000
3. Hexadecimal, as in 8B.39.C2.43

- The 32-bit IP address is a structured or hierachical address. The network address uniquely identifies each network. Every machine on the same network shares that network address as part of its IP address. The IP address 131.57.30.57, the 131.57 is the network address and 30.57 is the node address. The node address is assigned to and uniquely identifies, each machine on a network.
- The router might able to speed a packet on its way after reading only the first bits of address. The format used for IP address are shown in Fig. 1.1.1 (b).

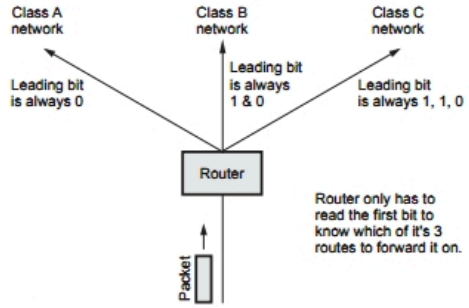


Fig. 1.1.1 (a) Leading bits of a network address

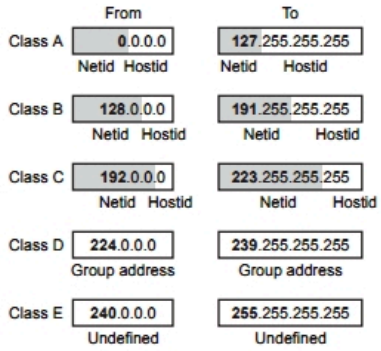


Fig. 1.1.1 (b) Classes range of IP

1.1.2 Classful Addressing

- The IP address structure is divided into five address classes : Class A, Class B, Class C, Class D and Class E, identified by the most significant bits of the addresses.
- Fig. 1.1.2 shows the five classes of IP addresses.
- Class D addresses are used for multicast services that allow a host to send information to a group of hosts simultaneously. Class E addresses are reserved for future use.
- Class A addresses were designed for large organizations with a large number of attached hosts or routers.
- Class B addresses were designed for midsize organizations with tens of thousands of attached hosts or routers.
- One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size.

Class	Number of blocks	Block size
A	128	16777216
B	16384	65536
C	2097152	256
D	1	268435456
E	1	268435456

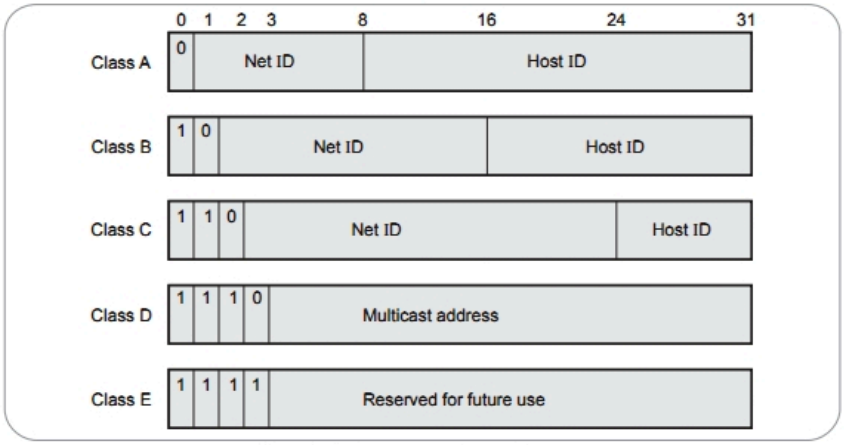


Fig. 1.1.2 Five classes of IP addresses

- In a class A network, the first byte is assigned to the network address and the remaining three bytes used for the node addresses. The class A format is

  Network.Node.Node.Node

  For example : 14.28.101.120 in this IP address 14 is the network address and 28.101.120 is the node address.
- In class B network, the first two bytes are assigned to the network address and the remaining two bytes are used for node addresses. The format is

  Network.Network.Node.Node

  For example : 150.51.30.40 in this IP address network address is 150.51 and node address is 30.40.
- In class C network, the first three bytes are assigned to network address and only one byte is used for node address. The format is

  Network.Network.Network.Node
- **For example :** 200.20.42.120 in this example 200.20.42 is the network address and 120 is the node address.

1.1.3 Classless Addressing

- In classless addressing variable length blocks are assigned that belong to no class. In this, the entire address space is divided into blocks of different sizes. An organization is granted a block suitable for its purposes.
- Fig. 1.1.3 shows the architecture of classless addressing.
- In classless addressing, when an entity, small or large, needs to be connected to the internet it is granted a block of addresses. The size of the block varies based on the nature and size of the entity.

Restriction

- To simplify the handling of addresses, the internet authorities impose three restrictions on classless address blocks.

1. The addresses in a block must be contiguous, one after another.
2. The number of addresses in a block must be a power of 2.
3. The first address must be evenly divisible by the number of addresses.

- In IPv4 addressing, a block of addresses can be defined as x.y.z.t/n in which x.y.z.t defines one of the addresses and the /n define the mask. The address and the /n notation completely define the whole block.
- IPv4 is the delivery mechanism used by the TCP/IP protocols. IPv4 is an unreliable and connectionless datagram protocol.
- IPv4 is also a connectionless protocol for a packet switching network that uses the datagram approach.

1.1.4 Special IP Address

Some IP addresses are reserved for special purposes.

Sr. No.	Special address	Net ID	Host ID
1.	Network address	Specific	All 0
2.	Direct broadcast address	Specific	All 1
3.	Limited broadcast address	All 1s	All 1
4.	This host on this network	All 0s	All 0
5.	Loopback address	127	Any
6.	Specific host on this network	All 0s	Specific

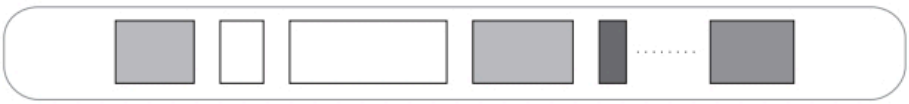


Fig. 1.1.3 Architecture of classless addressing

1.1.5 Network Address Translation

- Within the company, every machine has a unique address of the form 10 X.Y.Z. when a packet leaves the company premises, it passes through the NAT box that convert the internal IP source address 10.0.0.1. NAT box is often combined in a single device with a firewall. It is also possible to integrate the NAT box into the company router.
- Fig. 1.1.4 shows placement of NAT box.
- Whenever an outgoing packet enters the NAT box, the 10.X.Y.Z. SA is replaced by the company true IP address. In, addition, TCP source port field is replaced by an index into the NAT box 65536 entry translation table. This table entry contains the original IP address and original source port. Finally both the IP and TCP header checksums are recomputed and inserted into the packet.
- When process want to establish a TCP connection with a remote process, it attached itself to an unused TCP port on its own machine. This is called a source port and tells the TCP code where to send incoming packets belonging to this connection. The process also supplies a destination port to tell who to give the packet to on the remote side.

Board Questions

1. *Describe different IP address classes.* **MSBTE : Summer-15, Marks 4**
2. *List any four IP functions.* **MSBTE : Summer-15, Marks 4**
3. *Define IP addressing. List IP address classes with their range of addresses.* **MSBTE : Summer-16, Marks 4**
4. *Describe the various IP address classes with suitable examples.* **MSBTE : Winter-16, Marks 4**
5. *State different IP address classes. Explain any one in brief.* **MSBTE : Summer-17, Marks 4**

1.2 Internet Protocol : Datagram Format

- Packets in the IPv4 layer are called datagrams. A datagram is a variable length packet consisting of two parts : Header and data.
- Fig. 1.2.1 shows IPv4 header format

1. **VER** is the field that contains the IP protocol version. The current version is 4.5 is an experimental version. 6 is the version for IPv6.
2. **HLEN** is the length of the IP header in multiples of 32 bits without the data field.The minimum value for a correct header is 5 (i.e. 20 bytes), the maximum value is 15 (i.e., 60 bytes).

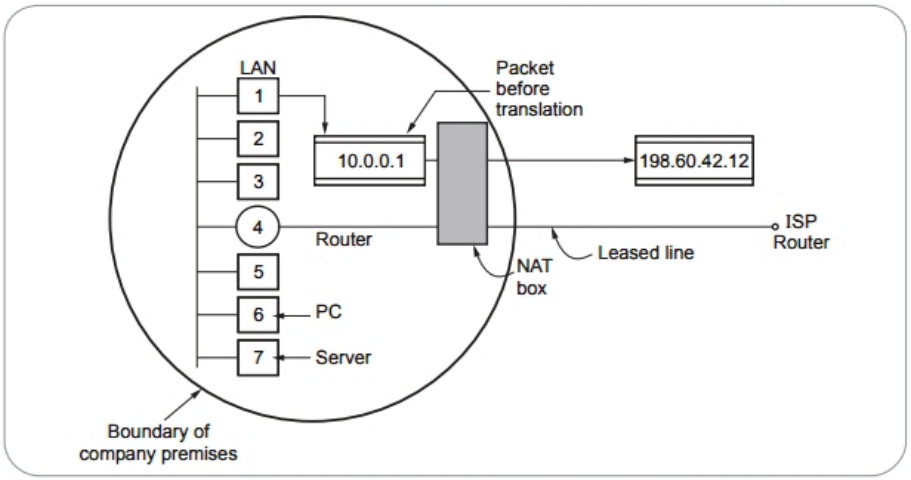


Fig. 1.1.4 NAT

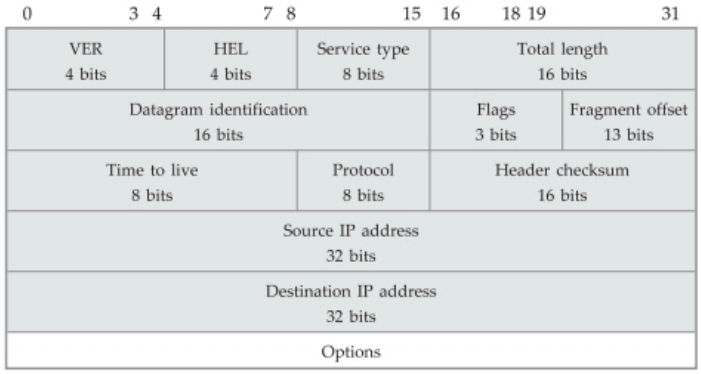


Fig. 1.2.1 IPv4 header format

3. **Service type** The service type is an indication of the quality of service requested for this IP datagram. It contains the following information.

Precedence	Types of service	R

Precedence specifies the nature / priority :

000	Routine
001	Priority
010	Immediate
011	Flash
100	Flash override
101	Critical
110	Internetwork control
111	Internetwork control

TOS specifies the type of service value :

TOS bits	Description
1000	Minimize delay
0100	Maximum throughout
0010	Maximize reliability
0001	Minimize monetary cose
0000	Normal service

The last bit is reserved for future use.

4. **Total length** specifies the total length of the datagram, header and data, in octets.
5. **Identification** is a unique number assigned by the sender used with fragmentation.
6. **Flags** contain control flags :
   a. The first bit is reserved and must be zero;
   b. The 2^{nd} bit is DF (Do not Fragment), 0 means allow fragmentation;
   c. The third is MF (More Fragments), 0 means that this is the last fragment.
7. **Fragment offset** is used to reassemble the full datagram. The value in this field contains the number of 64-bit segments (header bytes are not counted) contained in earlier fragments. If this is the first (or only) fragment, this field contains a value of zero.
8. **TTL** (Time To Live) specifies the time (in seconds) the datagram is allowed to travel. In practice, this is used as a hop counter to detect routing loops.
9. **Protocol number** indicates the higher level protocol to which IP should deliver the data in this datagram. E.g., ICMP = 1; TCP = 6; UDP = 17.
10. **Header checksum** is a checksum for the information contained in the header. If the header checksum does not match the contents, the datagram is discarded.

11. **Source/Destination IP addresses** are the 32-bit source/destination IP addresses.
12. **IP options** is a variable-length field (there may be zero or more options) used for control or debugging and measurement. For instance :
    a. The **loose source routing** option provide a means for the source of an IP datagram to supply explicit routing information;
    b. The **timestamp** option tell the routers along the route to put timestamps in the option data.
13. **Padding** is used to ensure that the IP header ends on a 32 bit boundary. The padding is zero.

1.2.1 Fragmentation

- IP provides fragmentation/reassembly of datagrams. The maximum length of an IP datagram is 65,535 octets. When an IP datagram travels from one host to another, it may pass through different physical networks. Each physical network has a maximum frame size, called Maximum Transmission Unit (MTU), which limits the datagram length.
- A fragment is treated as a normal IP datagram while being transported to their destination. Thus, fragments of a datagram each have a header. If one of the fragments gets lost, the complete datagram is considered lost. It is possible that fragments of the same IP datagram reach the destination host via multiple routes. Finally, since they may pass through networks with a smaller MTU than the sender's one, they are subject to further fragmentation. Fig. 1.2.2 shows the MTU.

Fragmentation process

- The DF flag bit is checked to see if fragmentation is allowed. If the bit is set, the datagram will be discarded and an ICMP error returned to the originator.
- Based on the MTU value, the data field is split into two or more parts. All newly created data portions must have a length that is a multiple of 8 octets, with the exception of the last data portion. Each data portion is placed in an IP datagram.
- Fig. 1.2.3 shows the examples of fragmentation.

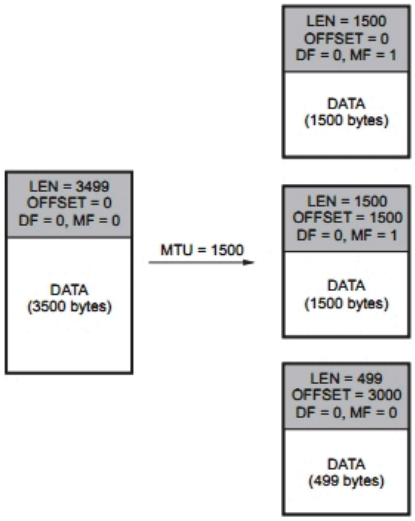


Fig. 1.2.3 Examples of fragmentation

- Modification to the headers of fragments :
    a. The MF flag is set in all fragments except the last;
    b. The fragment offset field is updated;

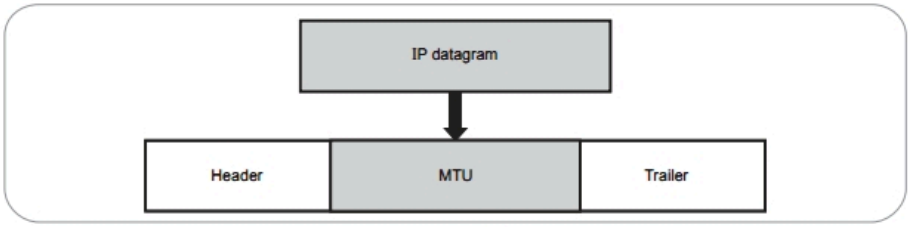


Fig. 1.2.2 MTU

c. If options were included in the original datagram, they may be copied to all fragment datagram's or only the first datagram (depends on the option);

d. The header length field is set;

e. The total length field is set;

f. The header checksum is re-calculated.

- At the destination host, data are reassembled into the original datagram. The identification field set by the sending host is used together with the source and destination IP addresses in the datagram. Fragmentation does not alter this field.
- In order to reassemble the fragments, the receiving host allocates a storage buffer when the first fragment arrives. The host also starts a timer. If the timer is exceeded and fragments remain outstanding, the datagram is discarded. When subsequent fragments of the datagram arrive, data are copied into the buffer storage at the location indicated by the fragment offset field. When all fragments have arrived, the original unfragmented datagram is restored and passed to upper layers, if needed.

Problem in fragmentation

1. The end node has no way of knowing how many fragments there be. The end node has to manage enough buffer space to handle reassembly process.
2. If any fragments lost, all datagram must be discarded.
3. End node starts a timer when received the first fragment, if any fragments fails to arrive (usually 30 secs), all datagram's must be discarded.
4. Since the IP service is connectionless. No attempt is made by IP to recover these situations, through ICMP error message may be generated.

1.2.2 Options

- The header of the IPv4 datagram is made of two parts : A fixed part and a variable part. Options used in IPv4 are as follows

1) Single byte : No opeation and end of operation

2) Multiple byte : Record route, strict source route, loose source route and timestamp

1. **No operation** option is 1-byte option used as a filter between options.
2. **End of option** is a 1-byte option used for padding at the end of the option field.
3. Record route option is used to record the internet routers that handle the datagram. It can list upto nine router addresses. It can be used for debugging and management purposes.
4. Strict source route option is used by the source to predetermine a route for the datagram as it travels through the Internet.
5. Loose source route option is similar to the strict source route, but it is less rigid. Each router in the list must be visited, but the datagram can visit other routers as well.
6. Timestamp option is used to record the time of datagram processing by a router.

1.2.3 Subnetting

- If a organization is large or if its computers are geographically dispersed, it makes good sense to divide network into smaller ones, connected together by routers. The benefits for doing things this way include.
    1. Reduced network traffic
    2. Optimized network performance
    3. Simplified network management
    4. Facilities spanning large geographical distances.
- If Network Information Center (NIC) assign only one network address to an organization which having multiple network, that organization has a problem. A single network address can be used to refer to multiple physical networks. An organization can request individual network **address** for each one of its physical networks. If these were granted, there wouldn't be enough to go around for everyone.
- Another problem is, if each router on the internet needed to know about each existing physical network, routing tables would be impossibly huge. This is physical overhead on the router. To solve this type of problem, the subnet addressing method is used.

- To allow a single network address to span multiple physical networks is called **subnet addressing** or **subnet routing** or **subnetting**. Subnetting is a required part of IP addressing.
- To understand subnet addressing, consider the next example. Consider the site has a single class B IP network address assigned to it, but the organization has two or more physical networks. Only local routers know that there are multiple physical networks and how to route traffic among them.
- In the example, the organization is using the single class B network address for two networks. For the subnet address scheme to work, every machine on the network must know which part of the host address will be used as the subnet address. This is accomplished by assigning each machine a subnet mask.

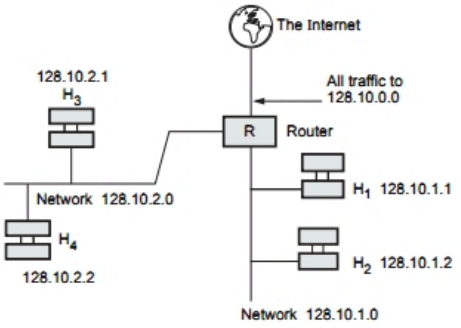


Fig. 1.2.4 Multiple network

- The network administrator creates a 32-bit subnet mask comprised of ones and zeros. The ones in the subnet mask represent the positions that refer to the network or subnet addresses. The zeros represent the positions that refer to the host part of the address. Class B address format is Net.Net.Node.Node. The third byte, normally assigned as part of the host address is now used to represent the subnet address. Hence, these bit positions are represented with ones in the subnet mask. The fourth byte is the only part in example that represents the unique host address.

Subnet mask code

1 = Positions representing network or subnet addresses.

0 = Positions representing the host address.

Subnet mask format

$$\underbrace{1111\ \ 1111.\ \ 1111\ \ 1111}_{\text{Network address positions}}\ \ \underbrace{1111\ \ 1111.}_{\text{Subnet positions}}\ \ \underbrace{0000\ \ 0000}_{\text{Host positions}}$$

The subnet mask can also be denoted using the decimal equivalents of the binary patterns. The default subnet masks for the different classes of networks are as below in Table 1.2.1.

Class	Format	Defult subnet mask
A	Net.Node.Node.Node	255.0.0.0
B	Net.Net.Node.Node	255.255.0.0
C	Net.Net.Net.Node	255.255.255.0

Table 1.2.1 Default subnet mask of IP address

Masking

- A process that extracts the address of the physical network from an IP address is called Masking. If we done the subnetting, then masking extracts the subnetwork address from an IP address.
- To find the subnetwork address, two method are used. There are boundary level masking and non-boundary level masking, we take one by one.
- In boundary level masking, two masking numbers are consider (i.e. 0 or 255). In non-boundary level masking other value of masking is used Apart from 0 and 255.

A. Rules for boundary level masking

1. In this mask number is either 0 or 255.
2. If the mask number is 255 in the mask IP address, then the IP address is repeated in subnetwork address.
3. If the mask number is 0(zero) in the mask IP address, then the 0 is repeated in subnetwork address.

B. Rules for non-boundary level masking

1. In this mask numbers are not 0 or 255 mask number is greater than 0 or less than 255.

2. If the mask number is 255 in the mask IP address, then the original IP address (byte) is repeated in subnetwork address.
3. If the mask number is 0 in the mask IP address, then the 0 is repeated in the subnetwork address.
4. For any other mask numbers, bit-wise AND operator is used. Bit-wise ANDing is done in between mask number (byte) and IP address (byte).

- The first address in the block is used to identify the organization to rest of the Internet. This address is called the **network address.**

1. How many subnets ?

- Number of subnet is calculated as follows :

Number of subnet = 2^x

where x is the number of masked bits or the 1s (ones).

For example 11100000, the number of 1s gives us 2^3 subnets. In this example there are 8 subnets.

2. How many host per subnet ?

Number of host per subnet = $2^y - 2$

Where y is the number of unmasked bits or the 0s (zeros).

For example 11100000, the number of 0s gives us $2^5 - 2$ hosts. In this example there are 30 hosts per subnet. You need to subtract 2 for subnet address and the broadcast address.

3. What are the valid subnets ?

For valid subnet = 256 – Subnet mask = Block size. An example would be

256 – 224 = 32. The block size of a 224 mask is always 32.

Start counting at zero in block of 32 until you reach the subnet mask value and these are your subnets. 0, 32, 64, 96, 128, 160, 192, 224.

4. What is the broadcast address for each subnet ?

Our subnets are 0, 32, 64, 96, 128, 160, 192, 224, the broadcast address is always the number right before the next subnet. For example, the subnet 0 has a broadcast address of 31 because next subnet is 32. the subnet 32 has a broadcast address of 63 because next subnet is 64.

5. What are the valid hosts ?

Valid hosts are the numbers between the subnets, omitting the all 0s and all 1s. For example, if 32 is the subnet number and 63 is the broadcast address, then 32 to 63 is the valid host range. It is always between the subnet address and the broadcast address.

Ex. 1.2.1 *What is the sub-network address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0 ?*

Sol. : Using AND operation, we can find sub-network address.

1. Convert the given destination address into binary format :

200.45.34.56 => 11001000 00101101 00100010 00111000

2. Convert the given subnet mask address into binary format :

255.255.240.0 => 11111111 11111111 11110000 00000000

3. Do the AND operation using destination address and subnet mask address.

200.45.34.56 => 11001000 00101101 00100010 00111000

255.255.240.0=> 11111111 11111111 11110000 00000000

11001000 00101101 00100000 00000000

Subnetwork address is 200.45.32.0

Ex. 1.2.2 *For a network address 192.168.10.0 and subnet mask 255.255.255.224 then calculate :*
i) Number of subnet and number of host
ii) Valid subnet

Sol. : Given network address 192.168.10.0 is class C address. Subnet mask address is 255.255.255.224. Here three bits is browse for subnet.

i) Number of subnet and number of host :

255.255.255.224 convert into binary => 11111111 11111111 11111111 11100000

Number of subnet = $2^x = 2^3 = 8$

So there are 8 subnet.

Number of host per subnet = $2^y - 2 = 2^5 - 2 = 30$

ii) Valid subnets :

For valid subnet = 256 – Subnet mask = Block size. An example would be 256 – 224 = 32. The block size of a 224 mask is always 32.

Start counting at zero in block of 32 until you reach the subnet mask value and these are your subnets. 0, 32, 64, 96, 128, 160, 192, 224.

Ex 1.2.3 *Find the sub-network address for the following :*

Sr. No.	*IP address*	*Mask*
a)	*140.11.36.22*	*255.255.255.0*
b)	*120.14.22.16*	*255.255.128.0*

Sol. :

a) IP address Mask

140.11.36.22 255.255.255.0

The values of mask (i.e. 255.255.255.0) is boundary-level. So

IP address	140.11.36.22
Mask	255.255.255.0
	140.11.36.0

b) IP address 120.14.22.16

Mask 255.255.128.0

The byte 1, byte 2 and byte 4 is boundary values and byte 3 is non-boundary value.

Ex. 1.2.4 *Find the sub-network address for the following.*

Sr. No.	*IP address*	*Mask*
a)	*141.181.14.16*	*255.255.224.0*
b)	*200.34.22.156*	*255.255.255.240*
c)	*125.35.12.57*	*255.255.0.0*

Sol. :

a)

141.181.14.16	IP address
255.255.224.0	Mask
141.181.0.0	Sub-network address

b)

200.34.22.156	IP address
255.255.255.240	Mask
200.34.22.144	Sub-network address

c)

125.35.12.57	IP address
255.255.0.0	Mask
125.35.0.0	Sub-network address

(i.e. 128) So for byte-3 value use bit-wise AND operator. It is shown below.

120.14.22.16	IP address
255.255.128.0	Mask
120.14.0.0	Sub-network address

In the above example, the bit wise ANDing is done in between 22 and 128. it is as follows

22	Binary representation	0 0 0 1 0 1 1 0
128	Binary representation	1 0 0 0 0 0 0 0
0		0 0 0 0 0 0 0 0

Thus the sub-network address for this is 120.14.0.0.

Ex. 1.2.5 *Find the class of the following address.*
a) 1.22.200.10 b) 241.240.200.2
c) 227.3.6.8 d) 180.170.0.2

Sol. :

a) 1.22.200.10	Class A IP address
b) 241.240.200.2	Class E IP address
c) 227.3.6.8	Class D IP address
d) 180.170.0.2	Class B IP address

Ex. 1.2.6 *Find the netid and Hostid for the following.*
a) 19.34.21.5 b) 190.13.70.10 c) 246.3.4.10 d) 201.2.4.2

Sol. :

a) netid ⇒ 19 Hostid ⇒ 13.70.10

b) netid ⇒ 190.13 Hostid ⇒ 70.10

c) No netid and No Hostid because 246.3.4.10 is the class E address.

d) netid ⇒ 201.2.4 Hostid ⇒ 2

Ex. 1.2.7 *Consider sending a 3500 - byte datagram that has arrived at a router R_1 that needs to be sent over a link that has an MTU size of 1000 bytes to R_2. Then it has to traverse a link with an MTU of 600 bytes. Let the identification number of the original datagram be 465. How many fragments are delivered at the destination ? Show the parameters associated with each of these fragments.*

Sol. : The maximum size of data field in each fragment = 680 (because there are 20 bytes IP header). Thus the number of required fragments) = [3500 – 20/680] = 5.11 = 6

Each fragment will have Identification number 465. Each fragment except the last one will be of size 700 bytes (including IP header). The last datagram will be of size 360 bytes (including IP header). The offsets of the 4 fragments will be 0, 85, 170, 255. Each of the first 3 fragments will have flag=1; the last fragment will have flag=0.

1.2.4 Limitation of IPv4

- The lack of address space
- Lack of quality of service support
- Weak protocol extensibility - the insufficient size of the IPv4 header, which does not accommodate the required number of additional parameters;
- Lack of end-to-end connectivity
- The problem of security of communications - no means are provided to limit access to information hosted on the network. IPv4 has never been designed for security.

Board Questions

2. *State meaning of (i) Subnetting (ii) Supernetting with suitable examples.* **MSBTE : Summer-16, Marks 4**
2. *Explain the terms :*
   i) Subnetting ii) Supernetting iii) Masking
   iv) Classless IP addressing with suitable examples. **MSBTE : Winter-16, Marks 4**
3. *Explain subnet masking.* **MSBTE : Summer-17, Winter-17, Marks 4**
4. *Explain structure of IP frame header.* **MSBTE : Winter-17, 18, Marks 4**
5. *Describe the various IP address classes with suitable example.* **MSBTE : Summer-18, Marks 4**
6. *Explain registered and unregistered IP address.* **MSBTE : Summer-18, Marks 4**

1.3 ICMPv4

- There are some situations in which IP cannot deliver the packet to the destination host. For instance, this happens if the packet's TTL has expired, if the route to the specified destination address is missing from the routing table, if the gateway does not have sufficient buffer space for passing specific packet.
- It was noted earlier that if a router could not forward a packet for some reasons, the router would send an error message back ot the source to report the problem. The **Internet Control Message Protocol (ICMP)** is the protocol that handles error and other control messages.
- ICMP itself is a network layer protocol. However, its messages are not passed directly to the data link layer as would be expected. Although ICMP messages are encapsulated by IP packets.

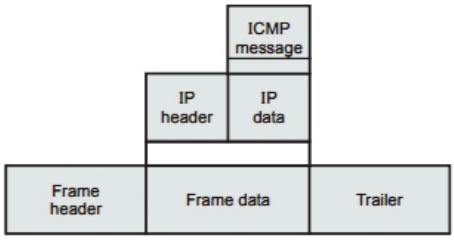


Fig. 1.3.1 ICMP encapsulation

- Fig. 1.3.1 shows an ICMP encapsulation.
- The value of the protocol field in the IP datagram is 1 to indicate that the IP data is an ICMP message.

1.3.1 Messages

- All ICMP messages fall in the following classes :
  1. Error reporting 2. Query.

- The error reporting messages report problems that a router or a host may encounter when it processes an IP packet.
- The query messages, which occurs in pairs, help a host or a network manager get specific information from a router or another host.
- ICMP used by both hosts and gateway for a variety of functions, and especially by network management. The main functions associated with the ICMP are as follows :

1. Error reporting
2. Reachability testing
3. Congestion control
4. Route change notification
5. Performance measuring
6. Subnet addressing.

- ICMP is used for error messages such as occur when something is detectably wrong with the packet format, with the selection of a router or with the condition of some intermediate node in the internet. Such abnormal conditions are reported to the source of the datagram for possible **remedial** action.
- For example, if user attempt to connect to a host, the user's system may get back an ICMP message saying "host unreachable". ICMP can also be used to find out some information about the network.
- ICMP is similar to UDP in that it handles messages that fit in one datagram. It is simpler than UDP. It does not even have port numbers in the header. Since all ICMP messages are interpreted by the network software itself, no port number is needed to say where an ICMP message is supported to go. ICMP also provides a way for new nodes to discover the subnet mask currently used in an internetwork. So ICMP is an integral part of any IP implementation, particularly those that run in routers.
- The ICMP TYPE field defines the meaning of the message as well as its format. The type include

Type field	ICMP message type
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect
8	Echo request
11	Time exceeded
12	Parameter problem
13	Timestamp request
14	Timestamp replay
15	Information request
16	Information replay
17	Address mask request
18	Address mask reply

- ICMP messages meaning is as follows.
  1. Echo reply means the device in the network is alive.
  2. Destination unreachable means packet is not delivered to the destination. Router cannot find the destination.
  3. Source quench message is used when host send too many packet i.e. choke packet.
  4. Time exceeded is used when time to live field hits to zero. Life time of datagram expires this type is used.
  5. Time stamp and timestamp-reply message provides a mechanism for sampling the delay characteristics of the Internet. Same as echo reply and echo request but with time limit.
  6. Parameter problem message is used by ICMP if the header field is valid.

Message Format

- Fig. 1.3.2 shows the basic error message format. An ICMP message is encapsulated into the data field of an IP packet. An ICMP header is 8 bytes long and a variable size data section.

1. **Type :** It is 8 bits field identifies the type of the message.
2. **Code :** Size of the code field is 8 bits. It provides the information or parameters of the message type.
3. **Checksum :** This 16-bit field is used to detect errors in the ICMP message.

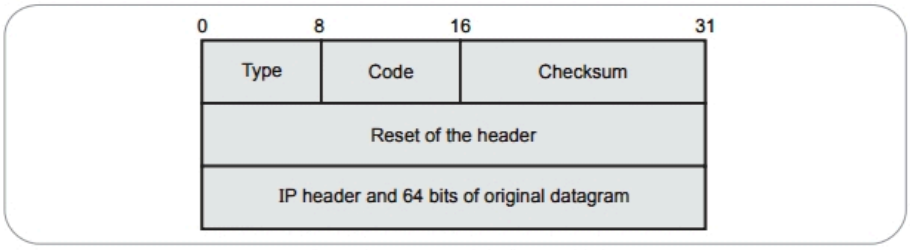


Fig. 1.3.2 ICMP error message format

4. IP header plus original datagram : This field can be used for diagnostic purposes by matching the information in the ICMP message with the original data in the IP packet.

1.3.2 Debugging Tools

1. Ping

- Ping stands for "Packet INternet Groper."
- An Internet utility used to determine whether a particular IP address is reachable online by sending out a packet and waiting for a response.
- Ping is used to test and debug a network as well as see if a user or server is online.
- Ping sends ICMP ECHO_REQUEST packets to any network addressable host (i.e. a server, a gateway router, etc.). The piece of equipment must be IP (Internet Protocol) addressable in order for ping to work
- Ping is useful for determining whether a host is up and running on the network. Ping returns information regarding the hosts response to the ICMP ECHO_REQUEST packets.
- The source host sends ICMP echo-request messages; the destination, if alive, responds with ICMP echo-reply messages.
- The ping program sets the identifier field in the echo-request and echo-reply message and starts the sequence number from 0; this number is incremented by 1 each time a new message is sent.
- Syntax :

```
$ ping  hostname
   OR
$ ping   xx.xx.xx.xx
```

- The ping command first sends an echo request packet to an address, then waits for a reply. The ping is successful only if :

a. the echo request gets to the destination, and

b. the destination is able to get an echo reply back to the source within a predetermined time called a timeout.

- The TTL value of a ping packet cannot be changed.

2. Traceroute

- The traceroute program in UNIX or tracert in Windows can be used to trace the route of a packet from the source to the destination
- The traceroute command is used to discover the routes that packets actually take when traveling to their destination.
- The device sends out a sequence of UDP datagrams to an invalid port address at the remote host.
- Three datagrams are sent, each with a Time-To-Live (TTL) field value set to one. The TTL value of 1 causes the datagram to "timeout" as soon as it hits the first host1 in the path; this host1 then responds with an ICMP Time Exceeded Message (TEM) indicating that the datagram has expired.
- Another three UDP messages are now sent, each with the TTL value set to 2, which causes the second host2 to return ICMP TEMs. This process continues until the packets actually reach the other destination.
- Since these datagrams are trying to access an invalid port at the destination host, ICMP Port Unreachable Messages are returned, indicating an unreachable port; this event signals the Traceroute program that it is finished.

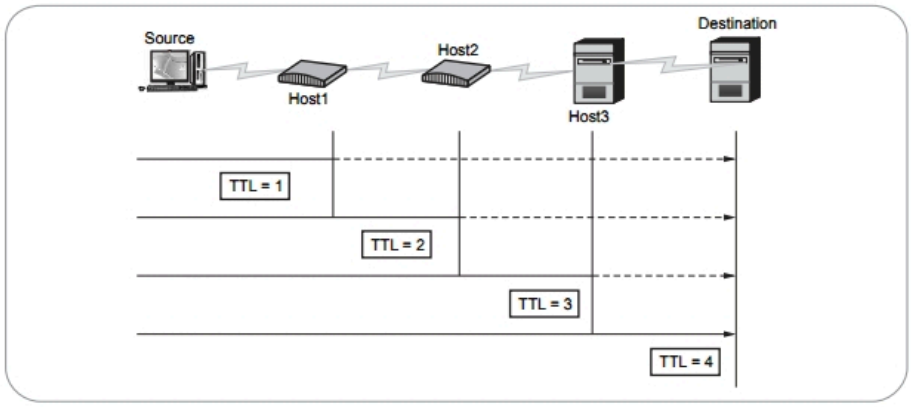


Fig. 1.3.3 Traceroute with TTL value

- Syntax :

$ traceroute technicalpublications.org

1.3.3 ICMP Checksum

- In ICMP the checksum is calculated over the entire message i.e. header and data.
- Checksum calculation at sender side using one's complement.

a. Checksum field is set to zero

b. Sum of all 16-bit words is calculated.

c. Sum is complemented to get the checksum

d. Checksum is stored in the checksum field.

- Receiver performs following steps

a. Sum of all words is calculated

b. Sum is complemented

c. If the result obtained in step 2 is 16 zeros(0), the message is accepted; otherwise it is rejected.

1.4 Mobile IP

- Mobile IP is an open standard, defined by the Internet Engineering Task Force (IETF), that allows users to keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP networks
- Mobile IP in wireless networks is intended to be a direct extension of the existing fixed/wire line networks with uniform end - to - end QoS guarantees.

Components of a Mobile IP Network

- Mobile IP has the following three components : Mobile Node, Home Agent and Foreign Agent
- Fig. 1.4.1 shows components of mobile IP network.
- The Mobile node is a device such as a cell phone, personal digital assistant, or laptop whose software enables network roaming capabilities.
- The Home Agent is a router on the home network serving as the anchor point for communication with the Mobile Node.
- The Foreign Agent is a router that may function as the point of attachment for the Mobile Node when it roams to a foreign network, delivering packets from the Home Agent to the Mobile Node.

1.4.1 Addressing

- The Mobile device have two addresses as well :

1. Home Address : The "normal", permanent IP address assigned to the mobile node. This is the address used by the device on its home network, and the one to which datagrams intended for the mobile node are always sent.
2. Care-Of Address : A secondary, temporary address used by a mobile node while it is 'traveling" away from its home network. It is a normal 32-bit IP address in most respects, but is used only by Mobile IP for forwarding IP datagrams and for administrative functions. Higher layers never use it, nor do regular IP devices when creating datagrams.

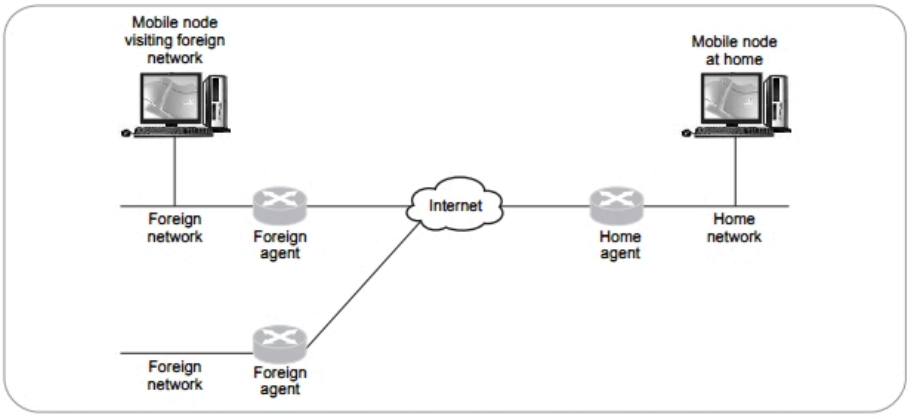


Fig. 1.4.1 Components of mobile IP network

Mobile IP Care-Of Address Types

- There are two different types, which correspond to two distinctly different methods of forwarding datagrams from the home agent router.

1. Foreign Agent Care-Of Address :

- This is a care-of address provided by a foreign agent in its Agent Advertisement message. It is the IP address of the foreign agent itself.
- When this type of care-of address is used, all datagrams captured by the home agent are not relayed directly to the mobile node, but indirectly to the foreign agent, which is responsible for final delivery.
- Since in this arrangement the mobile node has no distinct IP address valid on the foreign network, this is typically done using a layer two technology.

2. Co-Located Care-Of Address :

- This is a care-of address assigned directly to the mobile node using some means external to Mobile IP.
- For example, it may be assigned on the foreign network manually, or automatically using DHCP.
- In this situation, the care-of address is used to forward traffic from the home agent directly to the mobile node.
- When mobile host visits a foreign network, it receives its care of address during the agent discovery and registration phase.

1.4.2 Agents

- Mobile IP uses two types of agents : home agent and foreign agent

1. Home agent : Home agent is a router on a mobile node's home network that maintains information about the device's current location, as identified in its care-of address.

- The home agent uses tunneling mechanisms to forward Internet traffic so that the device's IP address doesn't have to be changed each time it connects from a different location.
- A home agent may work in conjunction with a foreign agent, which is a router on the visited network.

2. Foreign Agent : Foreign agent is usually a router attached to the foreign network. Foreign agent receives and delivers packets sent by the home agent to the mobile host

- Foreign Agent care-of address is an IP address of a Foreign Agent that has an interface on the foreign network being visited by a Mobile Node

1.4.3 Three Phases

- Three phases are as follows :

1. Agent Discovery : A mobile node uses a discovery procedure to identify home agents and foreign agents.

- Mobile uses a discovery procedure to identify home agents and foreign agents. Agents periodically send out ICMP router advertisements with mobile agent advertisement extensions.
- Mobile nodes can use ICMP router solicitation to get agent information immediately.

2. Registration : A mobile node uses an authenticated registration procedure to inform its home agent of its care-of address.

- Registration involves four steps :

a. The mobile node requests the forwarding service by sending a registration request to the foreign agent that the mobile node wants to use

b. The foreign agent relays the request to the mobile node's home agent

c. The home agent either accepts or denies the request and sends a registration reply to the foreign agent

d. The foreign agent relays the reply to the mobile node

- Co-located care-of address : Mobile sends registration directly to Home Agent
- Registration involves authentication : Mobile nodes typically wireless - subject to eavesdropping and active attacks
- Fig. 1.4.2 shows registration request and reply.

3. Data transfer : Tunneling is used to forward IP-datagrams from a home address to a care-of address

1.4.4 Inefficieny in Mobile IP

- Communication using mobile IP can be inefficient. The inefficiency can be severe or moderate. The severe case is called double crossing or 2X. The moderate case is called triangle routing or dog-leg routing.

1. Double crossing

- When a remote host communicates with a mobile host that has moved to the same network as the remote host then double crossing occurs.
- In local communication, mobile host sends a packet to remote host. In this case, there is no inefficiency. But when remote host sends a packet to the mobile host, the packet crosses the Internet twice.
- When the mobile host sends a packet to the remote host, there is no inefficiency; the communication is local. However, when the remote host sends a packet to the mobile host, the packet crosses the Internet twice.
- Fig. 1.4.3 shows double crossing.

2. Triangle routing

- It occurs when the remote host communicates with a mobile host that is not attached to the same network as the mobile host.
- When the mobile host sends a packet to the remote host, there is no inefficiency. However, when the remote host sends a packet to the mobile host, the

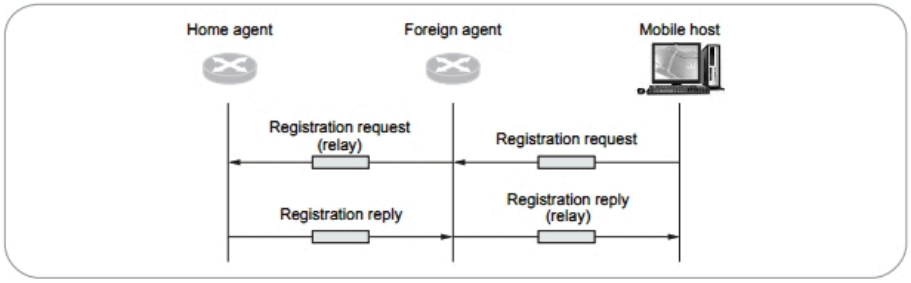


Fig. 1.4.2 Registration request and reply

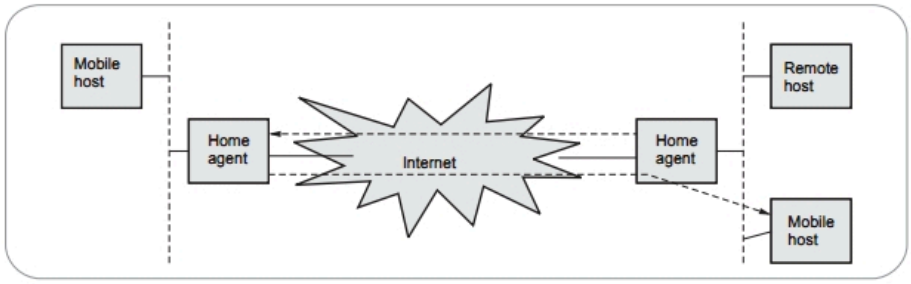


Fig. 1.4.3 Double crossing

packet goes from the remote host to the home agent and then to the mobile host.

Solution

- The remote host is to bind the care-of address to the home address of a mobile host.
- For example, when a home agent receives the first packet for a mobile host, it forwards the packet to the foreign agent; it could also send an update binding packet to the remote host so that future packets to this host could be sent to the care-of address. The remote host can keep this information in a cache.
- The problem with this strategy is that the cache entry becomes outdated once the mobile host moves. In this case the home agent needs to send a warning packet to the remote host to inform it of the change.

1.5 Virtual Private Network

Need of VPN

- A low cost and reliable network to connect networks that are located at different places. VPN is most suitable for such requirements.
- VPN uses public network (Internet) for connecting remotely located networks. Therefore the data communication is possible at cheaper cost and easily available.

VPN Architecture

- Generalized architecture of VPN is shown in Fig. 1.5.1.

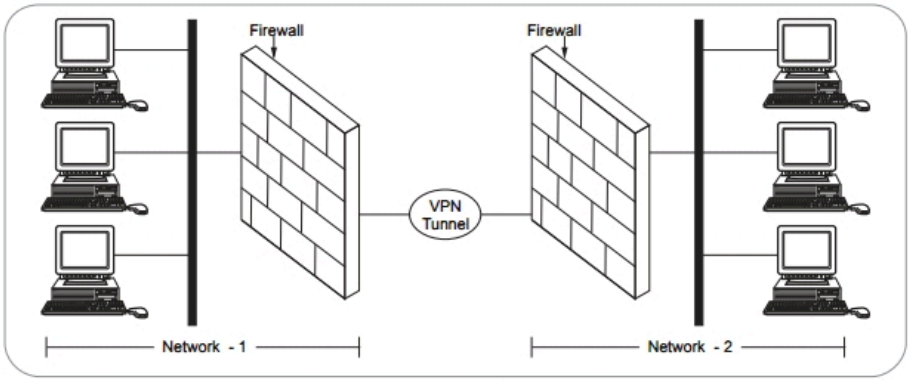


Fig. 1.5.1 VPN architecture

- Virtual Private Network (VPN) based on IPSec protocol are widely used for providing secure encrypted communication over insecure network, such as the internet.
- VPN can be implemented on the top of ATM.
- Authentication in IPSec is handled by the Internet Key Exchange (IKE) protocol.
- Virtual Private Network is a restricted to use logical computer network that is constructed from the system resources of a public and physical network such as the Internet, by using encryption.
- VPN technology is based on a tunneling strategy. Tunneling involves encapsulating packets constructed in a base protocol format within some other protocol.
- In the case of VPNs running over the Internet, packets in one of several VPN protocol formats are encapsulated within IP packets.
- Following network protocols have become popular as a result of VPN developments : PPTP, L2F, L2TP, IPsec, SOCKS etc.
- Authentication allows VPN clients and servers to correctly establish the identity of people on the network.
- Encryption allows potentially sensitive data to be hidden from the general public.

Advantages of VPNs

1. **Cost reduction :** VPNs are cost effective as compared to private networks.
2. **Scalability :** Increase in scalability as they allow more user to be added to the network and also flexible methods of accessing the network, such as ATM, ISDN, DSL and Wireless technologies.
3. **Utilize the backbone for connectivity purpose :** This situation helps to simplify the network topologies considerably, and leads in reducing the burden on management.

Disadvantages of VPNs

1. VPNs require an in-depth understanding of public network security issues and proper deployment of precautions.
2. The availability and performance of an organization's wide-area VPN depends on factors largely outside of their control.
3. VPN technologies from different vendors may not work well together due to immature standards.
4. VPNs need to accommodate protocols other than IP and existing internal network technology.

1.5.1 Tunneling

1) To send IP packet from host A to host B, the packet contains IP address of host B.
2) Then the packet is transmitted from host A.
3) When packet reaches to the router R_1 it removes IP packet.

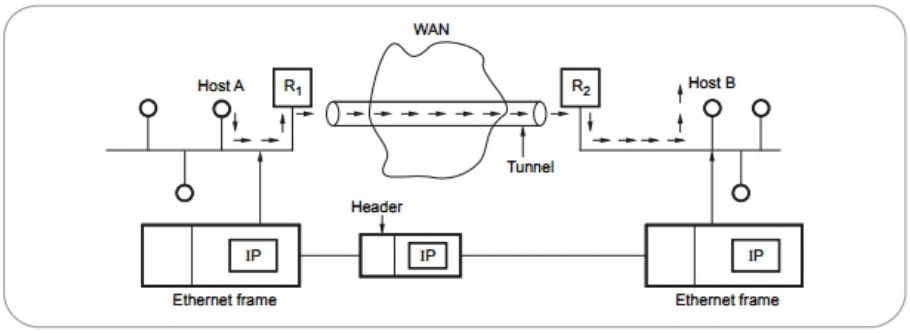


Fig. 1.5.2 Tunneling

4) Router R_1 insert the pay load field of the WAN network layer packet. After inserting payload field it send to Router R_2.

5) When Router R_2 gets the packet, it removes IP packet and send it to host B inside an Ethernet frame.

Fig. 1.5.2 shows tunneling a packet.

1.5.2 Tunneling Protocols

- Various tunneling protocols are developed for VPN. Important types of tunneling protocols are -

1. Point-to-Point Tunneling Protocol (PPTP)
2. Layer 2 Tunneling Protocol (L2TP)
3. IP Security (IPSec)

1.5.2.1 Point-to-Point Tunneling Protocol (PPTP)

- PPTP provides connectivity between single user and a LAN. It does not connects two LAN directly.
- PPTP is designed to work with windows NT system.
- Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across TCP/IP-based data networks. PPTP supports on-demand, multiprotocol, virtual private networking over public networks, such as the Internet.
- Point-to-Point Tunneling Protocol (PPTP) can also be used to tunnel a PPP session over an IP network. In this configuration the PPTP tunnel and the PPP session runs between the same two machines with the caller acting as a PNS. PPTP uses client-server architecture to decouple functions which exist in current Network Access Servers and support Virtual Private Networks. PPTP specifies a call-control and management protocol which allows the server to control access for dial-in circuit switched calls originating from a PSTN or ISDN, or to initiate outbound circuit switched connections.
- It is implemented only by the PAC and PNS. No other systems need to be aware of PPTP. Dial networks may be connected to a PAC without being aware of PPTP. Standard PPP client software should continue to operate on tunneled PPP links.
- PTP uses an extended version of GRE to carry user PPP packets. These enhancements allow for low-level congestion and flow control to be provided on the tunnels used to carry user data between PAC and PNS. This mechanism allows for efficient use of the bandwidth available for the tunnels and avoids unnecessary retransmissions and buffer overruns. PPTP does not dictate the particular algorithms to be used for this low level control but it does define the parameters that must be communicated in order to allow such algorithms to work.

1.5.2.2 Layer 2 Tunneling Protocol (L2TP)

- L2TP is developed by Internet Engineering Task Force (IETF). It is an improved version of PPTP.
- L2TP known as the secure open standard for VPN connections. It can support user-to-LAN connectivity as well as LAN-to-LAN connectivity.

1.6 Two Marks Questions with Answers

Q.1 *Identify the class/speciality of the following IP addresses :*
a) 110.34.56.45 *b) 127.1.1.1*
c) 212.208.63.23 *d) 255.255.255.255*

Ans. :

a) 110.34.56.45 - Class A

b) 127.1.1.1 - Loop back address

c) 212.208.63.23 - Class C

d) 255.255.255.255 - Broadcast address.

Q.2 *What is the network address ?*

Ans. : When an organization is given a block of addresses, the organization is free to allocate. The addresses to the devices that need to be connected to the Internet. The first address in the class is normally treated as a special address. The first address is called the **network address** and defines the organization network.

Q.3 *Define subnetting.*

Ans. : Subnetting is a technique that allows a network administrator to divide one physical network into smaller logical networks and thus,

control the flow of traffic for security or efficiency reasons.

Q.4 *How does one know where a fragment fits within the original datagram ?*

Ans. : The offset field serves this purpose. When a gateway fragments a datagram, it sets the offset field of each fragment to reflect, at what offset with respect to the original datagram the current fragment belongs.

Q.5 *What are the problems arising with NAT ? Name two of them.*

Ans. : The main problem is the violation of the end-to-end principle. Since the network address might change (due to NAT) some applications, especially P2P or VoIP ones, must take this into consideration. Furthermore, routers should not touch anything above layer 3.

Q.6 *Why is the IP header checksum recalculated at every router ?*

Ans. : The IP header checksum is recalculated at every router because some of the IP header fields will change, such as the TTL and (if fragmentation occurs) total length, MF flag, and fragment offset.

Q.7 *Why are IP addresses hierarchical with netid and hostid ?*

Ans. : IP address are hierarchical to reduce the size of routing tables. IP packets are routed only by netid until they reach their destination network where ARP is then used to resolve hostid to MAC address.

Q.8 *What is the time to live field in IP header ?*

Ans. : Time to live field is counter used to limit packet lifetimes. Counts in second and default value is 255 sec.

Q.9 *What is IP addressing ?*

Ans. : An **IP address** is a numerical label assigned to each device in a computer network that uses Internet protocol for communication.

Two important functions at IP address :

1) Host identification

2) Location addressing.

Q.10 *Find the class of each address*
a) 00000001 00001011 00001011 11101111
b) 14.23.120.8

Ans. : a) The first bit is 0. This is a class A address.

b) The first byte is 14 (between 0 and 127). This is a class A address.

Q.11 *What is the need of subnetting ?*

Ans. : Subnetting divides one large network into several smaller ones. Subnetting adds an intermediate level of hierarchy in IP addressing.

Q.12 *What is fragmentation and reassembly*

Ans. : IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. Large datagram are fragmented (divided) i.e. one datagram becomes several datagram of small sizes. This process is called **fragmentation**. At final destination the datagrams are **reassembled** with the help of IP header bits.

Q.13 *Expand ICMP and write the function.*

Ans. : ICMP stands for internet control message control.

Functions of ICMP :

1) Error reporting 2) Rechability testing

3) Congestion control 4) Route change notification

5) Performance measuring 6) Subnet addressing

Q.14 *When is ICMP redirect message used ?*

Ans. : The ICMP Redirect message is used to notify a remote host to send data packets on an alternative route. A host SHOULD NOT send an ICMP Redirect message. Redirects SHOULD only be sent by gateways.

The ICMP "redirect" message indicates that the gateway to which the host sent the datagram is no longer the best gateway to reach the net in question. The gateway will have forwarded the datagram, but the host should revise its routing

table to have a different immediate address for this net.

Q.15 *What is subnet masking ?*

MSBTE : Winter-18

Ans. : A subnet mask is a 32-bit number used to differentiate the network component of an IP address by dividing the IP address into a network address and host address

Q.16 *State the IP address classes.*

MSBTE : Winter-18

Ans. : IP address classes are Class A , Class B , Class C, Class D and Class E.

Q.17 *What is IP address ? State IP address classes.*

MSBTE : Winter-17

Ans. : IP address is network layer address, consisting of NETWORK portion, and HOST portion. It is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication

❑❑❑

UNIT - II

2 NEXT GENERATION IP

2.1 IPv6 Addressing

- Multiple addresses can be assigned to an interface
- Provider-based hierarchy to be used in the beginning
- Addresses should have 64-bit interface IDs in EUI-64 format
- IPv6 address is a 128-bit address includes two logical parts, a 64-bit network prefix and a 64-bit device ID.
- An IPv6 address has 128-bit

FE80:0000:0000:0000:0202:B3FF:FE1E:8329

1. Leading zeros in a block can be skipped

FE80:0:0:0:202:B3FF:FE1E:8329

2. A double colon can replace consecutive zeros

FE80::202:B3FF:FE1E:8329

- IPv6 specifies hexadecimal colon notation. The 128-bit is divided into eight sections, each 2 bytes in length. Fig. 2.1.1 shows binary and hexadecimal notation.
- In this address, many of the digits are zeros. The leading zeros of a section can be omitted. Only leading zero can be dropped, not the trailing zeros.
- Fig. 2.1.2 shows the abbreviated in IPv6
- Multiple addresses can be assigned to an interface. Provider-based hierarchy to be used in the beginning.

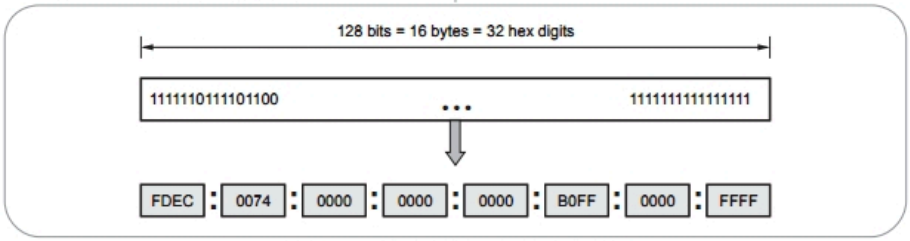


Fig. 2.1.1 Binary and hexadecimal notation

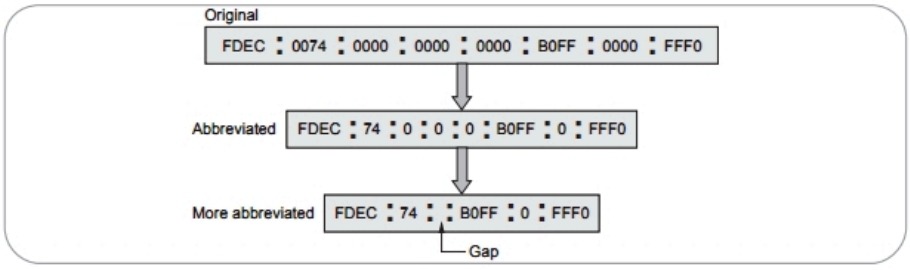


Fig. 2.1.2

2.1.1 Address Space Allocation

1. Unicast
2. Multicast (no broadcast)
3. Anycast

Unicast Address

- A single unique address identifying an IPv6 interface. It defines a single computer. The packet sent to unicast address must be delivered to that specific computer.
- Unicast address are of two types :
  1. Geographically based
  2. Provider based
- Fig. 2.1.3 shows provider based unicast address.

010	5	Provider Identifier	Subscriber Identifier	Subnet Identifier	Node Identifier

Fig. 2.1.3

- **Format Prefix :** Indicates type of address as Provider-Based Unicast. Always 3 bits, coded "010."
- **Registry Identifier :** Identifies the Internet address registry from which this ISP obtains addresses.
- **Subscriber Identifier :** Identifies the ISP's subscriber; this field contains the address assigned to this subscriber by the ISP. The ProviderID and SubscriberID fields together are 56 bits in length.
- **Provider Identifier :** Identifies the ISP; this field contains the address block assigned to this ISP by the address registry authority.
- **Subnet Identifier :** Each sub-network can have an identifier.
- **Node Identifier :** It is identity of node in the subnet.

Multicast Address

- IPv6 multicast addresses provide an identifier for a group of nodes. A node may belong to any number of multicast groups. Multicast addresses may not be used as a source address in IPv6 packets or appear in any routing header.
- A packet sent to a multicast address must be delivered to each member of the group.
- Fig. 2.1.4 shows the multicast address.

11111111 (8 bits)	Flag (4 bits)	Scope (4 bits)	Group ID (112 bits)

Fig. 2.1.4

- All multicast addresses are beginning with eight ones (0xFF).
- The next four bits are a set of flag bits (flgs); the three high-order bits are set to zero and the fourth bit (T-bit) indicates a permanently assigned multicast address (T=0) or a non-permanently assigned multicast address (T=1).
- The next four bits indicate the scope of the address (scope), or the part of the network for which this multicast address is relevant; options include node-local (0x1), link-local (0x2), site-local (0x5), organization-local (0x8), or global (0xE).
- The remaining 112 bits are the group identifier, which identifies the multicast group, either permanent or transient, within the given scope.

Anycast Address

- Anycast address also defines a group of nodes. An IPv6 address that is assigned to more than one interface.
- Packet sent to Anycast address is delivered to only one of the members of the Anycast group, the nearest one.

Reserved Addresses

- Reserved address is start with eight 0s.
- Reserved addresses are of following types :

a. Unspecified : Used when a host does not known its own address and sends an inquiry to find its address.

b. Loopback : Used by host to test itself.

c. Compatible : Used during the transition from IPv4 to IPv6.

d. Mapped : Also used during transition.

- Following are the some reserved addresses as follows :

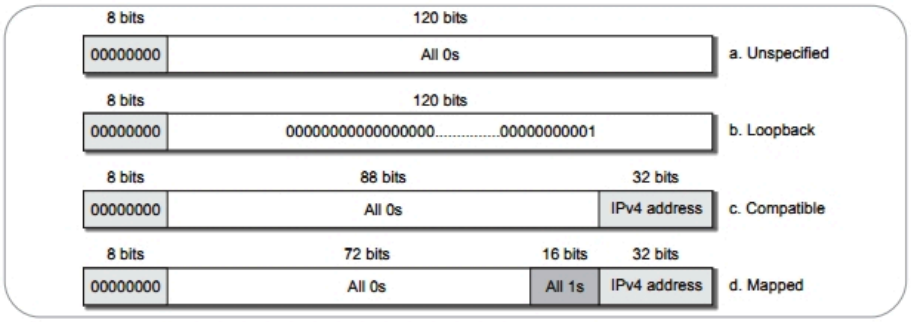


Fig. 2.1.5

2.1.2 Autoconfiguration and Renumbering

- IPv6 offers two types of autoconfiguration : stateless and stateful

1. Stateful Autoconfiguration

- Stateful autoconfiguration is the IPv6 equivalent of DHCP.
- A new protocol, called DHCPv6 is used to pass out addressing and service information in the same way that DHCP is used in IPv4.
- This is called "stateful" because the DHCP server and the client must both maintain state information to keep addresses from conflicting, to handle leases, and to renew addresses over time.
- The DHCPv6 protocol is not yet standardized.

2. Stateless Autoconfiguration

- It provides plug and play networking for hosts.
- With stateless autoconfiguration, a host gains an address via an interface automatically "leasing" an address and does not require the establishment of an server to delve out address space.
- Stateless autoconfiguration allows a host to propose an address which will probably be unique and propose its use on the network.
- Because no server has to approve the use of the address, or pass it out, stateless autoconfiguration is simpler.
- This is the default mode of operation for most IPv6 systems, including servers.
- Features of stateless autoconfiguration includes link-local addresses, multicasting, the Neighbor Discovery (ND) protocol, and the ability to generate the interface identifier of an address from the underlying data link layer address.

IPv6 Device Renumbering

- Renumbering is the process of changing the network numbers or host addresses for the devices on the network.
- In both IPv4 and IPv6, devices can only communicate with other devices with the same network number, even if they are connected to the same physical network.
- Renumbering of devices is a method related to autoconfiguration.
- Like host configuration, it can be implemented using protocols like DHCP, through the use of IP address "leases" that expire after a period of time.
- Under IPv6, networks can be renumbered by having routers specify an expiration interval for network prefixes when autoconfiguration is done.
- Later, they can send a new prefix to tell devices to regenerate their IP addresses. Devices can actually maintain the old "deprecated" address for a while and then move over to the new address.

2.2 Transition from IPv4 to IPv6

- Three strategies have been devised by the IETF to help the transition.

1. Dual stack 2. Tunneling 3. Header translation

2.2.1 Dual Stack

- All the host must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6.

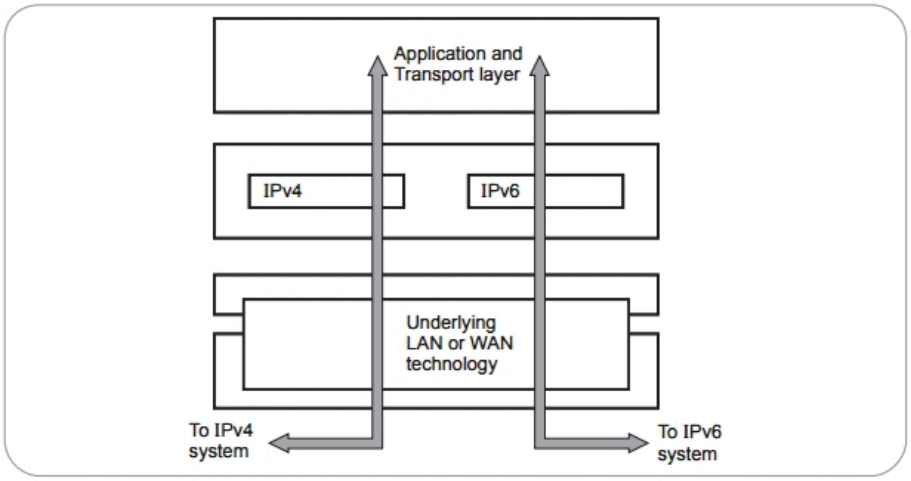


Fig. 2.2.1 Dual stack

- Fig. 2.2.1 shows the dual stack.
- To determine which version to use when sending a packet to destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

Tunneling

- When two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. The IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region.
- Fig. 2.2.2 shows the tunneling.

Header Translation

- Header translation is used when some of the system uses IPv4. The sender wants to use IPv6, but the receiver does not understand IPv6.
- Fig. 2.2.3 shows the header translation.
- The header format must be totally changed through header translation. The header of the IPv6 parket is converted to IPv4 header.

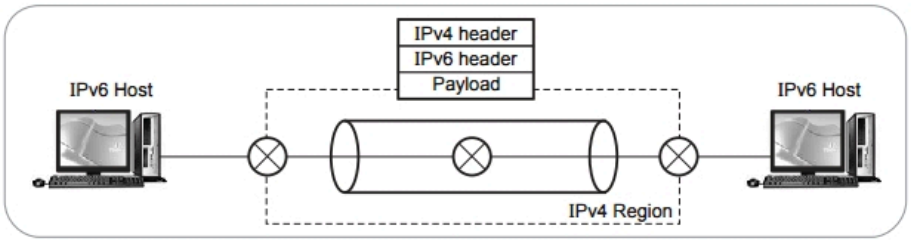


Fig. 2.2.2 Tunneling

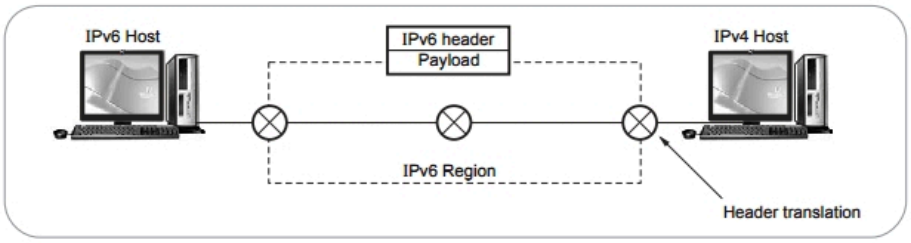


Fig. 2.2.3 Header translation

2.3 IPv6 Protocol

MSBTE : Summer-15,17,18, Winter-15,16,17,18

- The IPv6 packet is shown in Fig. 2.3.1. Each packet is composed of a mandatory base header followed by the payload. The payload consists of two parts : Optional and data.

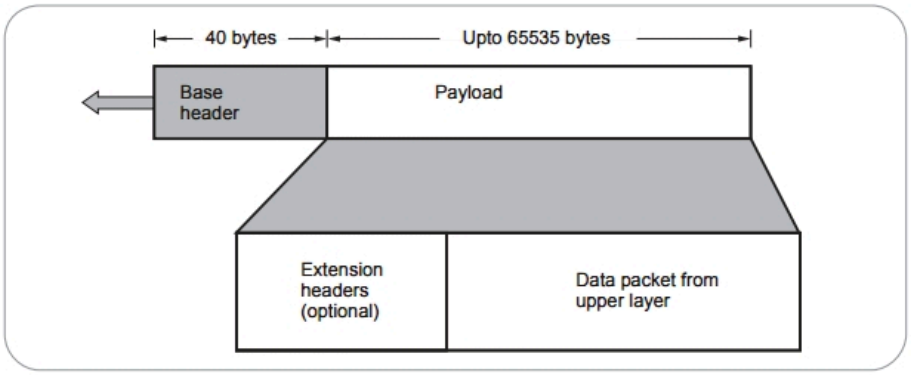


Fig. 2.3.1 IPv6 datagram header of payload

- Fig. 2.3.2 shows the IPv6 datagram header format.

1. **Versions :** This 4 bits field defines the version number of the IP. The value is 6 for IPv6.
2. **Priority :** The 4 bits priority field defines the priority of the packet with respect to traffic congestion.
3. **Flow label :** It is 24 bits field that is designed to provide special handling for a particular flow of data.
4. **Payload length :** The 16 bits payload length field defines the length of the IP datagram excluding the base header.
5. **Next header :** It is an 8 bits field defining the header that follows the base header in the datagram.
6. **Hop limit :** This 8 bits hop limit field serves the same purpose as the TTL field in IPv4.
7. **Source address :** The source address field is a 128 bits internet address that identifies the original.
8. **Destination address :** It is 128 bits Internet address that usually identifies the final destination of the datagram.

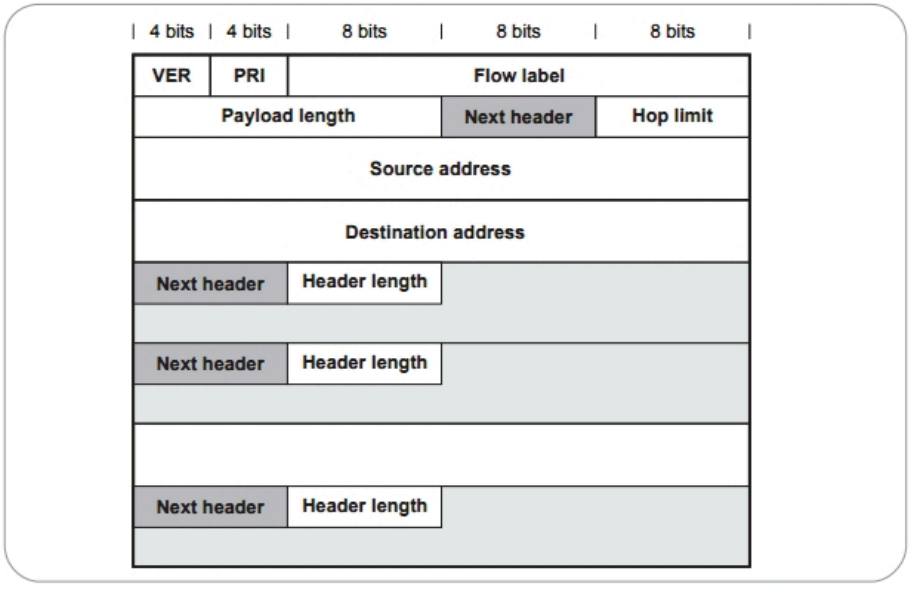


Fig. 2.3.2 IPv6 header

- Next header codes for IPv6

Code	Next header
0	Hop by hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null
60	Destination option

Priority

- The priority field defines the priority of each packet with respect to other packets from the same source. IPv6 divides traffic into two broad categories

1. Congestion controlled
2. Noncongestion controlled

- If a source adapts itself to traffic slowdown when there is congestion, the traffic is referred to as congestion controlled traffic. congestion controlled data are assigned priorities from 0 to 7.

Priority	Meaning
0	No specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

- A priority of 0 is the lowest; a priority of 7 is the highest.
- Noncongestion controlled traffic refers to a type of traffic that excepts minimum delay. Discarding of packets is not desirable. Retransmission in most cases is impossible. Real time audio and video are examples of this type of traffic.

- Priority numbers from 8 to 15 are assigned to noncongestion controlled traffic.

2.3.1 Extension Header

- The length of the base header is fixed at 40 bytes. Types of extension headers are
  1. Hop by hop option
  2. Source routing
  3. Fragmentation
  4. Authentication
  5. Encrypted security payload
  6. Destination option
- **Hop by hop option** is used when the source needs to pass information to all routers visited by the datagram.
- **Source routing** extension header combines the concepts of the strict source route and the loose source route options of IPv4.
- The concept of **fragmentation** is the same as that in IPv4. In IPv6, only the original source can fragment.
- The **authentication** header has a dual purpose : It validates the message sender and ensures the integrity of data.
- The **encrypted security payload** is an extension that provides confidentiality and guards against eavesdropping.
- The **destination option** is used when the source needs to pass information to the destination only. Intermediate routers are not permitted access to this information.

2.3.2 Comparison between IPv4 and IPv6

Sr. No.	IPv4	IPv6
1.	Header size is 32 bits.	Header size is 128 bits.
2.	It cannot support autoconfiguration.	Supports autoconfiguration
3.	Cannot support real time application.	Supports real time application.
4.	No security at network layer.	Provides security at network layer.
5.	Throughput and delay is more.	Throughput and delay is less.

2.3.3 Comparison between IPv4 and IPv6 Headers

1. The TTL field is called hop limit in IPv6.
2. Protocol field is replaced by the next header field.
3. Options field in IPv4 are implemented as extension headers in IPv6.
4. Header checksum field is eliminated.
5. Flag, identification and offset fields are eliminated from the base header in IPv6. they are included in the fragmentation extension header.
6. Header length is eliminated in IPv6.
7. Service field is eliminated in IPv6. The priority and flow label fields together take over the function of the service type field.

Board Questions

1. *Compare IPv4 and IPv6.*

MSBTE : Winter-15, 17, 18, Summer-15, 17, 18, Marks 4

2. *Differentiate IPv4 and IPv6.*

MSBTE : Winter-16, Marks 4

3. *State the limitation of IPv4.*

MSBTE : Summer-18, Marks 4

2.4 Two Marks Questions with Answers

Q.1 *What is the main reason for IPv6 being developed ?*

Ans. : The main issue surrounding IPv6 is addressing, or the lack of addressing. Many people believe that we are nearly out of the four billion addresses available in IPv4. IPv6 could be the solution to many problems, but IPv6 is still not fully developed and is not yet a standard.

Q.2 *What is unicast ?*

Ans. : Unicast is a communication between a single host and a single receiver.

Q.3 *What is multicast ?*

Ans. : Multicast is communication between a single host and multiple receivers.

Q.4 *What is anycast ?*

Ans. : Anycast is a communication between a single sender and a list of addresses.

Q.5 *Why IPv4 to IPv6 transition is required ?*

Ans. : As publicly available IPv4 addresses have been exhausted. IPv4, the current internet protocol version has crossed 30 years of time period. The expanding user base and increased number of IP-enabled devices created a need for an upgraded version.

From mobile apps to non-traditional computing devices populating the Internet of Things, businesses rely on ITs ability to deliver new services to both end users and customers. But these services and the infrastructure used to support them require IP addresses and that means an IPv6 migration.

Q.6 *Check whether the following IPv6 address notations are correct ?*

a) : : OF53:6382:AB00:67DB:BB27:7332.

b) 7803:42F2:::88EC-D4BA:B75D:11CD

Ans. :

a) : : OF53:6382:AB00:67DB:BB27:7332 : Correct

b) 7803:42F2:::88EC-D4BA:B75D:11CD : Incorrect because of two many (:)

Q.7 *State any two features of IPv6.*

MSBTE : Winter-16

Ans. : • IPv6 provides authentication and encryption.

• IPv6 uses end-to-end fragmentation.

Q.8 *Differentiate between IPv4 and IPv6 (two point) .*

MSBTE : Summer-16

Ans. : • IPv4 is 32 bits and IPv6 is 128 bits.

• IPv4 supports manual and DHCP configuration. IPv6 supports auto-configuration and renumbering.

❑❑❑

UNIT - III

3 UNICAST AND MULTICAST ROUTING PROTOCOLS

3.1 Introduction to Routing

- A host or a router has a routing table with an entry for each destination, or a combination of destinations, to route IP packets. Routing table can be either static or dynamic.
- A static routing table contains information entered manually. The administrator enters the route for each destination into the table.
- Dynamic routing table is updated periodically by using one of the dynamic routing protocols such as RIP, OSPE or BGP.
- The main function of the network layer is to route packets from source to destination. To accomplish this a route through the network must be selected, generally more than one route is possible. The selection of route is generally based on some performance criteria. The simplest criteria is to choose shortest root through the network.
- The shortest root means a route that passes through the least number of nodes. This shortest root selection results in least number of hops per packet. A routing algorithm is designed to perform this task. The routing algorithm is a part of network layer software.

Properties of routing algorithm

Certain properties which are desirable in a routing algorithm are -

Correctness, simplicity, robustness, stability, fairness, optimality and efficiency.

1. Correctness and simplicity are self-explanatory.
2. Robustness means the ability to cope with changes in the topology and traffic without requiring all jobs in hosts to be aborted and network to be rebooted everytime.
3. Stability refers to equilibrium state of algorithm. It is the technique that react to changing conditions such as congestions. Under any conditions the network must not react too slow or experience unstable swings from one extreme to another.
4. Some performance criteria may favour the exchange of data packets between nearby stations and discourage the exchange between distant stations. Some compromise is needed between fairness and optimality.

3.1.1 Routing Algorithm Classification

- Routing algorithm can be classified in several ways. Based on their responsiveness it can be classified into two types -
  1. Static (non-adaptive) Routing Algorithms.
  2. Dynamic (adaptive) Routing Algorithms.

1. Static (non-adaptive) routing algorithms

- In static routing the network topology determines the initial paths. The precalculated paths are then loaded to the routing table and are fixed for a longer period. Static routing is suitable for small networks. Static routing becomes **cumber some** for bigger networks.
- The disadvantage of static routing is its inability to respond quickly to network failure.

2. Dynamic (Adaptive) routing algorithms

- Dynamic routing algorithms change their routing decision if there is change in topology, traffic. Each router continuously checks the network status by communicating with neighbours. Thus a change in network topology is eventually propagated to all the routers. Based on this information gathered,

each router computes the suitable path to the destination.

- The disadvantage of dynamic routing is its complexity in the router.

Routing tables

- Once the routing decision is made, this information is to be stored in routing table so that the router knows how to forward a packet. In virtual circuit packet switching, the routing table contains each incoming packet number and outgoing packet number and output port to which the packet is to forward. In datagram networks, routing table contains the next hop to which to forward the packet, based on the destination address.

3.1.2 Advantages and Disadvantages of Static Routing

Advantages

1. Minimal CPU/Memory overhead.
2. Granular control on how traffic is routed.
3. Simple to configure and maintain.
4. Secure as only defined routes can be accessed.
5. Bandwidth is not used for sending routing updates.

Disadvantages

1. Manual update of routes after changes
2. Explicit addition of routes for all networks
3. Impractical on large network.

3.1.3 Advantages and Disadvantages of Dynamic Routing

Advantages

1. Simpler to configure on larger networks.
2. Will dynamically choose a different (or better) route if a link goes down.
3. Ability to load balance between multiple links.

Disadvantages

1. Updates are shared between routers, thus consuming bandwidth.
2. Routing protocols put additional load on router CPU/RAM.
3. The choice of the "best route" is in the hands of the routing protocol, and not the network administrator

3.1.4 Difference between Static and Dynamic Routing

Sr. No.	Static routing (Non adaptive)	Dynamic routing (Adaptive)
1.	Static routing manually sets up the optimal paths between the source and the destination computers.	Dynamic routing uses dynamic protocols to update the routing table and to find the optimal path between the source and the destination computers.
2.	The routers that use the static routing algorithm do not have any controlling mechanism if any faults in the routing paths.	The dynamic routing algorithms are used in the dynamic routers and these routers can sense a faulty router in the network.
3.	These routers do not sense the faulty computers encountered while finding the path between two computers or routers in a network.	the dynamic router eliminates the faulty router and finds out another possible optimal path from the source to the destination.
4.	The static routing is suitable for very small networks and they cannot be used in large networks	Dynamic routing is used for larger networks.
5.	The static routing is the simplest way of routing the data packets from a source to a destination in a network.	The dynamic routing uses complex algorithms for routing the data packets.
6.	The static routing has the advantage that it requires minimal memory.	Dynamic routers have quite a few memory overheads, depending on the routing algorithms used.
7.	The network administrator finds out the optimal path and makes the changes in the routing table in the case of static routing.	In the dynamic routing algorithm, the algorithm and the protocol is responsible for routing the packets and making the changes accordingly in the routing table.

3.1.5 Intra and Inter-domain Routing

- An internet is divided into autonomous systems. An **autonomous system** is a 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 system is referred to as **interdomain** routing.
- Distance vector and link state routing is the example of intradomain routing protocols.
- Path vector is an example of interdomain routing protocol.
- Fig. 3.1.2 shows an autonomous system.
- Only one interdomain routing protocol handles routing between autonomous systems.

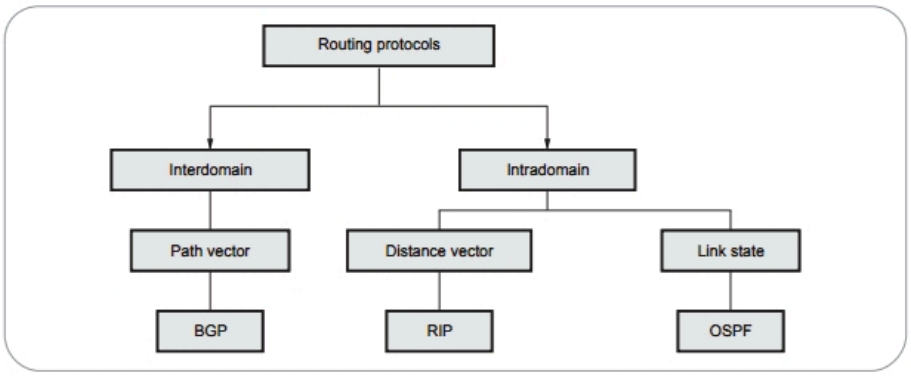


Fig. 3.1.1 Classification of routing protocols

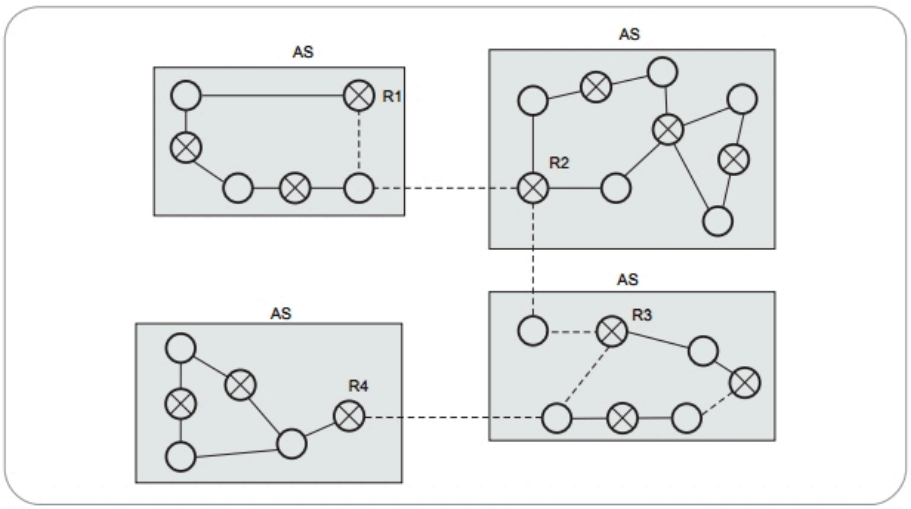


Fig. 3.1.2 Autonomous system

3.1.6 Comparison between Intra and Inter-domain Routing

Sr. No.	Intra-domain routing	Inter-domain routing
1.	Routing within an AS.	Routing between AS's.
2.	Ignores the Internet outside the autonomous system.	Assumes that the Internet consists of a collection of interconnected AS's.
3.	Protocols for Intra-domain routing are also called Interior Gateway Protocols.	Protocols for inter-domain routing are also called Exterior Gateway Protocols.
4.	Popular protocols are RIP and OSPF.	Routing protocols are BGP.

3.2 Routing Algorithms

3.2.1 Distance Vector Routing

- Distance vector routing algorithm is the dynamic routing algorithm. It was designed mainly for small network topologies. Distance vector routing algorithm is sometimes called by other names, most commonly the distributed **Bellman-Ford** routing algorithm and the **Ford-Fulkerson** algorithm.
- The term distance vector derives from the fact that the protocol includes its routing updates with a vector of distances, or hop counts.
- In this algorithm, each router maintains a routing table indexed by, and containing one entry for, each router in the subnet. This entry contains two parts :
  a. The preferred outgoing line to use for that destination.
  b. An estimate of the time or distance to that destination.
- The metric used might be number of hops, time delay in milliseconds, total number of packets queued along the path, etc.
- Assume that delay is used as a metric and that the router knows the delay to each of its neighbours. All nodes exchange information only with their neighbouring nodes. Nodes participating in the same local network are considered neighbouring nodes.
- Fig. 3.2.1 shows the subnet with 12 routers.
- Once every 'T' msec each router sends to each neighbor a list of its estimated delays to each destination. It also receives a similar list from each neighbor.
- By performing calculation for each neighbour, a router can find out which estimate seems the best and use that estimate and the corresponding line in its new routing table. Old routing table is not used in the calculation.
- Routing table is shown below.

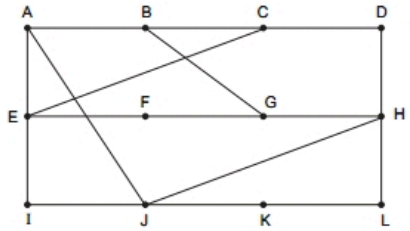
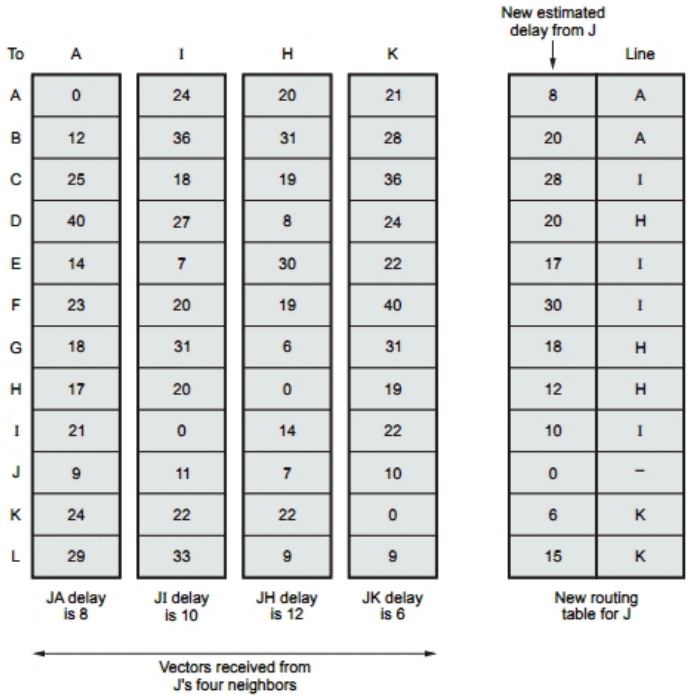
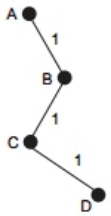


Fig. 3.2.1 Subnet



3.2.1.1 Count-to-Infinity Problem

- Fig. 3.2.2 shows an imagined network and denotes the distances from router A to every other router. Until now everything works fine.
- Suppose that link (A, B) is broken. Router B observed it, but in his routing table he sees, that router C has a route to A with 2 hops. The problem is, that B does not know that C has router B as successor in his routing table on the route to A.



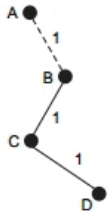
Routing table for A

B	C	D
1	2	3

Fig. 3.2.2

That followed **count-to-infinity** problem. Router B actualizes his routing table and takes the router to A over router C.

- In Fig. 3.2.3, we can see the new distances to A. In router C's routing the route to A contains router B as next hop router, so if B has increased his costs to A, C is forced to do so. Router C increases his cost to A about B + 1 = 4.



B	C	D
3	2	3

B	C	D
3	4	3

B	C	D
5	4	5

Fig. 3.2.3

- Now we see the conseuqence of the distributed Bellman-Ford protocal : Because router B takes the path over C to A, he reactualizes his routing table and so on.
- There are several partial solutions to the count-to-infinity problem. The first one is to use some relatively small number as an approximation of infinity. For example, we might decide that the maximum number of hops to get across a certain network is never going to be more than 16 and so we could pick 16 as the value that represents infinity.
- This at least bounds the amount of time that it takes to count to infinity. Of course, it could also present a problem if our network grew to a point where some nodes were separated by more than 16 hops.
- One technique to improve the time to stabilize routing is called **split horizon**. Split horizon technique implies that routing information about some network stored in the routing table of a specific router is never sent to the router from which it was received.

3.2.1.2 Issues with the Distance Vector Routing

1. The primary drawback of this algorithm is its vulnerability to the 'Count-to-Infinity' problem. There have been proposed many partial solutions but none works under all circumstances.
2. Another drawback of this scheme is that it does not take into account Link Bandwidth.
3. Yet another problem with this algorithm is that it takes appreciably long time for convergence as the network-size grows.
4. A fallout of the Count-to-Infinity issue and slow convergence has been to limit the maximum number of hops to 15 which means more than 16-router subnets, it may not be appropriate routing algorithm.

Ex. 3.2.1 *For the network given in Fig. 3.2.4, give global distance - vector tables when*
i) Each node knows only the distances to its immediate neighbors.
ii) Each node has reported the information it had in the preceding step to its immediate neighbors.
iii) Step (iv) happens a second time.

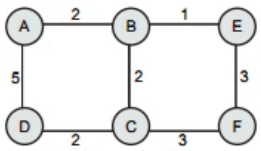


Fig. 3.2.4

Sol. : • Each node constructs a one-dimensional array containing the "distances"(costs) to all other nodes and distributes that vector to its immediate neighbors.
- The starting assumption for distance-vector routing is that each node knows the cost of the link to each of its directly connected neighbors.
- A link that is down is assigned an infinite cost.

Initial distances stored at each node (global view)

Information Stored at Node	Distance to Reach Node					
	A	B	C	D	E	F
A	0	2	?	5	?	?
B	2	0	2	?	1	?
C	?	2	0	2	?	3
D	5	?	2	0	?	?
E	?	1	?	?	0	3
F	?	?	3	?	3	0

- Note that each node only knows the information in one row of the table.

1. Every node sends a message to its directly connected neighbors containing its personal list of distance. (for example, A sends its information to its neighbors B, and D)
2. If any of the recipients of the information from A find that A is advertising a path shorter than the one they currently know about, they update their list to give the new path length and note that they should send packets for that destination through A.
3. After every node has exchanged a few updates with its directly connected neighbors, all nodes will know the least-cost path to all the other nodes.

4. In addition to updating their list of distances when they receive updates, the nodes need to keep track of which node told them about the path that they used to calculate the cost, so that they can create their forwarding table.

- Final distances stored at each node (global view).

Information Stored at Node	Distance to Reach Node					
	A	B	C	D	E	F
A	0	2	4	5	3	6
B	2	0	2	4	1	4
C	4	2	0	2	3	3
D	5	4	2	0	5	5
E	3	1	3	5	0	3
F	6	4	3	5	3	0

- In practice, each node's forwarding table consists of a set of triples of the form : (Destination, Cost, NextHop).
- For example, below table shows the complete routing table maintained at node B for the network

Destination	Cost	NextHop
A	2	A
C	2	C
D	4	C
E	1	E
F	4	E

3.2.2 Link State Routing

- Link state routing is the second major class of intradomain routing protocol. It is **dynamic** type routing algorithm.
- The idea behind link state routing is simple and can be stated as five parts. Each router must do the following :

1. **Learning about the neighbors :** When a router is booted, it sends a special HELLO packet on each point-to-point line. The router on the other end is expected to send back a reply telling who it is. When two or more routers are connected by a LAN, the LAN can be modeled as a node.
2. **Measuring line cost :** To determine the cost for a line, a router sends a special ECHO packet over the line that the other side is required to send back immediately. By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay. Should the load be taken into account when measuring the delay ?
3. **Building link state packets :** State packets may be built periodically, or when some significant event occurs, such as a line or neighbour going down or coming back up again.
4. **Distributing the link state packets :** The basic algorithm

- Each state packet contains a sequence number that is incremented for each new packet sent.
- Routers keep track of all the (source router, sequence) pairs they see.
- 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 (i.e., flooding). 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 as being obsolete.

Problems with the basic algorithm :

1. The sequence numbers may wrap around, causing confusion. Solution : using a 32-bit sequence number. With one packet per second, it would take 137 years to wrap around.
2. If a router ever crashes, it will lose track of its own sequence number. If it starts again at the sequence number 0, new packets will be rejected as obsolete/duplicate by other routers.
3. If a sequence number is ever corrupted and 65,540 is received instead of 4 (a 1-bit error), packets 5-65540 will be rejected as obsolete.

- The solution to router crashes and sequence number corruption is to associate an age with each state packet from any router and decrement the age once per second. When the age hits zero, the information from that router is discarded. Normally a new packet comes in every 10 seconds, so router information only times out when a router is down.

Some refinements to the basic algorithm make it more robust

- When a state packet comes in to a router for flooding, it is put in a holding area to wait a short while first. If another state packet from the same source comes in before it is transferred, their sequence numbers are compared. If they are equal, the duplicate is discarded. If they are different, the older one is thrown out. To guard against errors on the lines, all state packets are acknowledged. When a line goes idle, the holding area is scanned in round robin to select a packet or acknowledgement to send.

5. **Computing the new routes :** Once a router has accumulated a full set of link state packets, it can construct the entire subnet graph. Then Dijkstra's algorithm can be run locally to construct the shortest path to all possible destinations.

- Link state routing protocols use event driven updates rather than periodic updates. Link state routing is widely used in actual networks. OSPF protocol uses in a link state algorithm.
- Link state routing protocols are as follows :
  a. Open Shortest Path First (OSPF)
  b. Netware Link Services Protocol (NLSP).
  c. Apple's AURP.
  d. ISO's Intermediate System-Intemediate System (IS-IS).

3.2.3 Difference between Distance Vector and Link State Routing

Sr. No.	Distance vector	Link state
1.	Bellman-ford algorithm used to calculate the shortest cost path.	Dijkstra's algorithm used to calculate link state cost.
2.	Sends message to their neighbors.	Sends message to every other node in the network.
3.	It is decentralized routing algorithm.	It is centralized global routing algorithm.
4.	Sends larger updates only to neighbouring routers.	Send small updates every where.
5.	Protocol example - RIP	Protocol example - OSPF and BGP.
6.	Require less CPU power and less memory space.	Require more CPU power and more memory space.
7.	Simple to implement and support.	Expensive to implement and support.

3.2.4 Bellman-Ford Algorithm

- In shortest path routine the path length between each node is measured as a function of distance, bandwidth, average traffic, communication cost, mean queue length, measured delay etc.
- By changing the weighing function, the algorithm then computes the shortest path measured according to any one of a number of criteria or a combination of criteria. For this a graph of subnet is drawn. With each node of graph representing a router and each arc of the graph representing a communication link. Each link has a cost associated with it. To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.
- Two algorithms for computing the shortest path between two nodes of a graph are known.
  i) Dijkstra's algorithm
  ii) Bellman-Ford algorithm.

i) Dijkstra's algorithm :

- Each node is labelled with its distance from the source node along the best known path. Initially no paths are known, so all nodes are labelled with infinity. The algorithm proceed in stages. As the algorithm proceeds, the paths are found, the labels are changed, reflecting better paths. Stepwise proceeding of algorithm is as follows.

Step-I : Source node is initialized and can be indicated as a filled circle.

Step-II : Initial path cost to neighbouring nodes (adjacent nodes) or link cost is computed and these nodes are relabelled considering source node.

Step-III : Examine the all adjacent nodes and find the smallest label, make it permanent.

Step-IV : The smallest label node is now working node, then step-II and step-III are repeated till the destination node reaches.

Following example illustrates Dijkstra's algorithm.

Ex. 3.2.2 *Find the shortest path between node A and node H for the following Fig. 3.2.5 by applying Dijkstra's algorithm. Show each steps output.*

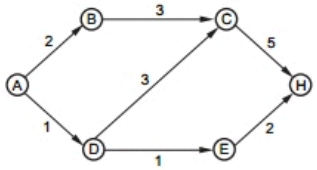


Fig. 3.2.5

Sol. : Step-I : Node A is initialized as source node.

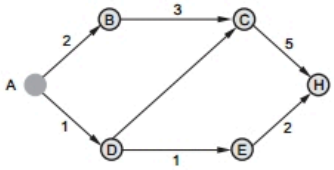


Fig. 3.2.5 (a)

Step-II : Link cost is computed for the adjacent node.

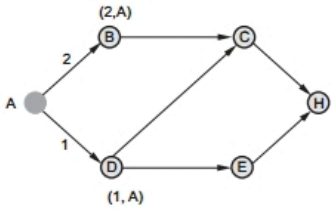


Fig. 3.2.5 (b)

Step-III : Since AD is smallest path, now D is working node.

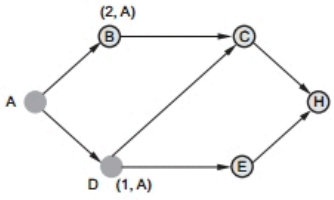


Fig. 3.2.5 (c)

Step-IV : Adjacent nodes to D are C and E.

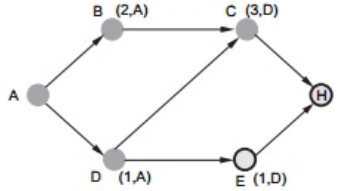


Fig. 3.2.5 (d)

Step-V : Since shortest is E, now E is working node.

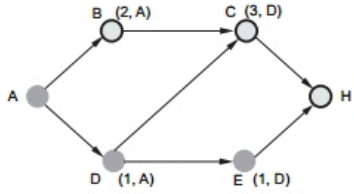


Fig. 3.2.5 (e)

Step-VI :

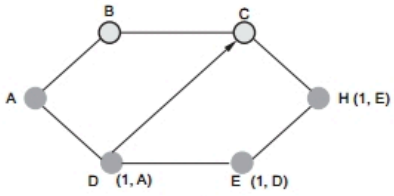


Fig. 3.2.5 (f)

Hence the shortest path between node A and node H is ADEH.

ii) Bellman-Ford algorithm :

- Bellman-Ford algorithm is somewhat similar to Dijkstra's algorithm but here the shortest paths from a given source node is computed subject to the constraint that the path contain at most one link, i.e. from source node, at each step least-cost path with maximum number of links are found. Finally the least-cost path to each node and the cost of that path is computed. Bellman-Ford algorithm is illustrated in the following example.

Ex. 3.2.3 *Find the shortest path between node A and node H using Bellman-Ford algorithm, for the Fig. 3.2.6 shown in example 3.2.2.*

Sol. : Step-1 :

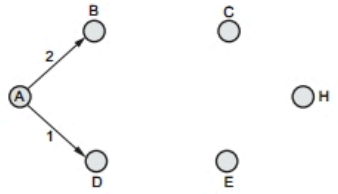


Fig. 3.2.6 (a)

Distance AD is shorter than AB. So route AD is chosen.

Step-2 :

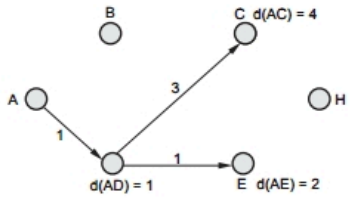


Fig. 3.2.6 (b)

$\because$ d(AE) < d(AC)

$\therefore$ d(AE) is chosen.

Step-3 :

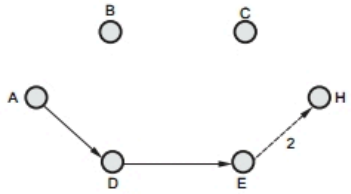


Fig. 3.2.6 (c)

So the shortest distance is ADEH, the result is same as in Dijkstra's algorithm.

3.2.5 Path Vector Routing

- RIP and OSPF are not suitable for inter-domain routing protocols. Both require homogenous metrics that may be the case within an AS, but we cannot assume then same for several AS systems.
- Flooding the link state information across multiple AS systems is not scalable.
- It is different from the distance vector routing and link state routing. Each entry in the routing table contains the destination network, the next router and the path to reach the destination.
- Distance vector routing is subject to instability if there are more than a few hops in the domain of operation.
- Link state routing needs a huge amount of resources to calculate routing tables. It also creates heavy traffic because of flooding.
- Path vector routing protocol provides information about how to reach a network given a certain router and identifies which autonomous system should be visited.
- The path vector routing is different from distance vector algorithm, in which each path has information about cost and distance.
- BGP is an example of a path vector protocol. In BGP the routing table maintains the autonomous systems that are traversed in order to reach the destination system. Exterior Gateway Protocol (EGP) does not use path vectors.
- In path vector routing we assume there is one node in each autonomous system which acts on behalf of the entire autonomous system. This node is called the **speaker node.**
- The speaker node creates a routing table and sends information to its neighboring speaker nodes in neighboring autonomous systems. The idea is the same as Distance vector routing except that only speaker nodes in each autonomous system can communicate with each other.
- The speaker node sends information of the path, not the metric of the nodes, in its autonomous system or other autonomous systems. The path vector routing algorithm is somewhat similar to the distance vector algorithm in the sense that each border router advertises the destinations it can reach to its neighboring router.
- A route is defined as a pairing between a destination and the attributes of the path to that destination, thus the name, path vector routing, where the routers receive a vector that contains paths to a set of destinations.

- The main advantage of a path vector protocol is its flexibility.

3.3 Unicast Routing Protocol

- Routing table can be static or dynamic. Manual entries are done in static table.
- Dynamic table is updated automatically when there is a change somewhere in the internet.
- Now a day, dynamic table is used because of sudden changes in the internet. One of the routers in the internet may fail or link between any two routers is down. So because of these reasons dynamic table is required.
- Routing protocol is a combination of rules and procedures that let routers in the internet inform each other of changes.

3.3.1 Routing Information Protocol (RIP)

- In RIP, routing updates are exchanged between neighbours approximately every 30 seconds using a so-called **RIP response message**. The response message sent by a router or host contains a list of upto 25 destination networks within an autonomous system (AS). Response messages are also known as **RIP advertisements**.
- Fig. 3.3.1 shows a portion of an autonomous system.
- Forwarding table in router D before receiving advertisement from router A. For this example, the table indicates that to send a datagram from router D to destination network W, the datagram should first be forwarded to neighbouring router A; the table also indicates that destination network W is two hops away along the shortest path.
- The Table 3.3.1 also indicates that network Z is seven hops away via router B.

Destination network	Next router	Number of hops to destination
W	A	2
Y	B	2
Z	B	7
X	–	1
.....	.....	.....

Table 3.3.1 Forwarding table

- Now suppose that 30 seconds later, router D receives from router A the advertisement shown in Table 3.3.2.

Destination network	Next router	Number of hops to destination
Z	C	4
W	–	1
X	–	1
.....	.....	.....

Table 3.3.2 Advertisement from router A

- Note that the advertisement is nothing other than the forwarding table information from router A. This information indicates, in particular, that network Z is only four hops away from router A. Router D, upon receiving this advertisement, merges the advertisement with the old routing table.
- Router D learns that there is now a path through router A to network Z that is shorter than the path through router B. Thus, router D updates its forwarding table to account for the shorter shortest path, as shown in Table 3.3.3.

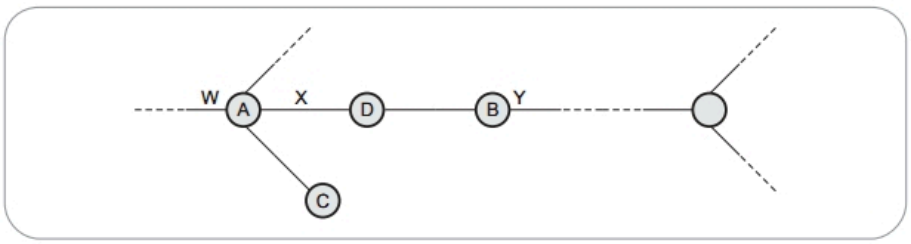


Fig. 3.3.5 Portion of AS

Destination network	Next router	Number of hops to destination
W	A	2
Y	B	2
Z	A	3
.....	.....	.....

Table 3.3.3

- RIP routers exchange advertisements approximately every 30 seconds. If a router does not hear from its neighbour atleast once every 180 seconds, that neighbour is considered to be no longer reachable; i.e. either the neighbour has died or the connecting link has gone down. When this happens, RIP modifies the local forwarding table and then propagates this information by sending advertisements to its neighbouring routers.
- A router can also request information about its neighbour's cost to a given destination using RIP's request message. Routers send RIP request and response messages to each other over UDP using port number 520.

RIP Message Format

- Fig. 3.3.2 shows the RIP message format.

1. **Command :** This is 8 bits field specifies the type of message: 1 for request and 2 for response.
2. **Version :** This is 8 bits field define the version.
3. **Family :** This 16 bits field defines the family of the protocol used. For TCP/IP the value is 2.
4. **Network address :** The address field defines the address of the destination network.
5. **Distance :** This 32 bits field defines the hop count from the advertising router to the destination network.

Request and Response

- RIP support two types of messages : Request and Response.

Request

- A request message is sent by a router that has just comp up or by a router that has some time out entries.

Response

- A response message can be either solicited or unsolicited.

1. Solicited response
   - Is sent only in answer to a request.
   - Containing information about the destination specified in the corresponding request.
2. Unsolicited response
   - Is sent periodically, every 30 seconds.
   - **Containing** information covering the whole routing table.

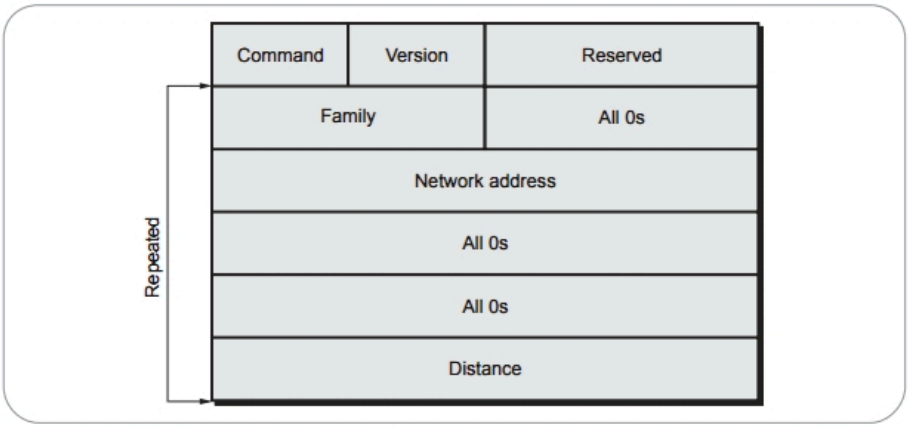
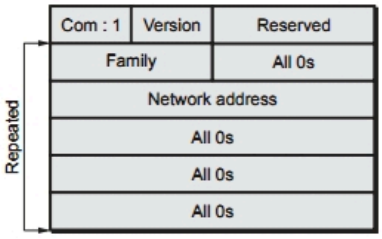
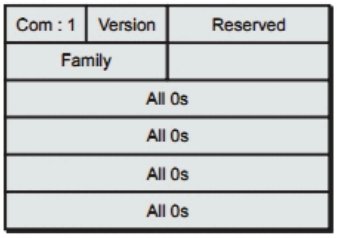


Fig. 3.3.2 RPI message format

Fig. 3.3.3 shows the request message.



(a) Request for some



(b) Request for all

Fig. 3.3.3 Request message format

Timers in RIP

- RIP uses three timers to support its operation.
  1. Periodic timer (25 - 35 sec)
  2. Expiration (180 sec)
  3. Garbage collection (120 sec).

1. **Periodic timer :** This type of timer controls the advertising of regular update messages. Each router has one periodic timer that is randomly set to a number between 25 to 35 seconds.
2. **Expiration timer :** The expiration timer governs the validity of a route. In normal situation, the new update for the route occurs every 30 seconds. But, if there is a problem on an internet and no update is received within the allotted 180 seconds, the route is considered expired and the hop count of the route is set to 16. Each router has its own expiration timer.
3. **Garbage collection timer :** When the information about a route becomes invalid, the router continues to advertise the route with a metric value of 16 and the garbage collection timer is set to 120 sec for that route. When the count reaches zero, the route is purged from the table.

RIPv2

- RIP version 2 was designed to overcome some of the shortcomings of version 1. Replaced fields in version 1 that were filled with 0s for the TCP/IP protocols with some new fields.
- **Advantages**
  1. An AS can include several hundred routers with RIP-2 protocol.
  2. Compatible upgrade of RIPv1 including subnet routing, authentication, CIDR aggregation, route tags and multicast transmission.
  3. Subnet support : Uses more convenient partitioning using variable-length subnets
  4. An end system can run RIP in passive mode to listen for routing information without supplying any.
  5. Low requirement in memory and processing at the node .
  6. RIP and RIP2 are for the IPv4 network while the RIPng is designed for the IPv6 network.

Fig. 3.3.4 shows the message format.

1. **Command -** The command field is used to specify the purpose of the datagram.
2. **Version -** The RIP version number. The current version is 2.
3. **Identifier -** Indicates what type of address is specified in this particular entry.
4. **Route tag -** Attribute assigned to a route which must be preserved and readvertised with a route. The route tag provides a method of separating internal RIP routes from external RIP routes, which may have been imported from an EGP or another IGP.
5. **IP address -** The destination IP address.
6. **Subnet mask -** Value applied to the IP address to yield the non-host portion of the address. If zero, then no subnet mask has been included for this entry.

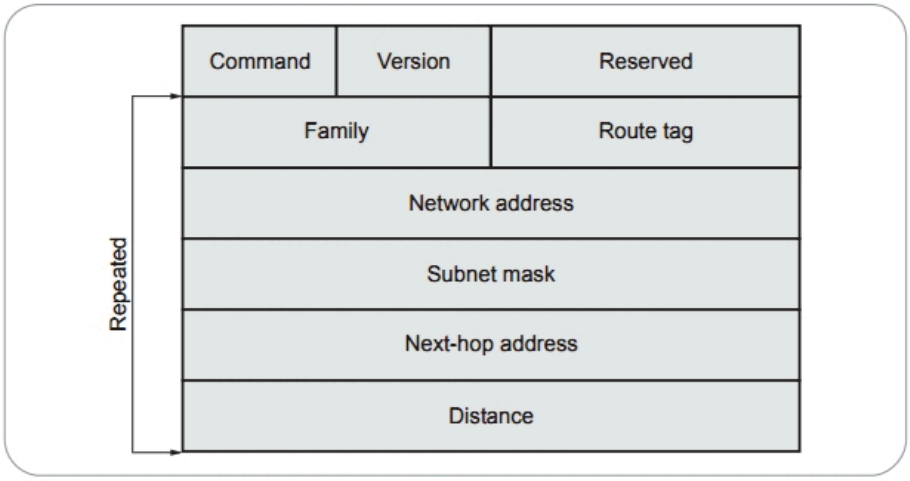


Fig. 3.3.4 Message format of RIPv2

7. **Next hop** - Immediate next hop IP address to which packets to the destination specified by this route entry should be forwarded.
8. **Distance** - Represents the total cost of getting a datagram from the host to that destination.

Authentication

- Authentication is added to protect the message against unauthorized advertisement. No new field is added to the packet.
- To indicate that the entry is authentication information and not routing information, the value of FFFFH is entered in the family field.
- Fig. 3.3.5 shows the authentication.

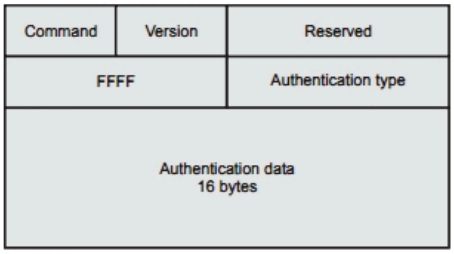


Fig. 3.3.5 Authentication

- Authentication type defines the protocol used for authentication.
- Authentication data is the actual data.

RIP2 - Disadvantages

1. RIP2 supports generic notion of authentication, but only "password" is defined so far. Still not very secure.
2. RIP2 packet size increases as the number of networks increases hence it is not suitable for large networks.
3. RIP2 generates more protocol traffic than OSPF, because it propagates routing information by periodically transmitting the entire routing table to neighbour routers.
4. RIP2 may be slow to adjust for link failures.

Advantages of RIP and Disadvantages of RIP version 1

Advantages of RIP

1. RIP is very useful in a small network, where it has very little overhead in terms of bandwidth used and configuration and management time.
2. Easy to implement than newer IGP's.
3. Many implementations are available in the RIP field.

Disadvantages of RIP1

1. Minimal amount of information for router to route the packet and also very large amount of unused space.
2. Subnet support : Supports subnet routes only within the subnet network.
3. Not secure; anyone can act as a router just by sending RIP1 messages.

RIP1 was developed for an AS that originally included less than a 100 routers.

3.3.2 Open Shortest Path First (OSPF)

- OSPF is a link state routing protocol. OSPF is based on the distributed map concept all nodes have a copy of the network map, which is regularly updated. Each node contains a routing directory database. This database contains informations about the routers interfaces that are operable, as well as status information about adjacent routers. This information is periodically broadcast to all routers in the same domain.
- The OSPF computes the shortest path to the other routers. OSPF protocol is now widely used as the interior router protocol in TCP/IP networks. OSPF computes a route through the internet that incurs the least cost based on a user-configurable metric of cost. The user can configure the cost to express a function of delay, data rate, or other factors. OSPF is able to equalize loads over multiple equal cost paths.
- OSPF is classified as an Internal Gateway Protocol (IGP) because it support routing within one autonomous system only. The exchange of routing information between autonomous systems is the responsibility of another protocol an External Gateway Protocol (EGP). OSPF can support one or many networks.
- Following is the **features** of the OSPF.
  1. OSPF supports multiple circuit load balancing because it can store multiple routes to a destination.
  2. OSPF can converge very quickly to network topology change.
  3. OSPF support multiple metrics.
  4. OSPF is not susceptible to routing loops.
  5. OSPF support for variable length subnetting by including the subnet mask in the routing message.
- OSPF introduces a two level hierarchy for improving scalability. It allows an AS to be partitioned into several groups called areas, that are interconnected by a central backbone area as shown in the Fig. 3.3.6.

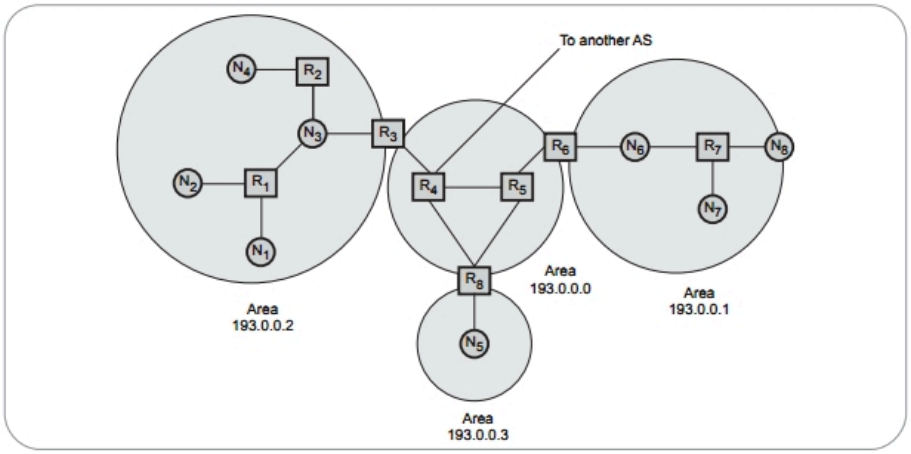


Fig. 3.3.6 OSPF areas

- An area is identified by a 32-bit number known as the area ID. The backbone area is identified with area ID 193.0.0.0 The information from other area is summarized by area border router that have connections to multiple areas.
- OSPF uses four types of routers.
  1. An internal router is a router with all its links connected to the networks within the same area.
  2. An area border router is a router that has its links connected to more than one area.
  3. A backbone router is a router that has its links connected to the backbone.
  4. An Autonomous System Boundary Router (ASBR) is a router that has its links connected to another autonomous system.
- As shown in the Fig. 3.3.6 routers R_1, R_2 and R_7 are internal routers. Routers R_3, R_6, R_8 are area border routers. Routers R_3, R_4, R_5, R_6, R_8 are backbone routers. Router R_4 is an ASBR.
- A hello protocol allows neighbours to be discovered automatically. Two routers are said to be neighbours if they have an interface to a common network. The OSPF protocol runs directly over IP, using IP protocol 89. The header format for OSPF is shown in the Fig. 3.3.7.
- OSPF header analysis is given below :
  1. **Version :** This field specifies the protocol version.
  2. **Type :** This field indicates messages as one of the following type.
     a. Hello b. Database description
     c. Link status d. Link status update
     e. Link status acknowledgement.
  3. **Packet length :** This field specifies the length of OSPF packet in bytes, including the OSPF header.
  4. **Router ID :** It identifies the sending router. This field is typically set to the IP address of one of its interfaces.
  5. **Area ID :** This field identifies the area this packet belongs to (Transmitted).
  6. **Checksum :** The checksum field is used to detect errors in the packet. The checksum is performed on the entire packet.
  7. **Authentication type :** It identifies the authentication type that is used.
  8. **Authentication :** This field includes a value from the authentication type.

The OSPF operation consists of the following stages.

1. OSPF send the Hello messages for discovering the neighbours and designated routers are elected in multiaccess networks.
2. Adjacencies are established and link state databases are synchronized.
3. Link state advertisement are exchanged by adjacent routers to allow topological databases to be maintained and to advertise inter area and inter AS routes. The routers use the information in the database to generate routing tables.

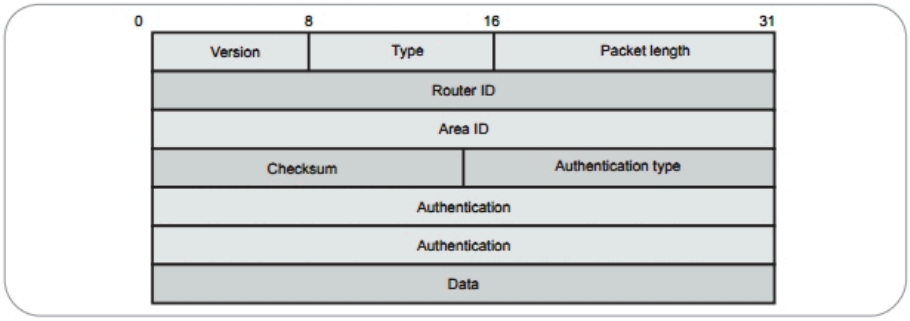


Fig. 3.3.7 OSPF common header

OSPF Advantages

1. Low traffic overhead. OSPF is enconomical of network bandwidth on links between routers.
2. Fast convergence. OSPF routers flood updates to changes in the network around the internet, so that all routers quickly agree on the new topology after a failure.
3. Larger network metrics. This allows a network planner the freedom to assign costs for each path around the network, to give fine control over routing paths.
4. Area based topology. Large OSPF networks are organized as a set of areas linked by a backbone. Routing within each area is isolated to minimize cross area discovery traffic.
5. Route summaries. OSPF can minimize the routes propagated across an area boundary by collapsing several related sub-net routes into one. This reduces routing table sizes, and increases the practical size of a network.
6. Support for complex address structures. OSPF allows variable size sub-netting within a network number, and sub-nets of a network number to be physically disconnected. This reduces waste of address space, and makes changing a network incrementally much easier.
7. Authentication. OSPF supports the use of passwords for dynamic discovery traffic, and checks that paths are operational in both directions. The main use for this is to prevent misconfigured routers from "poisoning" the routing tables throughout the internet.

OSPF Disadvantages

1. Memory overhead. OSPF uses a link state database to keep track of all routers and networks within each attached area. With a complex topology, this database can be much larger than the corresponding routing pool, and may limit the maximum size of an area.
2. Processor overhead. During steady state operation the OSPF CPU usage is low, mainly due to the traffic between routers. However, when a topology change is detected, there is a large amount of processing required to support flodding of changes, and recalculation of the routing table.
3. Configuration. OSPF can be complex to configure.

3.3.3 BGP4

- The purpose of an exterior gateway protocol is to enable two different Autonomous System (AS) to exchange routing information so that IP traffic can flow across the autonomous system border.
- BGP was developed for use in conjunction with internets that employ the TCP/IP protocol suite. The BGP is an interdomain routing protocol that is used to exchange network reachability information among BGP routers (Also called BGP speakers).
- Each BGP speaker establishes a TCP connection with one or more BGP speakers (routers). Two routers are considered to be neighbours if they are attached to the same subnetwork.
- If the two routers are in different autonomous systems, they may wish to exchange routing information.
- BGP performs three functional procedures.
  1. Neighbour acquisition
  2. Neighbour reachability
  3. Network reachability.
- Neighbour acquisition procedures used for exchanging the routing information between two routers in different Autonomous Systems (AS). To perform neighbour acquisition, one router sends an open message to another. If the target router accepts the request, it returns a keepalive message in response.
- Once a neighbour relationship is established, the neighbour reachability procedure is used to maintain the relationship. Both sides needs to be assured that the other side still exists and is still engaged in the neighbour relationship. For this purpose, both routers send keepalive messages to each other. Both sides router maintains a database of the subnetworks that it can reach and the perferred route for reaching that subnetwork.
- If the database changes, router issues an update message that is broadcast to all other routers implementing BGP. By the broadcasting of these

updata message, all the BGP routers can build up and maintain routing information.

- BGP connections inside an autonomous system are called internal BGP (iBGP) and BGP connections between different autonomous systems are called external BGP (eBGP).
- Fig. 3.3.8 shows the internal and external BGP.

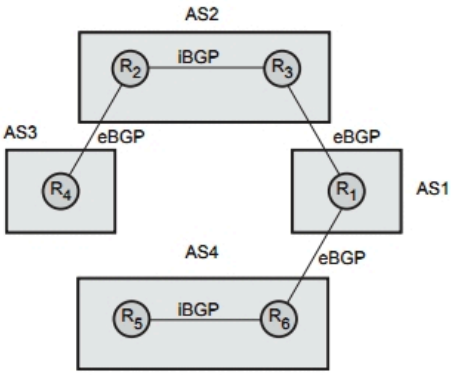


Fig. 3.3.8 Internal and external BGP

BGP messages : Header of the all BGP messages is fixed size that identifies the message type. Fig. 3.3.9 shows the BGP message header format.

1. **Marker :** Marker field is used for authentication. The sender may insert value in this field that would be used as part of an authentication mechanism to enable the recepient to verify the identity of the sender.
2. **Length :** This field indicates the total length of the message in octets, including the BGP header. Value of the length must be between 19 and 4096.
3. **Type :** Type field indicates type of message. BGP defines four message type.
   a) OPEN b) UPDATE
   c) NOTIFICATION d) KEEPALIVE

- Following Fig. 3.3.10 shows the four types of BGP message formats.
- To acquire a neighbour, a router first opens a TCP connection to the neighbour router of interest. It then sends the open message. This message identifies the AS to which the sender belongs and provides the IP address of the router. It also includes a Hold time parameter.
- If the recipient is prepared to open a neighbour relationship, it calculate a value of Hold Timer that is the minimum of its Hold Time in the open message. This calculated value is the maximum number of seconds that may elapse between the receipt of successive keepalive and update message by the sender.
- The KEEPALIVE message is just the BGP header with the type field set to 4. The KEEPALIVE messages are exchanged often enough as to not cause the hold timer to expire. A recommended time between successive KEEPALIVE messages is one-third of the hold time interval. This value ensures that KEEPALIVE messages arrive at the receiving router almost always before the hold timer expires even if the transmission delay of a TCP is variable. If the hold time is zero, then KEEPALIVE messages will not be sent.
- When a BGP router detects an error, the router sends a NOTIFICATION message and then close the TCP connection. After the connection is established, BGP peers exchange routing information by using the UPDATE messages.
- The UPDATE messages may contain three pieces of information. Unfeasible routes, path attributes and network layer reachability information.

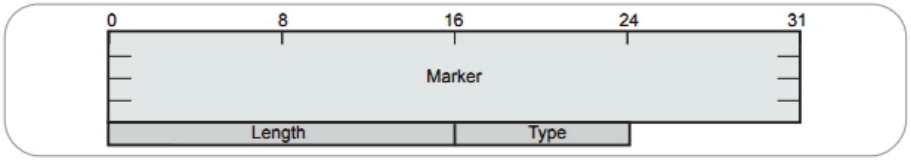


Fig. 3.3.9 BGP header format

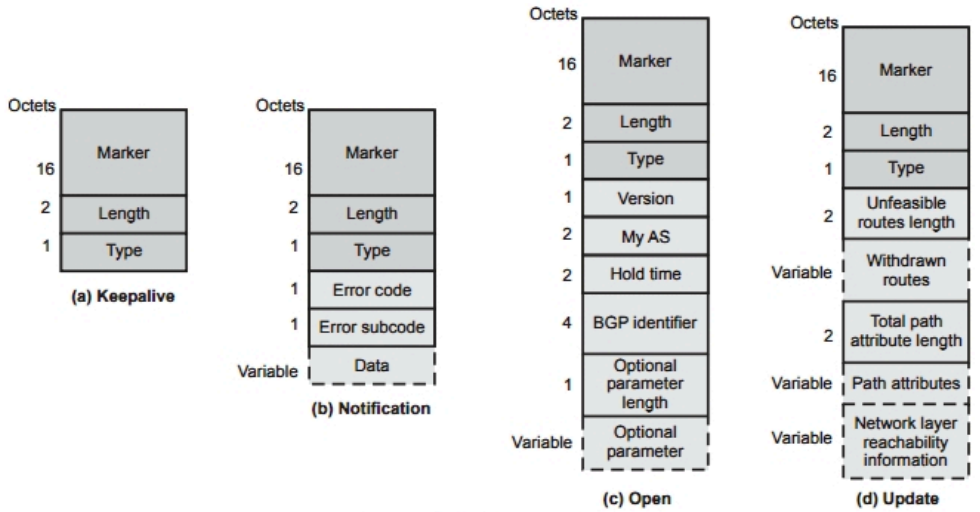


Fig. 3.3.10 BGP message format

- An UPDATE message can advertise a single route and withdraw a list of route. An update message may contain one or both types of information. The UPDATE messages are used to construct a graph of Autonomous System (AS) connectivity. The withdrawn routes field provides a list of IP address prefixes for the routes that need to be withdrawn from BGP routing tables. The unfeasible routes length field indicates the total length of the withdrawn routes field in actets.
- An UPDATE message can withdraw multiple unfeasible routes from service. A BGP router uses Network Layer Reachability Information (NLRI), the total path attributes length and the path attributes to advertise a route. The NLRI field contains a list of IP address perfixed that can be reached by the route.

Advantages of BGP

1. BGP is a very robust and scalable routing protocol.
2. CIDR is used by BGP to reduce the size of the Internet routing tables.
3. BGP easily solves the count-to-infinity problem.

Disadvantages of BGP

1. BGP is complex.
2. BGP routes to destination networks, rather than to specific hosts or routers.

3.3.4 Comparison between RIP and OSPF

Sr. No.	RIP	OSPF
1.	RIP is easy to configure.	OSPF is complicated to configure and requires network design and planning.
2.	An end system (a system with only one network interface) can run RIP in passive mode to listen for routing information.	OSPF does not have a passive mode.
3.	RIP may be slow to adjust for link failures.	OSPF is quick to adjust for link failures.
4.	RIP generates more protocol traffic than OSPF.	OSPF generates less protocol traffic than RIP.
5.	RIP is not well suited to large networks, because RIP packet size increases as the number of networks increases.	OSPF works well in large networks.
6.	RIP is distance vector routing protocol.	OSPF is link state routing protocol.

3.4 Introduction

- Multicasting means sending of a packet from one sender to multiple receivers with a single send operation. A message can be unicast, multicast or broadcast.

3.4.1 Unicast

- Protocols involving just one sender and one receiver are often referred to as unicast protocols. There is one source and one destination.
- Fig. 3.4.1 shows the unicasting.

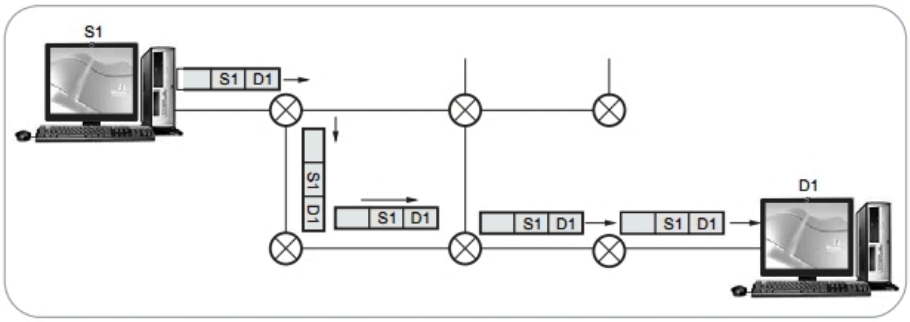


Fig. 3.4.1 Unicasting

- A unicast packet starts from the source (S1) and passes through routers to reach the destination (D1).
- In unicasting when router receives a packet, it forwards the packet through only one of its interfaces as defined in the routing table. The router may discard the packet if it cannot find the destination address in its routing table.

3.4.2 Multicast

- In multicast, there is one source and a group of destinations. The relationship is one to many.
- Fig. 3.4.2 shows the multicasting. (See Fig. 3.4.2 on next page)
- The source address is a unicast address, but the destination address is group address, which define one or more destinations.
- In multicasting, when a router receives a packet, it may forward it through several of its interfaces.
- Multicasting starts with one single packet from the source that is duplicated by the routers. The destination address in each packet is the same for all duplicates.

3.4.3 Broadcast

- In this communication, the relationship between the source and the destination is one to all. There is only one source, but all the other hosts are the destination.
- Internet is not supporting broadcasting. Broadcasting create large amount of traffic and it is wasted of bandwidth.

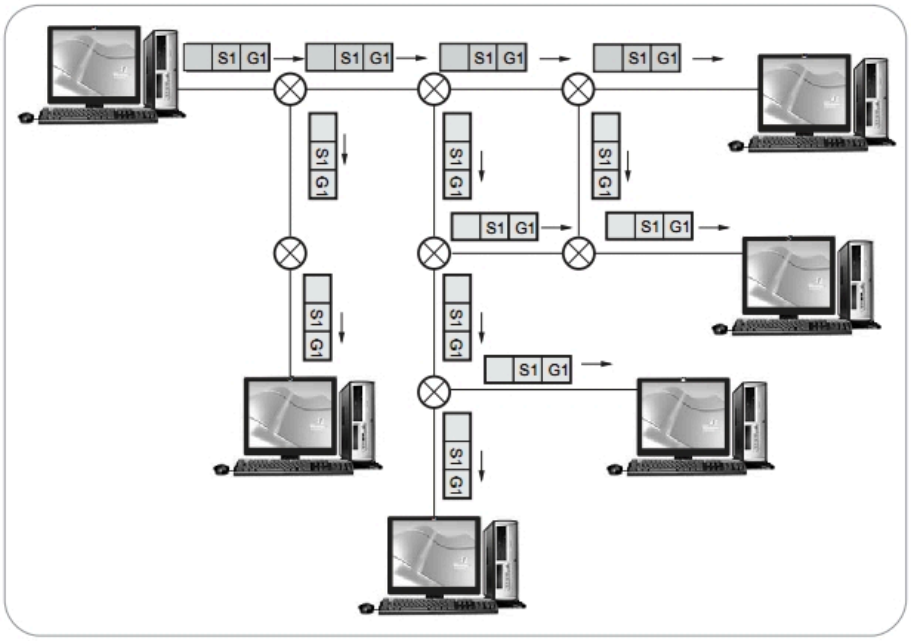


Fig. 3.4.2 Multicasting

3.5 Intra-domain Multicast Protocols

- Multicasting means sending of a packet from one sender to multiple receivers with a single send operation. A message can be unicast, multicast or broadcast.
- Multicast routing is concerned about where the packet came from.
- In multicast, there is one source and a group of destinations. The relationship is one to many.
- The source address is a unicast address, but the destination address is group address, which define one or more destinations.
- In multicasting, when a router receives a packet, it may forward it through several of its interfaces.
- Multicasting starts with one single packet from the source that is duplicated by the routers. The destination address in each packet is the same for all duplicates.

Multicast Applications

- A number of emerging network applications require the delivery of packets from one or more senders to a group of receivers. These applications includes following.
  1. Bulk data transfer - For example, the transfer of a software upgrade from the software developer to users needing the upgrade.
  2. Streaming continuous media- For example, the transfer of the audio, video and text of a live lecture to a set of distributed lecture participants.
  3. Shared data applications - For example, a white board or teleconferencing application that is shared among many distributed participants.
  4. Data feeds - For example, stock quotes.
  5. Web cache updating.

6. Interactive gaming - For example, distributed interactive virtual enviroments multiplayers games such as quake.

3.5.1 DVMRP

- Distance Vector Multicast Routing Protocol (DVMRP) is an Internet routing protocol that provides an efficient mechanism for connection-less datagram delivery to a group of hosts across an internetwork. It is a distributed protocol that dynamically generates IP multicast delivery trees using a technique called reverse path multicasting.
- DVMRP uses a distance vector distributed routing algorithm in order to build per-source-group multicast delivery trees.
- Each router maintains a 'multicast routing table' by exchanging distance vector information among routers. First multicast routing protocol ever deployed in the Internet is similar to RIP.
- It constructs a source tree for each group using reverse path forwarding. Tree provides a shortest path between source and each receiver. There is a "designated forwarder" in each subnet.
- Multiple routers on the same LAN select designated forwarder by lower metric or lower IP address. Once tree is created, it is used to forward messages from source to receivers.
- If all routers in the network do not support DVMRP then unicast tunnels are used to connect multicast enabled networks.
- Flood multicast packets based on reverse path forwarding rule to all routers. Leaf routers check and sends prune message to upstream router when no group member is on their network.
- Upstream router prunes the interface with no dependent downstream router. Graft message to create a new branch for late participants.

RPF (Reverse Path Forwarding)

- Simple algorithm developed to avoid duplicate packets on multi-access links.
- RPF algorithm takes advantage of the IP routing table to compute a multicast tree for each source.
- RPF check
  1. When a multicast packet is received, note its source (S) and interface (I).
  2. If I belongs to the shortest path from S, forward to all interfaces except I.
  3. If test in step 2 is false, drop the packet.
- Packet is never forwarded back out the RPF interface!

MBone

- MBone is multicast internet backbone. It established in 1992 with 40 subnets in 4 countries.
- Interconnected set of routers and subnets that provide IP multicast delivery in internet.
- MBone routers run a protocol to decide where to forward IP multicast packets. Routers treat MBone topology as a single flat routing domain. Entry for every subnet in the MBone.
- There is a problem of additional processing resources and memory. If nothing is done the MBone will collapse.
- Solution lies in using hierarchical distance-vector multicast routing for the MBone. Use two-level hierarchy in which the MBone is divided into regions and the regions contain subnets.
- The routing protocol in each region maintains topological information only for its own region, not for other regions.
- Problems with DVMRP-oriented approach
  1. Need to periodically flood and prune to determine group members.
  2. Need to source per-source and per-group prune records at each router.
  3. Charge routers not involved in multicast.
  4. Dependence on similarity of multicast/unicast algorithms across Internet.

3.5.2 MOSPF

- Multicast extensions to OSPF (MOSPF) provides enhancements to OSPF Version 2 to support IP multicast routing.
- MOSPF works by including multicast information in OSPF link state advertisements. An MOSPF router learns which multicast groups are active on which LANs. MOSPF builds a distribution tree for each source/group pair and computes a tree for active sources sending to the group.

- MOSPF provides the ability to forward multicast datagrams from one IP network to another through internet routers. MOSPF forwards a multicast datagram on the basis of both the datagram's source and destination.
- MOSPF is used internal to a single autonomous system. When supporting IP multicast over the entire internet, MOSPF would have to be used in concert with an inter-AS multicast routing protocol such as DVMRP.
- Routers running MOSPF works only in internetworks that are using but can be intermixed with non-multicast OSPF routers. Both types of routers can interoperate when forwarding regular (unicast) IP data traffic.

3.5.3 PIM

- PIM stands for protocol independent multicast. PIM is a multicast routing protocol that runs over an existing unicast routing infrastructure. There are two main modes in which PIM will operate in two main modes :
  1. Dense mode 2. Sparse mode.
- PIM must assume that all routers in the network are multicast enabled. It is possible for a router to manage traffic for groups that are separately using either of these modes.
- PIM-DM builds source-based trees using flood-and-prune, and is intended for large multicast groups where most networks have a group member.
- PIM-SM builds core-based trees as well as source-based trees with explicit joins.
- PIMv2 protocol messages are encapsulated in IP datagram. PIM messages can be sent as unicast or multicast packets. When sent as multicast packets, PIM uses the multicast IP address 224.0.0.13, which is reserved as the ALL-PIM-Routers group.

PIM-DM mode

- This mode assumes that all routers want to get the messages or data, so more initial data is sent out over the network.
- In the dense mode, the router assumes that all other routers want to receive multicast data for a specific group. If a router receives these packets and they are not a member of that group, it sends a prune message back to the source router for removing path.
- When running in dense mode, the prune messages time out every three minutes, at which time group messages are flooded out of all interfaces again until new prune messages are received.

PIM-SM mode

- Routers explicitly join and leave the group by using "Join" and "Leave" messages. These messages are sent to the rendezvous point node to each multicast group. A number of routers are configured to be rendezvous points. Fig. 3.5.1 shows join message.

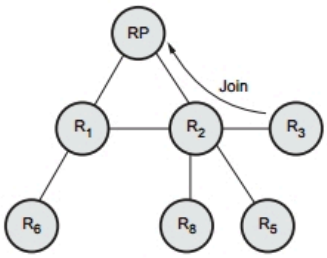


Fig. 3.5.1 Join message

- PIM has a set of procedures by which the routers in the domain can agree to use a specific node as the RP for a group. The router closest to the host receives a multicast PIM join message from the receiver device.
- Directly connected routers send the PIM join message to upstream routers between themselves and the Rendezvous Point (RP), which is a router that is a designated meeting point. The RP's job is to keep track of all multicast groups in use on the network. The RP then sends join messages upstream toward the source host.
- When a router receives the Join message, it creates a forwarding entry for the shared tree which implies, all senders for the group. It marks the interface on which the Join arrived to be the one on which packets are to be forwarded. It then also forwards the message on the right interface towards the RP. This is the only interface on which incoming packets for G are accepted. The RP receives the Join and this completes the construction of the tree branches.

3.6 Two Marks Questions with Answers

Q.1 *What is multicasting routing ?*

Ans. : Delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once.

Q.2 *Describe the difference between static and dynamic routing ?*

Ans. : Static routing is configured by the network administrator and is not capable of adjusting to changes in the network without network administrator intervention. Dynamic routing adjusts to changing network circumstances by analyzing incoming routing update messages without administrator intervention.

Q.3 *Define routing ?*

Ans. : Routing is the process of selecting paths in a network through which network traffic is sent.

Q.4 *What do you mean by unicast routing ?*

Ans. : Unicast routing is a process of forwarding unicasted traffic from a source to destination on an Internet.

Q.5 *Define source routing.*

Ans. : All the information about the network topology is required to switch a packet across the network is provided by the source host. For switching that uses neither virtual circuits nor conventional datagrams is known as source routing.

Q.6 *Define BGP.*

Ans. : Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed routing and reachability information between autonomous systems on the Internet.

Q.7 *Give the comparison of unicast, multicast and broadcast routing.*

Ans. :

Sr. No.	Unicast	Multicast	Broadcast
1.	Unicast is a type of communication where a piece of information is sent from one point to another.	The information is sent from one or more points to set of other points.	The information is sent from one point to other points.
2.	Only one sender and one receiver	One or more sender and set of receiver	One sender and several recivers.

Q.8 *What are the benefits of Open Shortest Path First (OSPF) protocol ?*

Ans. : Benefits :

1. Low traffic overhead
2. Support for complex address structures
3. Fast convergence
4. Good security. OSPF supports interface-based plaintext and MD5 authentication
5. Area based topology. Large OSPF networks are organized as a set of areas linked by a backbone.

❑❑❑

UNIT - IV

4 TRANSPORT LAYER PROTOCOLS

4.1 User Datagram Protocol (UDP)

- UDP is a simple, datagram-oriented, transport layer protocol. This protocol is used in place of TCP. UDP is connectionless protocol provides no reliability or flow control mechanisms. It also has no error recovery procedures.
- Several application layer protocols such as TFTP (Trivial file transfer protocol) and the RPC use UDP. UDP makes use of the port concept to direct the datagrams to the proper upper-layer applications. UDP serves as a simple application interface to the IP.

4.1.1 User Datagram

- Fig. 4.1.1 (a) shows the encapsulation of a UDP datagram as an IP datagram.

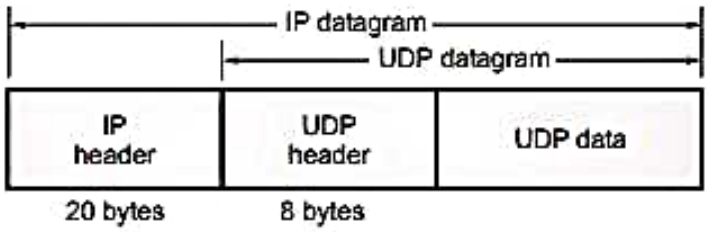


Fig. 4.1.1 (a) UDP encapsulation

- Fig. 4.1.1 (b) shows the format of the UDP header. The port number identify the sending process and the receiving process.
- The UDP datagram contains a source port number and destination port number. Source port number identifies the port of the sending application process. The destination port number identifies the receiving process on the destination host machine.

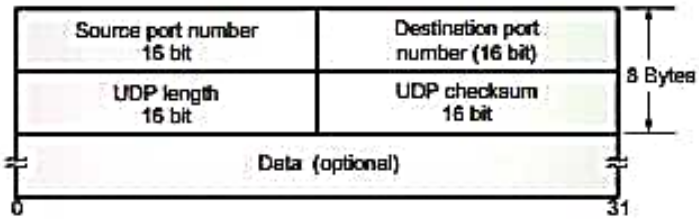


Fig. 4.1.1 (b) UDP header

- The UDP length field is the length of the UDP header and the UDP data in bytes. The minimum value for this field is 8 bytes.
- UDP checksum covers the UDP header and the UDP data. Both UDP and TCP include a 12 byte pseudo-header with the UDP datagram just for the checksum computation. This pseudo_header includes certain fields from the IP header. The purpose is to let UDP double check that the data has arrived at the correct destination.
- UDP checksum is end-to-end checksum. It is calculated by the sender, and then verified by receiver. It is designed to catch any modification of the UDP header or data anywhere between sender and receiver.
- Goal of the UDP checksum is to detect "errors" in transmitted segment. Function performed by sender and receiver is as follows :

Sender :

1. Treat segment contents as sequence of 16-bit integers

2. Checksum : addition (1's complement sum) of segment contents
3. Sender puts checksum value into UDP checksum field

Receiver :

1. Compute checksum of received segment
2. Check if computed checksum equals checksum field value : NO - error detected and YES - no error detected.

Why is there a UDP ?

1. No connection establishment (which can add delay)
2. Simple : no connection state at sender, receiver
3. Small segment header
4. No congestion control : UDP can blast away as fast as desired
5. Often used for streaming multimedia apps

4.1.2 UDP Services

- UDP services includes following :

1. Process-to-Process Communication - UDP provides process-to-process communication using **socket addresses**, a combination of IP addresses and port numbers.
2. Connectionless Service-UDP provides a connectionless service, i.e. each user datagram sent by UDP is an independent datagram.
3. UDP provides no flow control.
4. UDP does not provides no error control.
5. UDP does not provide congestion control.
6. UDP protocol encapsulates and decapsulates messages.
7. Queueing - Queues are associated with ports.
8. Multiplexing and demultiplexing-UDP provides multiplexing and demultiplexing of processes.

4.1.3 Ports for UDP

- UDP uses port numbers as the addressing mechanism in the transport layer.
- Following is the list of well-known port number used by UDP.

Port No.	Protocol	Description
7	Echo	Echoes a received datagram back to the sender.
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns the quote of the day
19	Chargen	Returns a string of characters
53	Nameserver	Domain Name Service
67	Bootps	Server port to download bootstrap information
68	Bootpc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol

4.1.4 UDP Applications

1. UDP is used for some route updating protocols such as RIP.
2. UDP is used for multicasting.
3. It is suitable for a process with internal flow and error control mechanisms.

Board Questions

1. *Write abbreviation / Acronym of following :*
   (i) SLIP (ii) PPP (iii) ARP (iv) RARP
   (v) FTP (vi) SMTP (vii) DNS (viii) UDP

   MSBTE : Summer-16, Marks 4

2. *Explain the various fields in the frame format of UDP with a neat diagram.*

   MSBTE : Winter-16, Marks 4

4.2 Transmission Control Protocol (TCP)

- Transmission Control Protocol (TCP) is the connection oriented protocol whereas User Data Protocol (UDP) is connectionless protocol. Both are internet protocols used in the transport layer.
- TCP provides a connection-oriented, reliable, byte stream service. The term connection oriented means the two applications using TCP must establish a TCP connection with each other before they can exchange data.

4.2.1 TCP Services

- TCP and UDP use the same network layer (IP), TCP provides totally different services. TCP provides a connection-oriented, reliable, byte stream service. There are exactly two end points communicating with each other on a TCP connection.
- TCP does not support multicasting and broadcasting. The application data is broken into what TCP considers the best sized chunks to send. The unit of information passed by TCP to IP is called a segment.
- When TCP sends a segment it maintains a timer, waiting for the other end to acknowledge reception of segment. If an acknowledgement isn't received in time, the segment is retransmitted.
- When TCP receives data from the other end of the connection, it sends an acknowledgement. TCP maintains a checksum on its header and data.
- TCP segments are transmitted as IP datagrams, and since IP datagrams can arrive out of order, TCP segments can arrive out of order. Since IP datagrams can get duplicated, a receiving TCP must discard duplicate data.
- TCP also provides flow control. Each end of a TCP connection has a finite amount of buffer space. A receiving TCP only allows the other end to send as much data as the receiver has buffers for. This prevents a fast host from taking all the buffers on a slower host.
- A TCP connection is a byte stream, not a message stream. A stream of 8-bit bytes is exchanged across the TCP connection between the two applications. There are no record markers automatically inserted by TCP. This is called a **byte stream service.**
- If the application on one end writes 20 bytes followed by a write of 40 bytes, followed by a write of 80 bytes, the application at the other end of the connection cannot tell what size the individual writes there. The other end may read 140 bytes ones at a time or 140 bytes in two reads of 70 bytes at a time.
- TCP does not interpret the contents of the bytes at all. TCP has no idea if the data bytes being exchanged are binary data, ASCII character or any other.

4.2.2 TCP Features

- TCP features are listed below.
  1. TCP is connection oriented protocol.
  2. All TCP connections are full-duplex and point-to-point.
  3. TCP provides a byte stream.
  4. Every byte has its own 32 bit sequence number.
  5. Sending and receiving entities exchange data in segments
  6. Each segment is the 20 byte header and data.
  7. TCP does not support multicasting and broadcasting.

4.2.3 TCP Header

- The TCP data is encapsulated in an IP datagram as shown in the Fig. 4.2.1 (a).

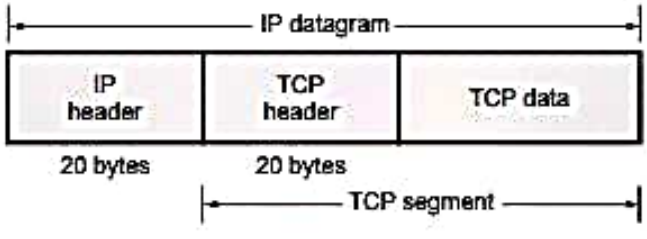


Fig. 4.2.1 (a) Encapsulation of TCP data in an IP datagram

- Fig. 4.2.1 (b) shows the format of the TCP header.
- Description of field in the TCP header as follows :

1. **Source port** : It specifies the application sending the segment. This is different from the IP address, which specifies an internet address.
2. **Destination port** : It identifies the receiving application port numbers below 256 are called well-known ports and have assigned to commonly used applications. For examples, port 23 corresponds to a Telnet function. Port 53 for DNS name server and port 21 assigned for FTP.
3. **Sequence number** : Each byte in the stream that TCP sends is numbered. The sequence number wraps back to 0 after $2^{32} - 1$.
4. **Acknowledgement number** : This field identifies the sequence number of the next data by the that the sender expects to receive if the ACK bit is set. If the ACK bit is not set, this field has no effect.
5. **Header length** : It specifies the length of the TCP header in 32-bit words. Because of option field, header length is used.
6. **Reserved** : This field is reserved for future use and must be set to 0 (zero).
7. TCP header contains six flag bits. One or more than one can be turned on at the same time. The function of each flag is as follows.
   a. **URG** : The Urgent pointer is valid if it set to 1.
   b. **ACK** : ACK bit is set to 1 to indicate that the acknowledgment number is valid.
   c. **PSH** : The receiver should pass this data to the application as soon as possible.
   d. **RST** : This flag is used to reset the connection. It is also used to reject an invalid segment.
   e. **SYN** : Synchronize sequence number to initiate a connection. The connection request has SYN = 1 and ACK = 0 to indicate that the piggyback acknowledgement field is not in use.
   f. **FIN** : The FIN bit is used to release a connection. It specifies that the sender is finished sending data.
8. **Window size** : It specifies the number of bytes the sender is willing to accept. This field can be used to control the flow of data and congestion.

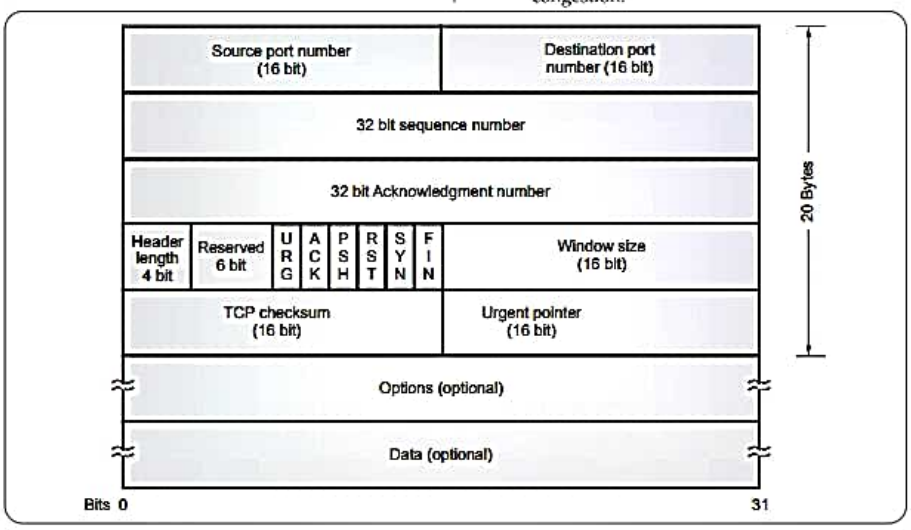


Fig. 4.2.1 (b) TCP header format

9. **Checksum :** Used for transport layer error detection.
10. **Urgent pointer :** If the URG flag bit is set, the segment contains urgent data meaning the receiving TCP entity must deliver it to the higher layers immediately.
11. **Options :** Size of this field is variable options field may be used to provide other functions that are not covered by the header.
12. **Data :** Data field size is variable. It contains user data.

- TCP header normal size is 20 bytes, unless options are present. Each TCP segment contains the source and destination port number to identify the sending and receiving application.
- The port number alongwith the source and destination IP addresses in the IP header, uniquely identify each connection. The combination of an IP address and a port number is sometimes called a **socket**.
- Sequence number is a 32-bit unsigned number. Sequence number identifies the byte in the stream of data from sending TCP to the receiving TCP that the first byte of data in this segment represents.
- When a new connection is being established, the SYN flag is turned on. The sequence number of the first byte of data sent by this host will be the ISN plus one because, the SYN flag consumes a sequence number.
- Every byte that is exchanged is numbered, the acknowledgement number contains the next sequence number that the sender of the acknowledgement excepts to receive. Therefore the sequence number plus 1 of the last successfully received byte of data. This field is valid only if the ACK flag is on.
- TCP provides full duplex service. Therefore, each end of a connection must contain a sequence number of the data flowing in each direction.
- TCP can be described as a sliding window protocol without selective or negative acknowledgements.
- The TCP header length tells how many 32-bit words are contained in the TCP header. This information is needed because the options field is of variable length with a 4-bit field, TCP is limited to a 60-byte header. Without options, the normal size is 20 bytes.
- TCP's flow control is handled using a variable size sliding window. This is the number of bytes, starting with the one specified by the acknowledgement number field, that the receiver is willing to accept.
- This is a 16-bit field, limiting the window to 65535 bytes.
- The checksum covers the TCP segment, the TCP header and the TCP data. Checksum field must be calculated and stored by the sender and then verified by the receiver.
- The urgent pointer is valid only if the URG flag is set. This pointer is a positive offset that must be added to the sequence number field of the segment to yield the sequence number of the last byte of urgent data. Option field is the maximum segment size option, called the Maximum Segment Size (MSS). MSS is the largest chunk of data that TCP will send to the other end.

4.2.4 TCP Protocol

- Sending and receiving TCP entities exchange data in the form of segments. A TCP segment consists of a fixed 20-byte header followed by zero or more data bytes.
- TCP software decides how big segments should be. Two limits restrict the segment size.
  1. Each segment including the TCP header must fit in the 65515 bytes IP payload.
  2. Each network has a Maximum Transfer Unit (MTU) and each segment must fit in the MTU.
- The basic protocol used by TCP entities is the sliding window protocol.

4.2.5 TCP Connection Establishment

- Connection establishment in a TCP session is initialized through a three-way handshake. To establish the connection, one side (server) passively waits for an incoming connection by executing the LISTEN and ACCEPT primitives, either specifying a specific source.
- Other side (client) executes a CONNECT primitive specifying the IP address and port to which it wants to connect, the maximum TCP segment size it is willing to accept, and optionally some user data.

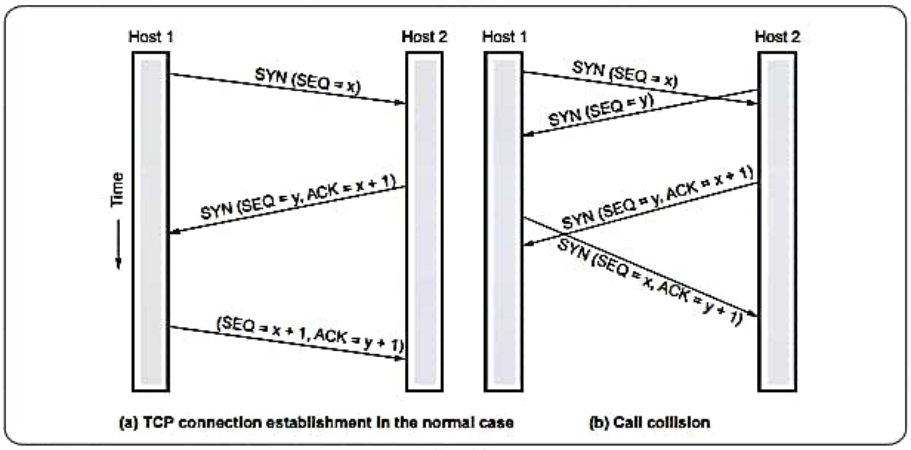


Fig. 4.2.2

- Fig 4.2.2 shows the TCP connection establishment in the normal case and call collision.
- A connection is established using a three-way handshake.
- The transmitter sends Connection Request (seq = x) to start a connection with transmitter message id x.
- The receiver replies Connection Accepted (seq = y, ACK = x+1), to acknowledge x and establish for its messages the identity y.
- Finally the transmitter confirms the connection with Connection Accepted (seq = x+1, ACK = y+1) to confirm its own identifier x and accept the receiver's identifier y.
- If the receiver wanted to reject x, it would send Reject(ACK = x).
- If the transmitter wanted to reject y it would send Reject(ACK = y).
- As part of the handshake the transmitter and receiver specify their MSS (Maximum Segment Size) that is the maximum size of a segment they can accept. A typical value for MSS is 1460.
- TCP connections are full duplex. The steps required establishing and release connections can be represented in a finite state machine.

Problem regarding 2-way handshake

- The only real problem with a 2-way handshake is that duplicate packets from a previous connection between the two nodes might still be floating on the network. After a SYN has been sent to the responder, it might receive a duplicate packet of a previous connection and it would regard it as a packet from the current connection which would be undesirable.
- Again spoofing is another issue of concern if a two way handshake is used. Suppose there is a node C which sends connection request to B saying that it is A. Now B sends an ACK to A which it rejects and asks B to close connection. Between these two events C can send a lot of packets which will be delivered to the application.

Three-way handshake

- The three-way handshake is the procedure used to establish a connection. This procedure normally is initiated by one TCP and responded to by another TCP.
- The three-way handshake involves the exchange of three messages between the client and the server.
- The procedure also works if two TCP simultaneously initiate the procedure. When simultaneous attempt occurs, each TCP receives a "SYN" segment which carries no acknowledgment after it has sent a "SYN". Of course, the arrival of an old duplicate "SYN" segment can potentially make it appear, to the recipient that a simultaneous

connection initiation is in progress. Proper use of "reset" segments can disambiguate these cases.

- The three-way handshake reduces the possibility of false connections. It is the implementation of a trade-off between memory and messages to provide information for this checking.
- Fig. 4.2.3 shows the three way handshake scenario for establishing a connection.

Normal Operation

- Host 1 select a sequence number, 'x' and sends a CONNECTION REQUEST TPDU containing it to Host 2. Host 2 replies with an ACK TPDU acknowledging 'x' and announcing its own initial sequence number 'y'.
- Host 1 acknowledges Host 2's choice of an initial sequence number in the first data TPDU that it sends.
- This is shown in Fig. 4.2.3 (a).

Old Duplicate

- The first TPDU is a delayed duplicate CONNECTION REQUEST from an old connection. This TPDU arrives at Host 2 without Host 1's knowledge.
- Host 2 sends ACK TPDU to Host 1 and ask for verification.

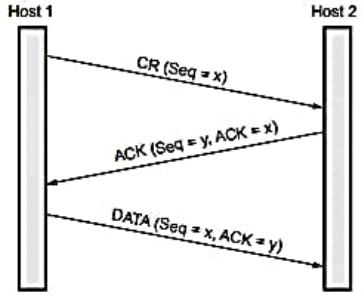


Fig. 4.2.3 (a) Normal operation

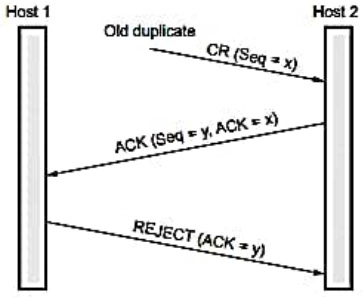


Fig. 4.2.3 (b) Old duplicate CR

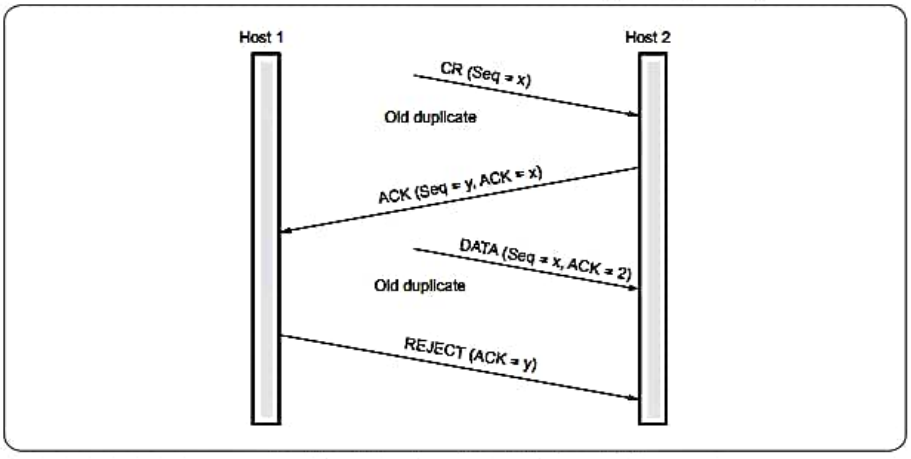


Fig. 4.2.3 (c) Duplicate CR and duplicate ACK

Fig. 4.2.3 Connection establishing using three-way handshake

- When Host 1 rejects Host 2's attempt to establish a connection, Host 2 realizes that it was tricked by a delayed duplicate and abandons the connection.
- So, the delay duplicate does no damage.
- For this, refer Fig. 4.2.3 (b).

Duplicate CR and Duplicate ACK

- When both a delayed CONNECTION REQUEST and an ACK are floating around in the subnet.
- Host 2 gets a delayed CONNECTION REQUEST and replies to it.
- When the second delayed TPDU arrives at Host 2, the fact that 'Z' has been acknowledged rather than 'y' tells Host 2 that this, too, is an old duplicate.

4.2.6 TCP Connection Release

- Any of the two parties involved in exchanging data can close the connection. When connection in one direction is terminated, the other party can continue sending data in the other direction.
- Four steps are required to close the connection in both direction. Fig. 4.2.4 shows four step connection termination.
- Steps are as follows
  1. The client TCP sends the first segment, a FIN segment.
  2. The server TCP sends the second segment, an ACK segment, to confirm the receipt of the FIN segment from the client.
  3. The server TCP can continue sending data in the server client direction. When it does not have any more data to send, it sends the third segment.
  4. The client TCP sends the fourth segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server.
- Connection release is easier than connection establishing. Connection releases are of two types : Symmetric release and Asymmetric release.
- Asymmetric release is abrupt and may result in data loss. One way to avoid data loss is to use symmetric release, in which each direction is released independently of the other one.
- Fig. 4.2.5 shows the abrupt disconnection with loss of data.

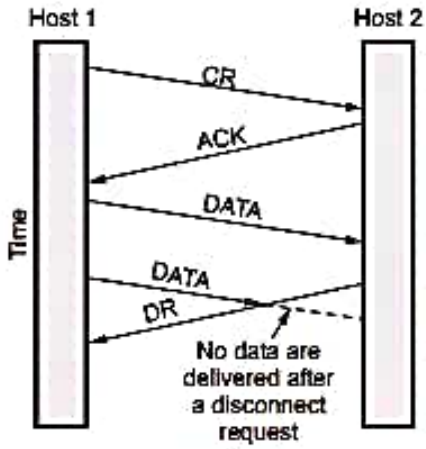


Fig. 4.2.5 Abrupt disconnection with loss of data

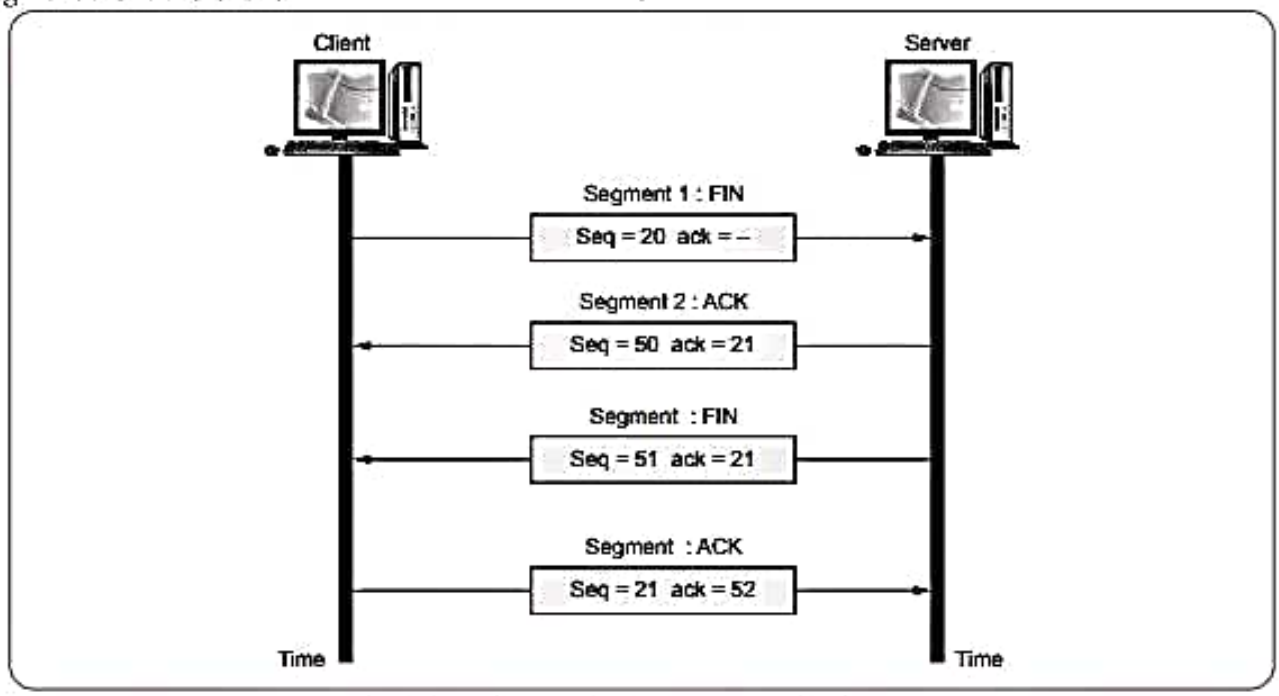


Fig. 4.2.4 Four steps connection termination

- After connection is established, Host 1 sends a TPDU that arrives properly at Host 2. Then Host 1 sends another TPDU.
- Unfortunately, Host 2 issues a DISCONNECT before the second TPDU arrives. The result is that the connection is released and data are lost.
- A more sophisticated release protocol is required to avoid data loss.

says:"I am done. Are you done too ?"

If responds: "I am done too. Goodbye."

This way does not always work.

- One way to avoid data loss is to use symmetric release, in which each direction is released independently of the other one.

Two army problem

- A white army is encamped in a valley.
- On both of the surrounding hillsides are blue armies.
- The white army is larger than either of the blue armies alone, but together they are larger than the white army.
- If either blue army attacks by itself, it will be defeated, but if the two blue armies attack simultaneously, they will be victorious.
- The communication medium between the two blue armies is to send messengers on foot down into the valley, where they might be captured and the message lost.
- Fig. 4.2.6 show the two army problem.
- The question is, does a protocol exist that allows the blue armies to win ?
- The answer is there is NO such protocol exists.
- Just substitute "disconnect" for "attack". If neither side is prepared to disconnect until it is convinced that the other side is prepared to disconnect too, the disconnection will never happen.
- In practice, one is usually prepared to take more risks when releasing connections than attacking white armies, so the situation is not entirely hopeless.
- Fig. 4.2.7 shows four protocol scenarios for releasing a connection.

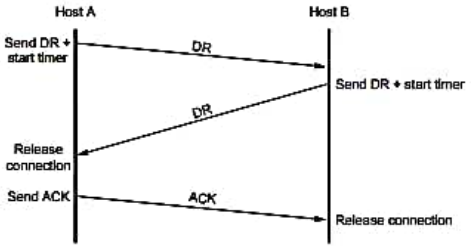


Fig. 4.2.7 (a) Releasing Connection

a) Normal case of three way handshake

- One of the user sends a DR (DISCONNECTION REQUEST) TPDU to initiate the connection release. When it arrives, the receipent sends back and DR TPDU and start a timer. When this DR arrives, the original sender sends back an ACK TPDU and releases the connection. Finally, when the ACK TPDU arrives, the receiver also releases the connection.

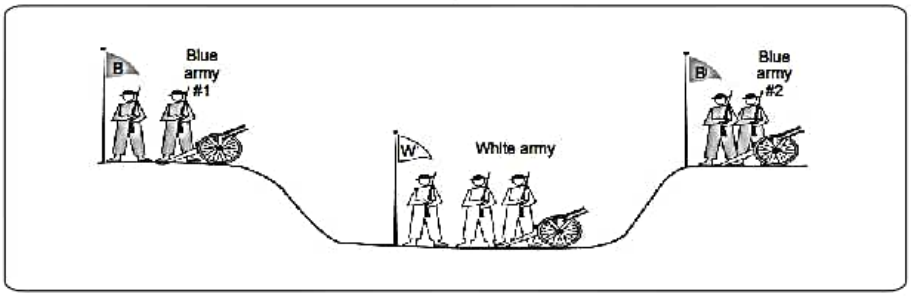


Fig. 4.2.6 Two army problem

- After connection is established, Host 1 sends a TPDU that arrives properly at Host 2. Then Host 1 sends another TPDU.
- Unfortunately, Host 2 issues a DISCONNECT before the second TPDU arrives. The result is that the connection is released and data are lost.
- A more sophisticated release protocol is required to avoid data loss.

says:"I am done. Are you done too ?"

If responds: "I am done too. Goodbye."

This way does not always work.

- One way to avoid data loss is to use symmetric release, in which each direction is released independently of the other one.

Two army problem

- A white army is encamped in a valley.
- On both of the surrounding hillsides are blue armies.
- The white army is larger than either of the blue armies alone, but together they are larger than the white army.
- If either blue army attacks by itself, it will be defeated, but if the two blue armies attack simultaneously, they will be victorious.
- The communication medium between the two blue armies is to send messengers on foot down into the valley, where they might be captured and the message lost.
- Fig. 4.2.6 show the two army problem.
- The question is, does a protocol exist that allows the blue armies to win ?
- The answer is there is NO such protocol exists.
- Just substitute "disconnect" for "attack". If neither side is prepared to disconnect until it is convinced that the other side is prepared to disconnect too, the disconnection will never happen.
- In practice, one is usually prepared to take more risks when releasing connections than attacking white armies, so the situation is not entirely hopeless.
- Fig. 4.2.7 shows four protocol scenarios for releasing a connection.

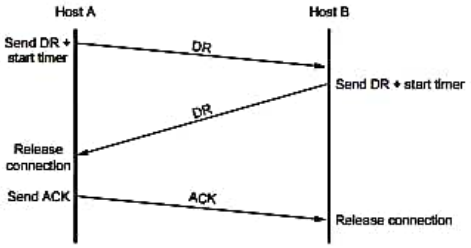


Fig. 4.2.7 (a) Releasing Connection

a) Normal case of three way handshake

- One of the user sends a DR (DISCONNECTION REQUEST) TPDU to initiate the connection release. When it arrives, the receipent sends back and DR TPDU and start a timer. When this DR arrives, the original sender sends back an ACK TPDU and releases the connection. Finally, when the ACK TPDU arrives, the receiver also releases the connection.

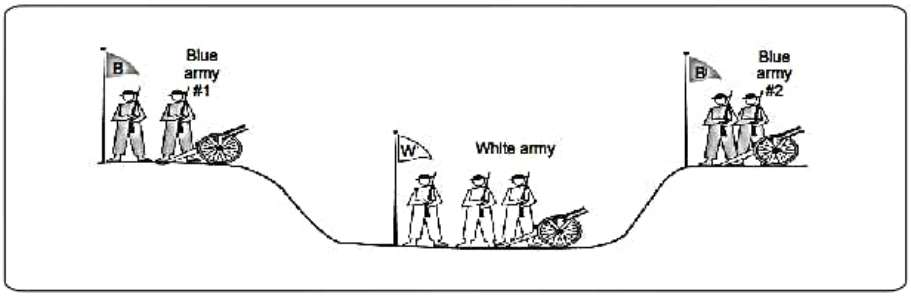


Fig. 4.2.6 Two army problem

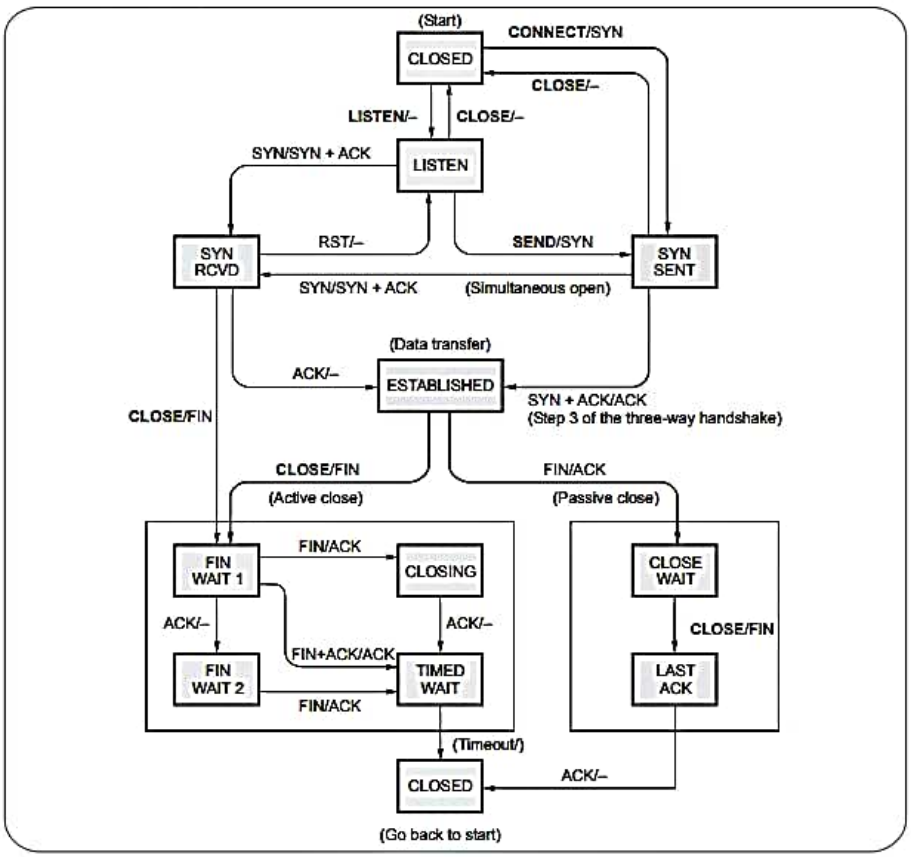


Fig. 4.2.8 TCP finite state machine

three-way handshake and switches into the ESTABLISHED state data can now be sent and received.

- When an application is finished, it executes a CLOSE primitive, which causes the local TCP entity to send a FIN segment and wait for the corresponding ACK (dashed box marked active close).
- When the ACK arrives, a transition is made to state FIN WAIT 2 and one direction of the connection is now closed. When the other side closes, too, a FIN comes in, which is acknowledged. Now both sides are closed, but TCP waits a time equal to the maximum packet lifetime to guarantee that all packets from the connection have died off, just in case the acknowledgement was lost. When the timer goes off, TCP deletes the connection record.
- Connection management from server view point, sever does a LISTEN and settles down to see who turns up. When a SYN comes in, it is acknowledged and the server goes to the SYN ACK state. When the server's SYN is itself acknowledged, the three way handshake is complete and the server goes to the ESTABLISHED state. Data transfer can now occur.

4.2.8 TCP Transmission Policy

- Fig. 4.2.9 shows window management in TCP.

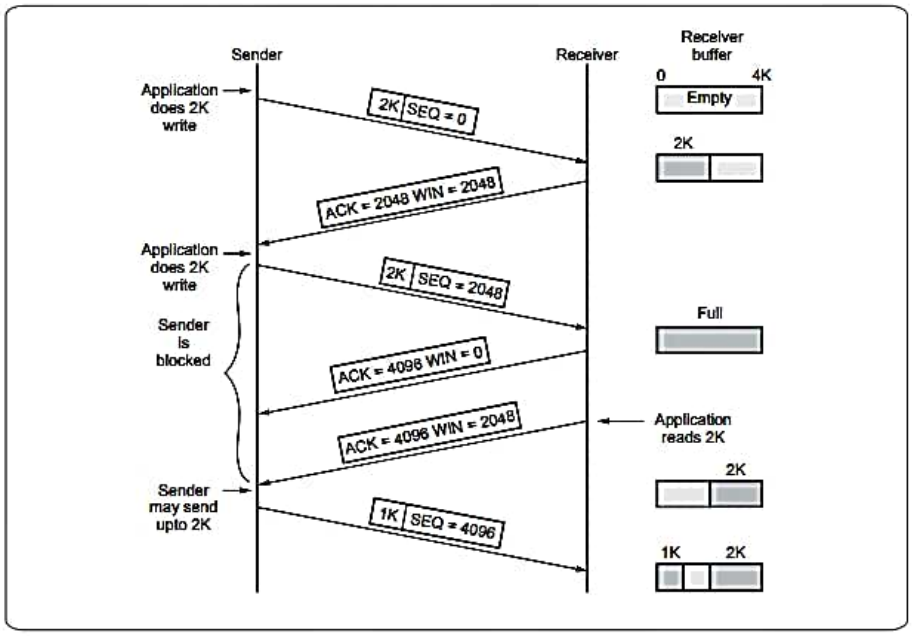


Fig. 4.2.9 Window management in TCP

- Let us assume that receiver buffer size is 4096-byte.
- If the sender transmits a 2048-byte segment that is correctly received, the receiver will acknowledge the segment.
- 2048 bytes of buffer space is only available and it will advertise a window of 2048 starting at the next byte expected.
- Again sender transmit one more 2048 bytes, which are acknowledged, but the advertised window size 0 (zero).
- Sender must stop until the application process has removed some data from the buffer.
- When the window is 0, the sender may not normally send segments because of two reasons :

1. Urgent data may be sent.
2. Sender may send a 1-byte segment to make the receiver reannounce the next byte excepted and window size.

4.2.4 Silly Window Syndrome

- When large block of data is passed from sender but the receiver reads data one byte at a time. Receiving side, the TCP buffer is full and the sender know the condition. The interactive application reads one character from the TCP stream.
- Receiving TCP tells to the sender to send the only 1 byte. Sender send 1 byte. Now buffer is full and receiver send acknowledgement the 1-byte segment and set the window 0. This operation is continuous. Fig. 4.2.10 shows these steps.
- Nagle algorithm and Clark's solution to the silly window syndrome are complementary. Clark solution is to prevent the receiver from sending a window update for 1 byte. Instead it is forced to wait until it has a decent amount of space available.

4.2.10 TCP Timer Management

- TCP manages four different timers for each connection.
  a) A **retransmission timer** is used when excepting an acknowledgement from the other end.
  b) A **persist timer** keeps window size information flowing even if the other end closes its receiver window.
  c) A **keep alive timer** detects when the other end on an otherwise idle connection crashes.
  d) A **2 maximum segment lifetime** (2 MSL) timer measures the time a connection has been in the TIME_WAIT state.
- Fundamental to TCP timeout and retransmission is the measurement of the Round-Trip Time (RTT) experienced on a given connection. The TCP must measure the RTT between sending byte with a particular sequence number and receiving an acknowledgement that covers that sequence number.
- For each connection, TCP maintains a variable RTT, that is the best current estimate of the round-trip time to the destination. When a segment is sent, a timer is started, both to see how long the acknowledgement takes and to trigger a retransmission if it takes too long.

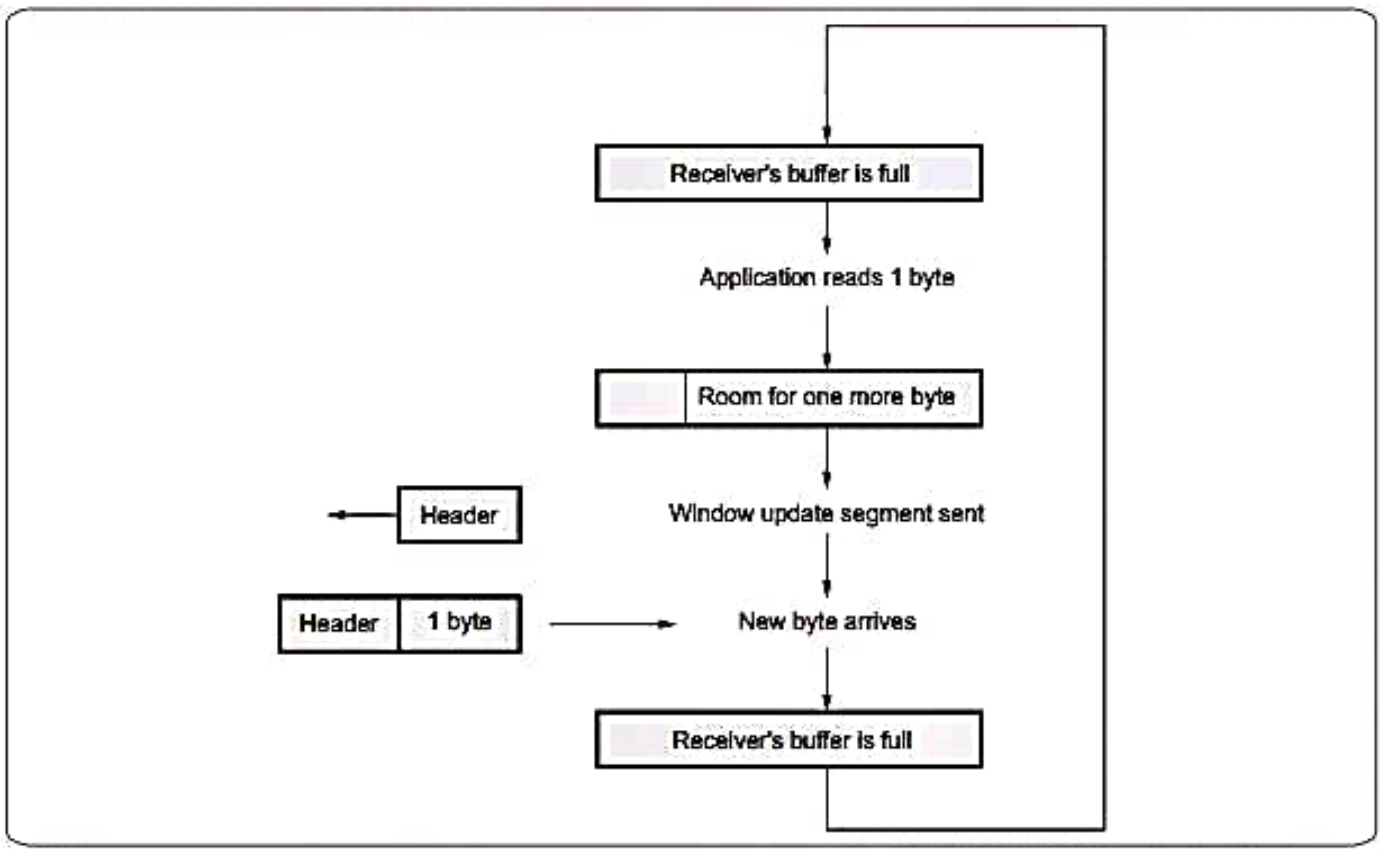


Fig. 4.2.10 Silly window syndrome

- If the acknowledgement get back before the timer expires, TCP measures how long the acknowledgement took i.e. M. The original TCP specification had TCP update a smoothed RTT estimator (R) using low-pass filter.

$$R \leftarrow \alpha R + (1-\alpha) M$$

where α is a smoothing factor with a recommended value 0.9. This smoothed RTT is updated every time when a new measurement is made. For given this smoothed estimator, which changes as the RTT changes, the retransmission timeout value (RTO) be set to

$$RTO = R\beta$$

where β = Delay variance factor with a recommended value 2.

- Unnecessary retransmission add to the network load, when the network is already loaded. Calculating the RTO based on both the mean and variance provide much better response to wide fluctuation in the round-trip time, than just calculating the RTO as a constant multiple of the mean. As described by Jacobson the mean deviation is a good approximation to the standard deviation, but easier to compute. This leads to the following equations that are applied to each RTT measurement M.

$$E_{rr} = M - A$$

$$A \leftarrow A + g E_{rr}$$

$$D \leftarrow D + h(|E_{rr}| - D)$$

$$RTO = A + 4D$$

where A = Smoothed RTT (estimator of average)

D = Smoothed mean deviation

E_{rr} = Difference between the measured value just obtained and the current RTT and estimator.

g = Gain

h = Gain of deviation

- Both A and D are used to calculate the next Retransmission Time Out (RTO). The gain (g) is for the average and is set to 0.125 and h is set to 0.25. The larger gain for the deviation makes the RTO go up faster when the RTT changes.

a) Karn's algorithm :

- A problem occurs when a packet is retransmitted. If the packet is retransmitted, a timeout occurs, the RTO is backed off. The packet is retransmitted with the longer RTO and an acknowledgement is received. The received acknowledgement is whether the first transmission or the second. This is called the retransmission ambiguity problem.
- Karn's algorithm specify that when a timeout and retransmission occur, we cannot update the RTT estimator when the acknowledgement for the retransmitted data finally arrives. Since the data was retransmitted, and the exponential back off has been applied to the RTO, we reuse this backed off RTO for the next transmission. Do not calculate a new RTO until an acknowledgement is received for a segment that was not retransmitted.

4.2.11 TCP Congestion Control

- When the load offered to any network is more than it can handle, congestion builds up. When a connection is established, the sender initializes the congestion window to the size of the maximum segment in use on the connection.
- When the congestion window is 'n' segments, if all 'n' are acknowledged on time, the congestion window is increased by the byte count corresponding to 'n' segments. In effects, each burst acknowledged doubles the congestion window.
- The congestion window keeps growing exponentially until either a timeout occurs or the receiver's window is reached.
- The Internet congestion control algorithm uses the threshold parameter which is initially 64 kB, in addition to the receiver and congestion windows. When a timeout occurs, the threshold is set to half of the current congestion window, and the congestion window is reset to one maximum segment.

- If the acknowledgement get back before the timer expires, TCP measures how long the acknowledgement took i.e. M. The original TCP specification had TCP update a smoothed RTT estimator (R) using low-pass filter.

$$R \leftarrow \alpha R + (1-\alpha) M$$

where α is a smoothing factor with a recommended value 0.9. This smoothed RTT is updated every time when a new measurement is made. For given this smoothed estimator, which changes as the RTT changes, the retransmission timeout value (RTO) be set to

$$RTO = R\beta$$

where β = Delay variance factor with a recommended value 2.

- Unnecessary retransmission add to the network load, when the network is already loaded. Calculating the RTO based on both the mean and variance provide much better response to wide fluctuation in the round-trip time, than just calculating the RTO as a constant multiple of the mean. As described by Jacobson the mean deviation is a good approximation to the standard deviation, but easier to compute. This leads to the following equations that are applied to each RTT measurement M.

$$E_{rr} = M - A$$

$$A \leftarrow A + g E_{rr}$$

$$D \leftarrow D + h(|E_{rr}| - D)$$

$$RTO = A + 4D$$

where A = Smoothed RTT (estimator of average)

D = Smoothed mean deviation

E_{rr} = Difference between the measured value just obtained and the current RTT and estimator.

g = Gain

h = Gain of deviation

- Both A and D are used to calculate the next Retransmission Time Out (RTO). The gain (g) is for the average and is set to 0.125 and h is set to 0.25. The larger gain for the deviation makes the RTO go up faster when the RTT changes.

a) Karn's algorithm :

- A problem occurs when a packet is retransmitted. If the packet is retransmitted, a timeout occurs, the RTO is backed off. The packet is retransmitted with the longer RTO and an acknowledgement is received. The received acknowledgement is whether the first transmission or the second. This is called the retransmission ambiguity problem.
- Karn's algorithm specify that when a timeout and retransmission occur, we cannot update the RTT estimator when the acknowledgement for the retransmitted data finally arrives. Since the data was retransmitted, and the exponential back off has been applied to the RTO, we reuse this backed off RTO for the next transmission. Do not calculate a new RTO until an acknowledgement is received for a segment that was not retransmitted.

4.2.11 TCP Congestion Control

- When the load offered to any network is more than it can handle, congestion builds up. When a connection is established, the sender initializes the congestion window to the size of the maximum segment in use on the connection.
- When the congestion window is 'n' segments, if all 'n' are acknowledged on time, the congestion window is increased by the byte count corresponding to 'n' segments. In effects, each burst acknowledged doubles the congestion window.
- The congestion window keeps growing exponentially until either a timeout occurs or the receiver's window is reached.
- The Internet congestion control algorithm uses the threshold parameter which is initially 64 kB, in addition to the receiver and congestion windows. When a timeout occurs, the threshold is set to half of the current congestion window, and the congestion window is reset to one maximum segment.

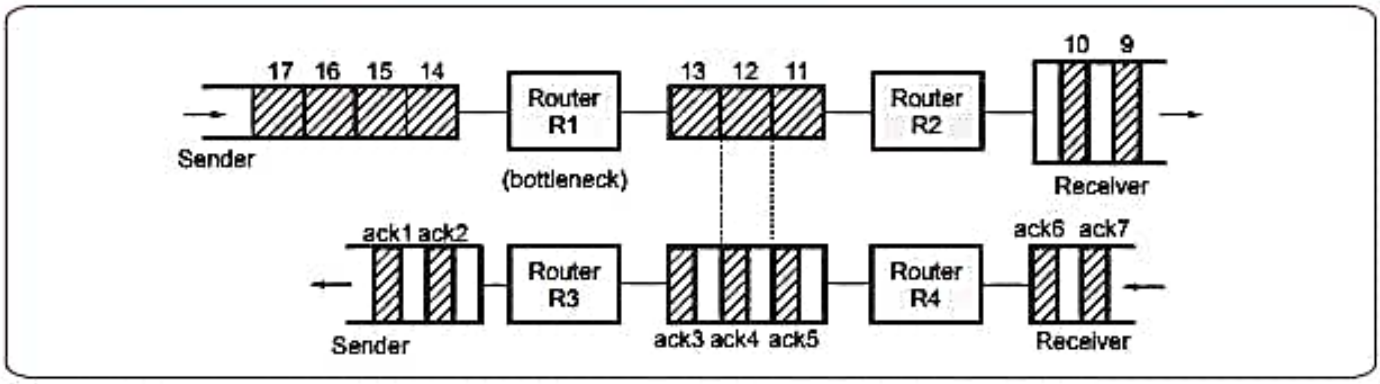


Fig. 4.2.12 Congestion caused by fast LAN sending a slow WAN

- Fig. 4.2.12 shows the one typical example for TCP congestion.
- The Router R1 is labelled as the bottleneck because it is the congestion point. Router R1 can receive packets from the LAN on its left faster than they can be sent out the WAN on its right.
- When router R2 put the received packets onto the LAN on its right, they maintain the same spacing as they did on the WAN on its left, eventhough the bandwidth of the LAN is higher.
- Slow start is the way to initiate data flow across a connection. *Congestion avoidance* is a way to deal with lost packets.

4.2.12 TCP Flow Control

- TCP interactive data flow uses Rlogin application. In TCP/IP the each interactive keystroke normally generates a data packet. The keystrokes are sent from the client to the server 1 byte at a time. Rlogin has the remote system; each characters that the client type is displayed on the other side (server).
- Fig. 4.2.13 shows the flow of data.
- The TCP acknowledgements operates as follows.

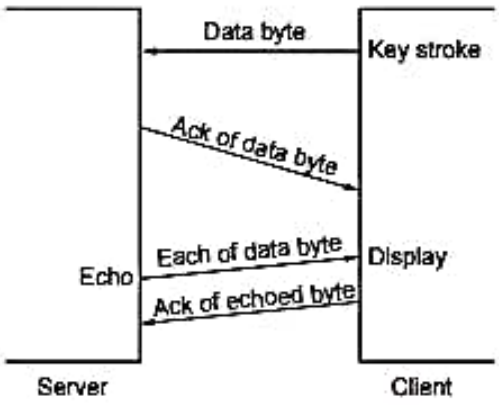


Fig. 4.2.13 Remote echo of interactive keystroke

- Line 1 sends the data byte with the sequence number 0. Line 2 ACKs this by setting the acknowledgement sequence number to 1, the sequence number of the last successfully received byte plus one. This is also called the sequence number of the next excepted byte.
- Line 2 also sends the data byte with a sequence number of 1 from the server to the client. This is ACKed by the client in line 3 by setting the acknowledgement sequence number to 2. Normally TCP does not send an ACK the instant it receives data. Instead, it delays the ACK, hoping to have data going in the same direction as the ACK, so the ACK can be sent alongwith the data. TCP will delay an ACK upto 200 ms to see if there is data to send with the ACK.

NAGLE algorithm :

- One byte at a time normally flows from the client to the server across a Rlogin connection. This generates 41-byte packet 20 bytes for the IP header and 20 bytes for TCP header and 1 byte of data. These small packets called as tinygrams. These tinygrams can add to congestion on WAN.
- Most LANs are not congested because tinygrams are not a problem on LANs. To solve the problem of congestion of WAN, the Nagle algorithm is used.
- The Nagle algorithm say that when TCP connection has outstanding data that has not yet been acknowledged, small segments cannot be sent until the outstanding data is acknowledged. Instead, small amounts of data are collected by TCP and sent in a single segment when the acknowledgement arrives.

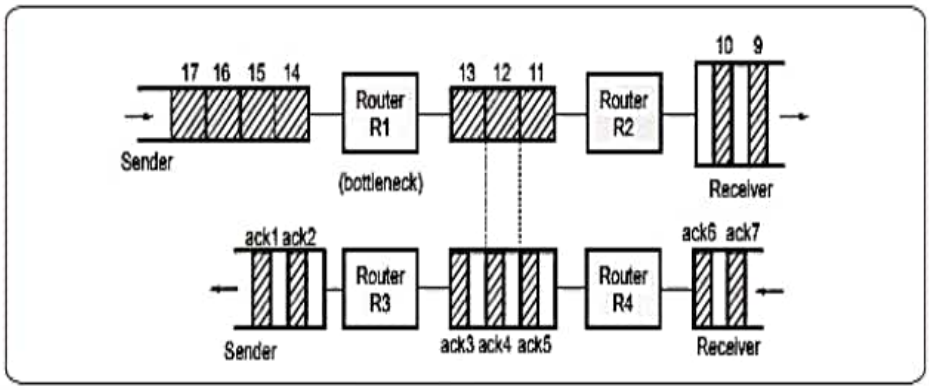


Fig. 4.2.12 Congestion caused by fast LAN sending a slow WAN

- Fig. 4.2.12 shows the one typical example for TCP congestion.
- The Router R1 is labelled as the bottleneck because it is the congestion point. Router R1 can receive packets from the LAN on its left faster than they can be sent out the WAN on its right.
- When router R2 put the received packets onto the LAN on its right, they maintain the same spacing as they did on the WAN on its left, eventhough the bandwidth of the LAN is higher.
- Slow start is the way to initiate data flow across a connection. *Congestion avoidance* is a way to deal with lost packets.

4.2.12 TCP Flow Control

- TCP interactive data flow uses Rlogin application. In TCP/IP the each interactive keystroke normally generates a data packet. The keystrokes are sent from the client to the server 1 byte at a time. Rlogin has the remote system; each characters that the client type is displayed on the other side (server).
- Fig. 4.2.13 shows the flow of data.
- The TCP acknowledgements operates as follows.

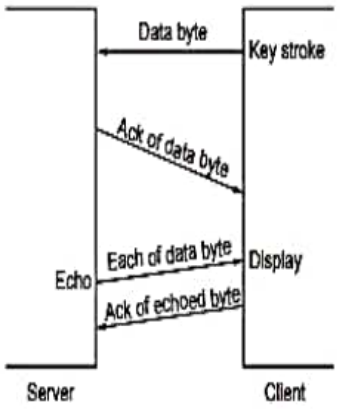


Fig. 4.2.13 Remote echo of interactive keystroke

- Line 1 sends the data byte with the sequence number 0. Line 2 ACKs this by setting the acknowledgement sequence number to 1, the sequence number of the last successfully received byte plus one. This is also called the sequence number of the next excepted byte.
- Line 2 also sends the data byte with a sequence number of 1 from the server to the client. This is ACKed by the client in line 3 by setting the acknowledgement sequence number to 2. Normally TCP does not send an ACK the instant it receives data. Instead, it delays the ACK, hoping to have data going in the same direction as the ACK, so the ACK can be sent alongwith the data. TCP will delay an ACK upto 200 ms to see if there is data to send with the ACK.

NAGLE algorithm :

- One byte at a time normally flows from the client to the server across a Rlogin connection. This generates 41-byte packet 20 bytes for the IP header and 20 bytes for TCP header and 1 byte of data. These small packets called as tinygrams. These tinygrams can add to congestion on WAN.
- Most LANs are not congested because tinygrams are not a problem on LANs. To solve the problem of congestion of WAN, the Nagle algorithm is used.
- The Nagle algorithm say that when TCP connection has outstanding data that has not yet been acknowledged, small segments cannot be sent until the outstanding data is acknowledged. Instead, small amounts of data are collected by TCP and sent in a single segment when the acknowledgement arrives.

ECN capable	yes	yes	no
Selective ACKs	yes	optional	no
Preservation of message boundaries	yes	no	yes
Path MTU discovery	yes	yes	no
Application PDU fragmentation	yes	yes	no
Application PDU bundling	yes	yes	no
Multistreaming	yes	no	no
Multihoming	yes	no	no
Protection against SYN flooding attacks	yes	no	Not applicable
Allows half-closed connections	no	yes	Not applicable
Reachability check	yes	yes	no
Psuedo-header for checksum	no	yes	yes
Time wait state	for vtags	for 4-tuple	Not applicable

4.3.2 SCTP Services

- Similar to TCP, SCTP provides a reliable and in-order data transfer service to HTTP. Additionally, SCTP provides other services unavailable in TCP. These services are summarized below.
  1. Multistreaming
  2. Process to process communication
  3. Four-way handshake during association establishment.
  4. No Maximum Segment Lifetime (MSL) during association termination.
  5. Multihoming for improved fault tolerance.
  6. Preserving application message boundaries.
  7. Reliable services
  8. Connection oriented service.
  9. Sequenced delivery of user datagrams within a stream

4.3.3 Features

- Seamless integration with Trillium protocol software SCTP users :
  - Next Generation Network protocols
    - SIP
    - Diameter
    - GCP (H.248 / MEGACO / MGCP)
  - SIGTRAN protocols
    - SUA
    - M3UA
    - M2UA
    - M2PA
    - IUA
    - V5UA
    - DUA
- Delivers datagrams reliably.
- Provides multiple streams to remove head-of-line blocking.

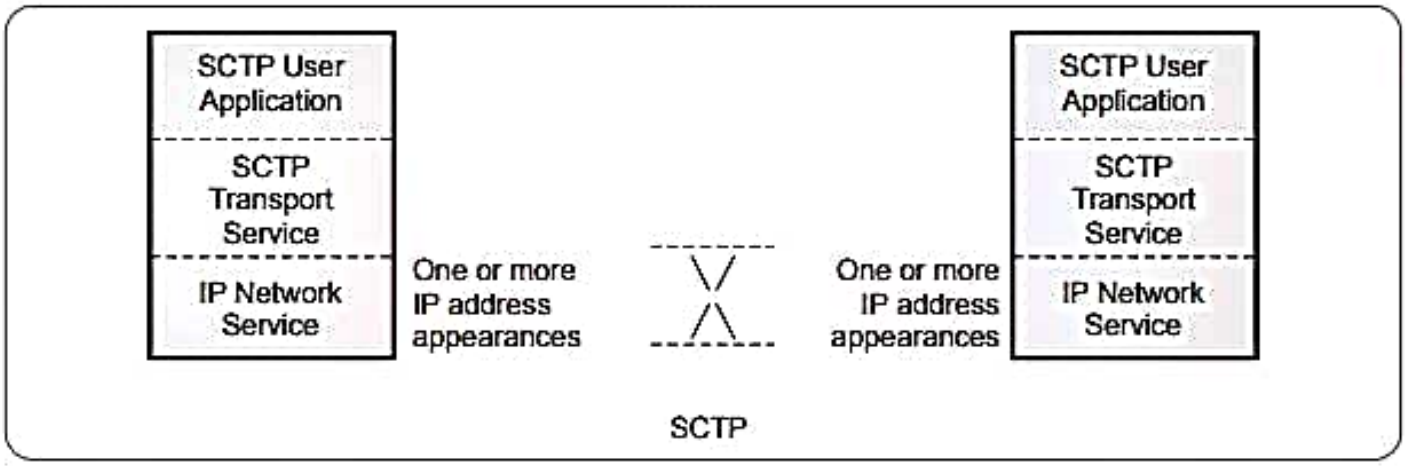


Fig. 4.3.1 Diagram showing the concept of SCTP association

- Delivers sequenced datagrams in a stream; a datagram lost in one stream does not block datagrams in other streams.
- Delivers out-of-order datagrams.
- Segments large user datagrams to confirm to the current path MTU size.
- Bundles multiple, small user datagrams in a SCTP datagram to improve bandwidth use.
- Supports multi-homing.
- Provides a service user, controlled heartbeat mechanism to monitor whether the endpoint is reachable.
- Provides endpoint failure notifications.
- Provides destination transport address failure notifications of a multi-home destination.
- Provides destination address failover mechanism.
- Provides interface to the service user to retrieve unsent/undelivered/unacknowledged datagrams for abnormal association termination.
- Supports DNS interface to resolve hostname parameter.
- Supports both Adler-32 and CRC-32 checksum algorithm at runtime (RFC 3309).
- Supports path probing procedure.
- Provides a management interface for configuration and control operations, and status and statistics retrieval; it also provides protocol state and alarm information at the management interface.
- Provides extensive run-time error checking support.
- Provides extensive debugging support to ease system integration and testing.
- Provides support for function call traces and tracing of incoming and outgoing PDUs; the trace information is provided at the management interface, which can be used to support remote logging and analysis operation. Supports IPv4 and IPv6.
- Supported user defined IP TOS parameters.
- Conforms to Trillium Advanced Portability Architecture (TAPA).
- Benefits of licensing Trillium protocol source code software from Continuous Computing.

4.3.4 Transmission Sequence Number

- SCTP allows multiple message streams to be exchanged on a single SCTP connection. Data from multiple streams can be sent in a single SCTP message as chunks. Selective acknowledgements are supported at individual chunk level.
- Recent additions to the SCTP protocol allow dynamic configuration of the IP addresses. Similar to SS7, SCTP can be switched over from one link to another.
  SCTP supports a make-before-break changeover, i.e. the packet stream is moved before removing the link that needs to be taken out of service.
- In this sequence diagram we will be examining some of the features of SCTP.
  1) SCTP Connection establishment.
  2) SCTP data exchange and selective acknowledgement.
  3) Addition of a new IP address to an SCTP connection.
  4) Switching over to the new IP address.
  5) Removing the old IP address.
  6) SCTP connection release.

4.3.5 SCTP Packet Format

- SCTP transmits data in the form of messages and each message contains one or more packets. The control chunks come before data chunks. Fig. 4.3.2 illustrates an SCTP packet format.
  (See Fig. 4.3.2 on next page)

4.3.5.1 General Header

- An SCTP packet contains a common header(General header), and one or more chunks. The SCTP common header contains the following information :
  1. Source and destination port numbers to enable multiplexing of different SCTP associations at the same address.
  2. A 32-bit verification tag that guards against the insertion of an out-of-date or false message into the SCTP asociation.
  3. A 32-bit checksum for error detection. The checksum can be either a 32-bit CRC checksum or Adler-32 checksum.

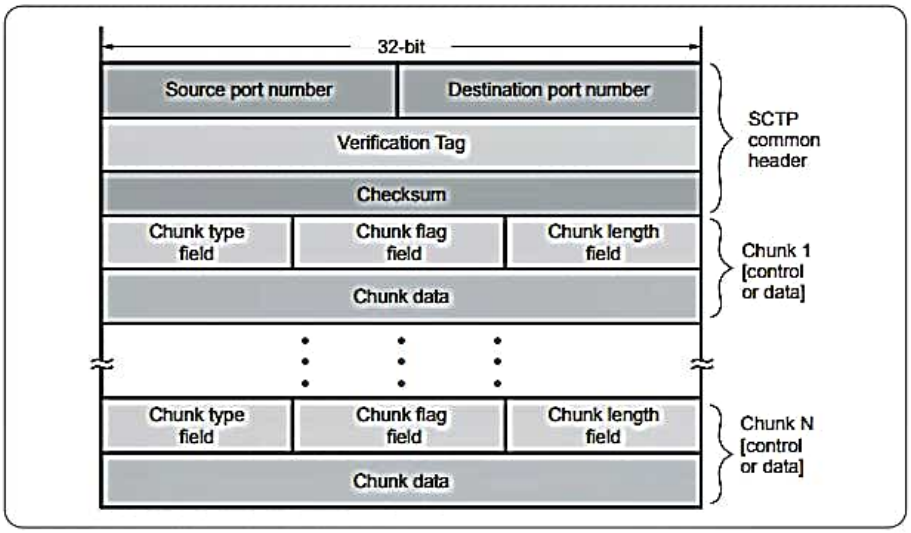


Fig. 4.3.2 SCTP Packet Format

- Every SCTP packet contains the common header as seen above. The header contains four different fields and is set for every SCTP packet.

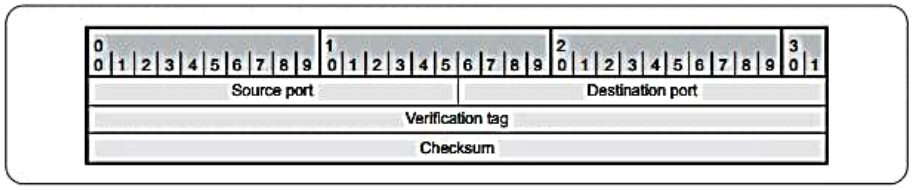


Fig. 4.3.3 Common SCTP headers

4.3.5.2 Chunk Layout

- A chunk can be either a control chunk or a DATA chunk. A control chunk incorporates different flags and parameters, depending on the chunk type. The DATA chunk incorporates flags to control segmentation and reassembly, and parameters for the Transmission Sequence Number (TSN), Stream Identifier (SID) and Stream Sequence Number (SSN), and a Payload Protocol ID. The DATA chunk contains the actual data payload.

4.3.5.3 Chunk Type

- This field identifies the type of information contained in the Chunk Data field. The value of the chunk field ranges from 0 to 254. The value 255 is reserved for future use, as an extension field. SCTP consists of one DATA chunk and 12 control chunks.

Chunk Number	Chunk Name
0	Payload Data (DATA)
1	Initiation (INIT)
2	Initiation Acknowledgement (INIT ACK)
3	Selective Acknowledgement (SACK)
4	Heartbeat Request (HEARTBEAT)
5	Heartbeat Acknowledgement (HEARTBEAT ACK)
6	Abort (ABORT)
7	Shutdown (SHUTDOWN)
8	Shutdown Acknowledgement (SHUTDOWN ACK)
9	Operation Error (ERROR)
10	State Cookie (COOKIE ECHO)
11	Cookie Acknowledgement (COOKIE ACK)
12	Reserved for Explicit Congestion Notification Echo (ECNE)
13	Reserved for Congestion Window Reduced (CWR)
14	Shutdown Complete (SHUTDOWN COMPLETE)
15 - 62	Reserved for IETF
63	IETF-defined chunk extensions
64 - 126	Reserved to IETF
127	IETF-defined chunk extensions
128-190	Reserved to IETF
191	IETF-defined chunk extensions
192-254	Reserved to IETF
255	IETF-defined chunk extensions

Table 4.3.1

Table 4.3.1 lists the description and parameters of the different chunk types.

Chunk	Description
Payload Data (DATA)	Used for data transfer.
Initiation (INIT)	Initiates an SCTP association between two endpoints.
Initiation Acknowledgement (INIT ACK)	Acknowledges the receipt of an INIT chunk. The receipt of the INIT ACK chunk establishes an association.
Selective Acknowledgement (SACK)	Acknowledges the receipt of the DATA chunks and also reports gaps in the data.

Cookie Echo (COOKIE ECHO)	Used during the initiation process. The endpoint initiating the association sends the COOKIE ECHO chunk to the peer endpoint.
Cookie Acknowledgement (COOKIE ACK)	Acknowledges the receipt of the COOKIE ECHO chunk. The COOKIE ACK chunk must take precedence over any DATA chunk or SACK chunk sent in the association. The COOKIE ACK chunk can be bundled with DATA chunks or SACK chunks
Heartbeat Request (HEARTBEAT)	Tests the connectivity of a specific destination address in the association.
Heartbeat Acknowledgement (HEARTBEAT ACK)	Acknowledges the receipt of the HEARTBEAT chunk.
Abort Association (ABORT)	Informs the peer endpoint to close the association. The ABORT chunk also informs the receiver of the reason for aborting the association.
Operation Error (ERROR)	Reports error conditions. The ERROR chunk contains parameters that determine the type of error.
Shutdown Association (SHUTDOWN)	Triggers a graceful shutdown of an association with a peer endpoint.
Shutdown Acknowledgement (SHUTDOWN ACK)	Acknowledges the receipt of the SHUTDOWN chunk at the end of the shutdown process.
Shutdown Complete (SHUTDOWN COMPLETE)	Concludes the shutdown procedure.

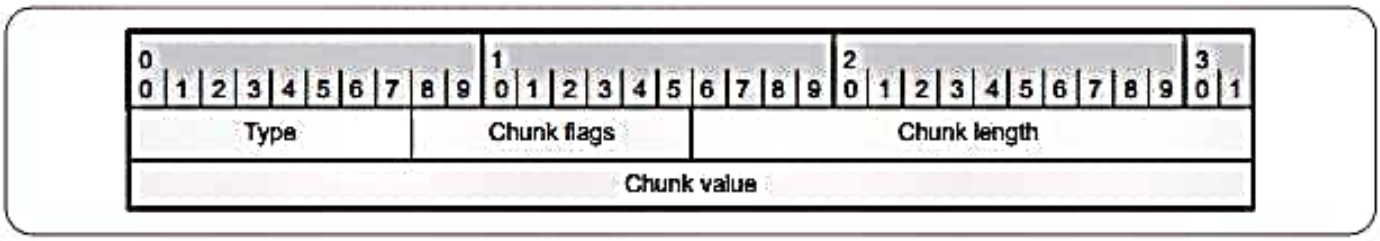


Fig. 4.3.4 Generic chunk headers

Chunk Flag

- Chunk field contains the flags, such as U (unordered bit), B (beginning fragment bit), and E (ending fragment bit). Usage of this field depends on the chunk type specified in the chunk type field. Unless otherwise specified, SCTP sets this field to 0 while transmitting the packet and ignores the chunk flag on receipt of the packet.

Chunk Length

- This field represents the size of the fields chunk type, chunk flag, chunk length, and chunk value, in bytes.

4.3.5.4 SCTP DATA Chunk

- Fig. 4.3.5 shows data chunk header.
- DATA chunks are used to send actual data through the stream and have rather complex headers in some ways, but not really worse than TCP headers in general. Each DATA chunk may be part of a different stream, since each SCTP connection can handle several different streams.

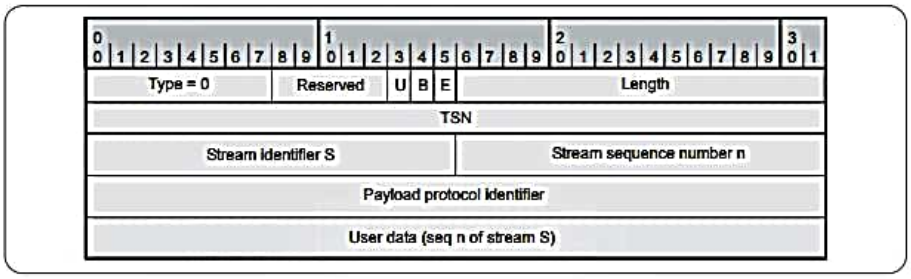


Fig. 4.3.5 Data chunk header

Type - bit 0-7 :

- The Type field should always be set to 0 for DATA chunks.

Reserved - bit 8-12 :

Not used today. Might be applicable for change.

U-bit - bit 13 : The U-bit is used to indicate if this is an unordered DATA chunk. If it is, the Stream Sequence Number must be ignored by the receiving host and send it on to the upper layer without delay or tries to re-order the DATA chunks.

B-bit - bit 14 : The B-bit is used to indicate the beginning of a fragmented DATA chunk. If this bit is set and the E (ending) bit is not set, it indicates that this is the first fragment of a chunk that has been fragmented into several DATA chunks.

E-bit - bit 15 : The E-bit is used to indicate the ending of a fragmented DATA chunk. If this flag is set on a chunk, it signals to the SCTP receiver that it can start reassembling the fragments and pass them on to the upper layer. If a packet has both the BE-bits set to 0, it signals that the chunk is a middle part of a fragmented chunk. If both BE-bits are set to 1 it signals that the packet is unfragmented and requires no reassembly etc.

Length - bit 16-31 : The length of the whole DATA chunk calculated in bytes,including the chunk type field and on until the end of the chunk.

TSN - bit 32-63 : The Transmission Sequence Number (TSN) is sent in the DATA chunk, and the receiving host uses the TSN to acknowledge that the chunk got through properly by replying with a SACK chunk. This is an overall value for the whole SCTP association.

Stream Identifier - bit 64-79 : The Stream Identifier is sent along with the DATA chunk to identify which stream the DATA chunk is associated with. This is used since SCTP can transport several streams within a single association.

Stream Sequence Number - bit 80-95 : This is the sequence number of the chunk for the specific stream identified by the Stream Identifier. This sequence number is specific for each stream identifier. If a chunk has been fragmented, the Stream Sequence Number must be the same for all fragments of the original chunk.

Payload Protocol Identifier - bit 96-127 :

This value is filled in by the upper layers, or applications using the SCTP protocol as a way to identify to each other the content of the DATA chunk. The field must always be sent, including in fragments since routers and firewalls, etc, on the way might need the information. If the value was set to 0, the value was not set by the upper layers.

User data - bit 128-n : This is the actual data that the chunk is transporting. It can be of variable

length, ending on an even octet. It is the data in the stream as specified by the stream sequence number n in the stream S.

4.4 Two Marks Questions with Answers

Q.1 *Write abbreviation/Acronym of following :*
i) UDP ii) TCP
iii) TFTP iv) RTT v) SCTP

MSBTE : Summer-16

Ans. : i) UDP - User Datagram Protocol

ii) TCP - Transmission Control Protocol

iii) TFTP- Trivial File Transfer Protocol

iv) RTT- Round-Trip Time

v) SCTP- Stream Control Transmission Protocol

Q.2 *What are the fields on which the UDP checksum is calculated ? Why ?*

Ans. : UDP checksum includes a pseudoheader, the UDP header and the data coming from the application layer.

Q.3 *Why is UDP pseudo header included in UDP checksum calculation ? What is the effect of an invalid checksum at the receiving UDP ?*

Ans. : To verify that the user datagram has reached its correct destination. Since UDP is a connectionless protocol, it does not throw any exceptions on receiving a invalid "checksum" UDP message. The transport layer on the other hand, might drop it on receiving this packet because of the wrong check sum.

Q.4 *What is TCP ?*

Ans. : TCP provides a connection oriented, reliable, byte stream service. The term connection-oriented means the two applications using TCP must establish a TCP connection with each other before they can exchange data.

Q.5 *What is the purpose of TCP push operation ?*

Ans. : TCP push operation is used for immediate response. The sending TCP must not wait for the window to be filled. It must create a segment and send immediately. The sending TCP must also set the push bit to let the receiving TCP know that the segment include data that must be delivered to the receiving application program as soon as possible and not to wait for more data to come.

Q.6 *What are the advantages of using UDP over TCP ?*

Ans. : Does not include the overhead needed to detect reliability and maintain connection-oriented semantics.

Q.7 *What factors govern the rate at which TCP sends segments ?*

Ans. :

1. The current window size specifies the amount of data that can be in transmission at any one time. Small windows imply little data ; large windows imply a large amount of data.
2. If our retransmit timer is too short, TCP retransmits segments that have been delayed, but not lost, increasing congestion at a time when the network is probably already congested.

Q.8 *What is the purpose of urgent pointer in the TCP header ?*

Ans. : In certain circumstances, it may be necessary for a TCP sender to notify the receiver of urgent data that should be processed by the receiving application as soon as possible. This 16-bit field tells the receiver when the last byte of urgent data in the segment ends.

Q.9 *What is a port ?*

Ans. : Applications running on different hosts communicate with TCP with the help of a concept called as ports. A port is a 16 bit unique number allocated to a particular application.

Q.10 *Give some examples of applications where UDP is preferred over TCP.*

Ans. : 1) In multicasting

2) Route update protocol in RIP.

Q.11 *How does transport layer perform duplication control ?*

Ans. : TCP uses a sequence number to identity each byte of data. It helps to avoid duplicate data and disordering during transmission.

❑❑❑

UNIT - V

5 APPLICATION LAYER

5.1 World Wide Web (WWW)

- World wide web is collection of millions of files stored on thousands of servers all over the world. These files represent documents, pictures, video, sounds, programs, interactive environments.
- Following are hardware, software and protocols that make up the web.

1. A web server is a computer connected to the Internet that runs a program that takes responsibility for storing, retrieving and distributing some of the web files. A web client (web browser) is a computer that requests files from the web.
2. Well-defined set of languages and protocols that are independent of the hardware or operating system are required to run on the computers.
3. The Hyper Text Markup Language (HTML) is the universal language of the web.
4. Java is a language for sending small applications over the web. Java script is a language for extending HTML to embed small programs called scripts in web pages. The main purpose of Java and scripts is to speed up the interactivity of web pages.
5. VB script and Activex controls are microsoft system that work with IE.
6. Pictures, drawings, charts and diagrams are displayed on web using image formats such as JPEG and GIF formats.
7. The Virtual Reality Modeling Language (VRML) is the web's way of describing three-dimensional objects.

- A web page is an HTML document that is stored on a web server. A web site is a collection of web pages belonging to a particular organization.
- URL of these pages share a common prefix, which is the address of the home page of the size. Search engines are a bottom-up approach for finding your way around the web. Some search engines search only the titles of web pages. While other search every word. Keywords can be combined with Boolean operations, such as AND, OR and NOT, to produce rather complicated queries.
- Home page is the front door of a web site. When a person or organization says "My web site is at www.sangeeta.com", the URL to which they refer is the URL of the site's home page. The home page introduces the rest of the web site and provides links that leads to other pages on the site.

5.1.1 Web Browsers

- A web browser is a program. Web browser is used to communicate with web servers on the Internet, which enables it to download and display the webpages. Netscape Navigator and Microsoft Internet Explorer are the most popular browser softwares available in market. Browser interact with web as well as computer operating system and with other programs.
- Internet explorer is the default browser in newly installed window 98 systems. Most browser windows have the same basic layout. Some of the basic elements are
  - Menu bar
  - Tool bar
  - Address or location window

- Viewing window
- Status bar

Some web pages are divided into independent pages, called frames.

- The purpose of the web browser is to display web pages, which may either arrive over the Internet. Web browser can be used to view files of any common web format that are stored on the user system. Window, Macintosh and some Unix desktops support the default web browser.
- There are different ways for opening the web page.
  1. Enter its URL into the address or location box of a web browser.
  2. Select it from the list that drops down from the address.
  3. Link to it from another web page.
  4. Link to it from a mail message or newsgroup article.

5.1.2 Working of WWW

- www uses client-server interaction. The browser program acts as a client that uses the Internet to contact a remote server for a copy of the requested page. The server on the remote system returns a copy of the page along with the additional information.
- The additional information a www server returns tells the browser two important things.
  1) It describes how to display the information.
  2) It gives a URL for each selectable item on the page.
- When a browser receives a page from a remote server, it displays the page and then waits for the user to select one of the highlighted items. Once a user makes a selection, the browser consults the hidden information that arrived with the page to find the URL that corresponds to the selection. The browser then uses the Internet to obtain the newly selected page of information.
- Each URL uniquely identifies a page of information by giving the name of a remote computer, a server on that computer and a specific page of information available from the server. Fig. 5.1.1 illustrates how the URL encodes the information.
- World Wide Web was developed using the client server architecture, which ensured cross-platform portability. The www is officially described as a "Wide area hypermedia information retrieval initiative". It is an information system that links data from many different Internet services under one set of protocols.
- Web clients, called browsers, interpret Hyper Text Markup Language documents delivered from web servers.
- The world wide web is a distributed, multimedia, hyper text system. It is distributed since information on the web can be located on any computer system connected to the Internet around the world.
- It is multimedia because the information it holds can be in the form of text, graphics, sound and video.
- Hyper text means that the information is available using hyper text technique, which involves selecting highlighted phrases or images that one selected retrieve information related to the selected highlighted subject.
- The information being retrieved can be information located any where in the world. The normal way to provide information on the world wide web is by writing documents in HTML (Hyper Text Markup Language).

5.1.2.1 The Client Side

- When a user clicks on a hyperlink, the brower carries out a series of steps in order to fetch the page pointed to.

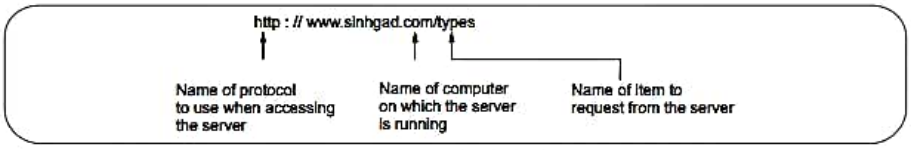


Fig. 5.1.1 Format of URL

1. The brower determines the URL.
2. The brower asks DNS for the IP address of www.vtubooks.com.
3. DNS replies with 172 · 16 · 16 · 1.
4. The brower makes a TCP connection to port 80 on 172 · 16 · 16 · 1.
5. It then sends over a request asking for file/home/index.html.
6. The www.vtubooks.com server sends the file/home/index.html.
7. TCP connection is released.
8. The brower displays all the text in home/index.html.
9. The brower fetches and displays all images in this file.

• Fig. 5.1.2 shows the web model.

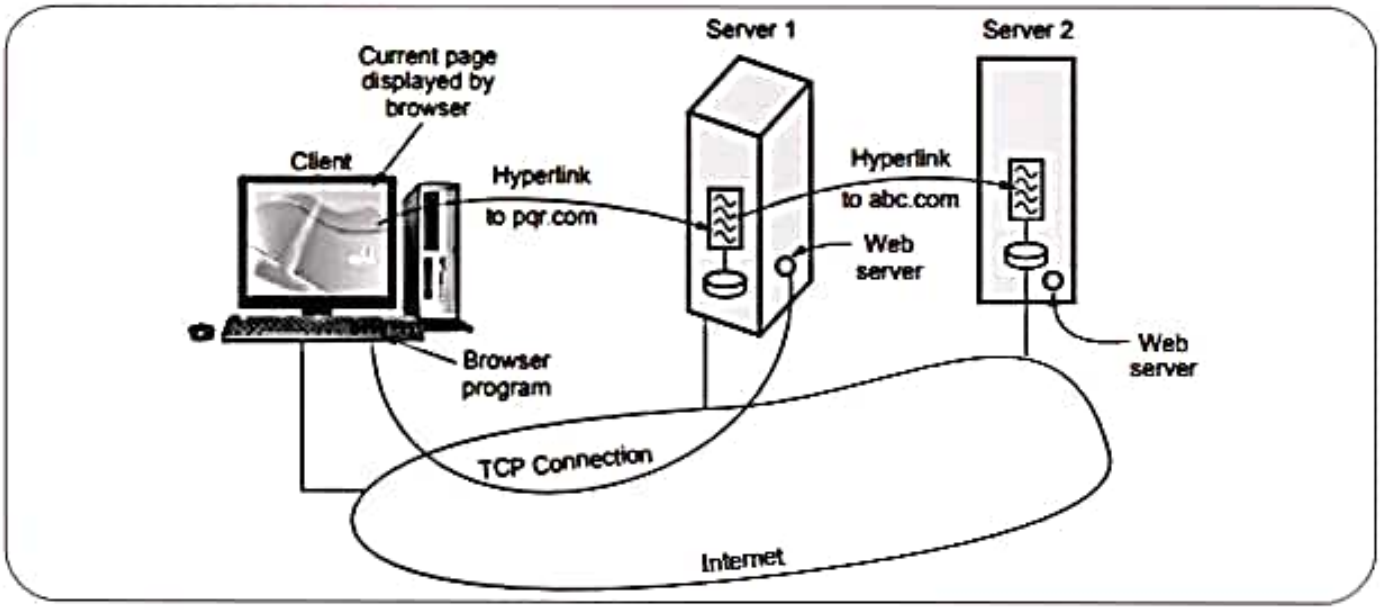


Fig. 5.1.2 Web model

5.1.2 The Server Side

• The steps that the server performs.

1. Accept a TCP connection from a client browser.
2. Get the name of the file required.
3. Get the file.
4. Return the file to the client.
5. Release the TCP connection.

5.1.3 Statelessness and Cookies

• The web is basically stateless. There is no concept of a login session. The browser sends a request to a server and gets back a file. Then the server forgets that it has ever seen that particular client.

• When a client requests a web page, the server can supply additional information along with the requested page. This information may include a cookie, which is a small file. Browsers store offered cookies in a cookies directory on the client's hard disk unless the user has disabled cookies.

- Cookies are just files or strings, not executable programs. In principle, a cookie could contain a virus, but since cookies are treated as data there is no official way for the virus to actually run and do damage.
- A cookie may contain upto five fields.
  a) Domain
  b) Path
  c) Content
  d) Expires
  e) Secure

  a) **Domain :** It tells where the cookies came from. Browsers are supposed to check that servers are not lying about their domain. Each domain may store no more than 20 cookies per client.

  b) **Path :** The path is a path in the server's directory structure that identifies which parts of the server's file tree may use the cookie. It is often 1, which means the whole tree.

  c) **Content :** It takes the form name = value. Both name and value can be anything the server wants. This field is where the cookies content is stored.

  d) **Expires :** The expires field specifies when the cookies expires. If this field is absent, the browser discards the cookies when it exits. Such a cookies is called a **nonpersistent cookie.** If a time and date are supplied, the cookie is said to be **persistent** and is kept until it expires.

  e) **Secure :** This field can be set to indicate that the browser may only return the cookie to a secure server. This feature is used for e-commerce, banking and other secure applications.

Examples of cookies

Domain	Path	Content	Expires	Secure
toms-casino.com	/	customer ID=497793521	15-10-02, 17:00	Yes
joes-store.com	/	cart=1-00501; 1-07031; 2-13721	11-10-02, 15:20	No
sneaky.com	/	user ID=3456789	30-12-06, 11:00	Yes

5.1.4 Static Web Documents

- Hyper Text Markup Language (HTML) is intended as a common medium for typing together information from widely different sources. HTML documents are the Standard Generalized Markup Language (SGML) documents with generic semantic that are appropriate for representing information from a wide range of applications.
- HTML documents are in plain text format that contain embedded HTML tags. Documents can be created in any text editor. There are also many other tools, including editors, designed specifically to assist in creating HTML documents. To view an HTML document, the user needs a browser.
- HTML defines the structural elements in a document such as headers, and addresses, layout information and the use of inline graphics together with the ability to provide hyper text links. Web pages were written in HTML level 0.

- Cookies are just files or strings, not executable programs. In principle, a cookie could contain a virus, but since cookies are treated as data there is no official way for the virus to actually run and do damage.
- A cookie may contain upto five fields.
  a) Domain
  b) Path
  c) Content
  d) Expires
  e) Secure

  a) **Domain :** It tells where the cookies came from. Browsers are supposed to check that servers are not lying about their domain. Each domain may store no more than 20 cookies per client.

  b) **Path :** The path is a path in the server's directory structure that identifies which parts of the server's file tree may use the cookie. It is often 1, which means the whole tree.

  c) **Content :** It takes the form name = value. Both name and value can be anything the server wants. This field is where the cookies content is stored.

  d) **Expires :** The expires field specifies when the cookies expires. If this field is absent, the browser discards the cookies when it exits. Such a cookies is called a **nonpersistent cookie.** If a time and date are supplied, the cookie is said to be **persistent** and is kept until it expires.

  e) **Secure :** This field can be set to indicate that the browser may only return the cookie to a secure server. This feature is used for e-commerce, banking and other secure applications.

Examples of cookies

Domain	Path	Content	Expires	Secure
toms-casino.com	/	customer ID=497793521	15-10-02, 17:00	Yes
joes-store.com	/	cart=1-00501; 1-07031; 2-13721	11-10-02, 15:20	No
sneaky.com	/	user ID=3456789	30-12-06, 11:00	Yes

5.1.4 Static Web Documents

- Hyper Text Markup Language (HTML) is intended as a common medium for typing together information from widely different sources. HTML documents are the Standard Generalized Markup Language (SGML) documents with generic semantic that are appropriate for representing information from a wide range of applications.
- HTML documents are in plain text format that contain embedded HTML tags. Documents can be created in any text editor. There are also many other tools, including editors, designed specifically to assist in creating HTML documents. To view an HTML document, the user needs a browser.
- HTML defines the structural elements in a document such as headers, and addresses, layout information and the use of inline graphics together with the ability to provide hyper text links. Web pages were written in HTML level 0.

- The <H/> and </H/> tags are used to define the first level heading. Headings are generated by an <Hn> tags, where n is a digit in the range 1 to 6. <H/> is the most important heading and <H6> is the less important. Typically the lower numbered heading will be displayed in a larger and heavier font.
- The browser may also choose to use different colors for each level of heading. Typically <H1> headings are large and bold face with at least one blank line above and below.
- In contrast <H2> headings are in a smaller font, and with less space above and below. The
, <P> and <HR> tags all indicate a boundary between sections of text.
- The precise format can be determined by the style sheet associated with the page. The
 tag just forces a line break. <P> starts a paragraph, which might for example, insert a blank line and possibly some indentation. <HR> (horizontal-rule) tag forces the browser to generate a horizontal rule or line, across the display. It breaks pages into logical sections and is useful when creating forms. There is no equivalent vertical rule.

Advantages and Disadvantages of HTML

A) Advantages of HTML :

1. Applications are quickly developed, requiring substantially less time than is required when creating programs with languages such as C and Pascal.
2. Web applications are easy to maintain and update without disrupting the network data traffic.
3. Developing applications in HTML takes advantage of HTML general compatibility. Web applications can access other company data servers, such as FTP and WAIs databases.
4. Collecting information with HTML.
5. Web viewer request a document from a web site, its server sends the data and the connection between the two computers is dropped. This is the client server relationship. This relationship reduces the amount of time a server spends serving a client freeing it to serve other users.

B) Disadvantages :

1. **Locking :** HTML is not a compiled data format. Web pages cannot be locked. Users have free and open access to look at HTML sources.
2. **Security :** Information is easily accessible and travels unimpeded between hosts and desktops. The cost of this freedom is lack of inherent security.

5.1.4.1 XML and XSL

- HTML does not provide any structure to web pages. HTML mixes the content with the formatting with web pages in HTML, it is very difficult for a program to search particular word.
- To overcome this problem, two new language Extensible Markup Language (XML) and Extensible Style Language (XSL) are used. The XML and XSL specifications are much stricter than HTML specification.
- Web pages in XML and XSL are still static since they simply contain instructions to the browser about how to display the page, just as HTML pages do. XML allows the web site designer to make up definition files in which the structures are defined in advance. Defination files can be included, making it possible to use them to build complex web pages.

5.1.4.2 XHTML

- XHTML is new web standard and should be used for all new web pages to achieve maximum portability across platforms and browsers.
- Difference between XHTML and HTML are as follows :
  1. XHTML pages and browsers must strictly conform to the standard.
  2. All tags and attributes must be in lower case.
  3. Closing tags are required even for </p>.
  4. Attributes must be contained within quotation marks.
  5. Tags must nest properly.
  6. Every document must specify its type.

5.1.5 Dynamic Web Documents

Server side dynamic web page generation. Fig. 5.1.3 shows processing of information in HTML.

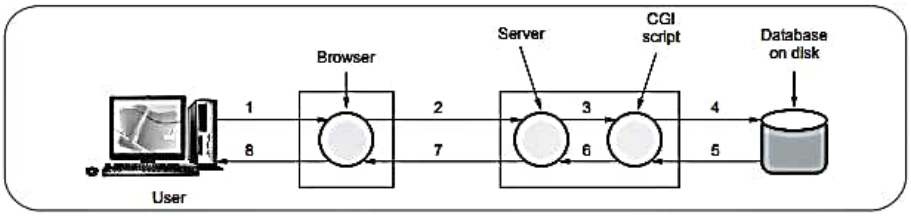


Fig. 5.1.3 Steps in processing information

1. User fills in form.
2. Form sent back.
3. Handed to CGI.
4. CGI queries database.
5. Record found.
6. CGI builds pages.
7. Page returned.
8. Page displayed.

5.1.5.1 Common Gateway Interface

- CGI makes dynamic computation of web pages possible. It allows a web server to associate some URLs with computer program instead of static documents on disk.
- When a browser request one of the special URLs the server runs the associated computer program and sends the output from the program back to the user. A server can have an arbitrary number of CGI programs that perform different computations.
- The server uses the URL in the incoming request to determine which CGI program to run. CGI working is as follows : CGI program is part of a web server.
- The browser sends a request to the server. If the requested URL corresponds to a CGI program, the server starts the appropriate program and passes to the program a copy of the request.
- The server then sends the output from the CGI program back to the browser in the form of reply.
- From a browser's point of view, there is no difference between a URL that corresponds to a static document and one that corresponds to a CGI program. Requests for both static documents and CGI output have the same syntatic form.

5.1.5.2 Java Technology

- Sun Microsystems, Incorporated has developed a popular active document technology called Java, the technology can be used to create animated web pages, pages that interact with the user, or pages that use the screen in unexpected ways.
- Java calls an active web page an *apple* ; the terminology is so widespread that most other vendors have either adopted it or chosen to use a minor variation.

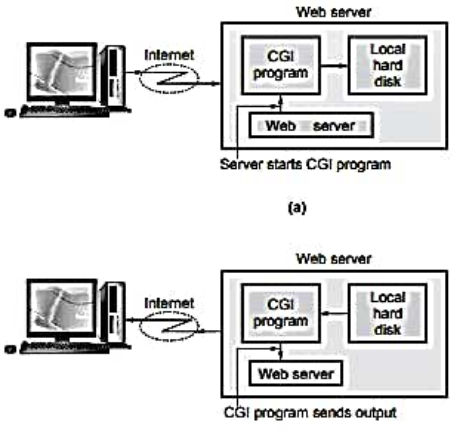


Fig. 5.1.4 Illustrates the CGI concepts

- Java became popular for four reasons.
  1) The designers chose to make the Java language similar to a widely-used programming language, meaning that professional programmers could learn to write Java applets easily.

2) No other active document technology was available.

3) Because the Java system includes software to handle common tasks such as controlling the screen, a programmer can use predefined pieces to create a Java applet quickly.

4) Java is so powerful that it provides more functionality than most other technologies. For example, Java can handle direct user interaction better than forms, can fetch a sequence of pages better than client-pull, can control multiple areas of the screen better than frames, and can manipulate a variety of data formats better than plugins. Thus, Java can substitute these by other technologies.

- Despite its many advantages over existing technologies, the strongest motivation for Java came from its ability to provide functionality that other technologies could not provide high quality animations. Because they use a computer's processing power to compute new images instead of trying to download them from a Web server, active document technologies like Java can change the display fast enough to present the illusion of smooth motion. Because none of the older Web technologies can provide the same functionality, many Web sites have been eager to use Java.

5.1.6 Browser Architecture

- Each browser usually consists of three parts.
  1. Controller
  2. Client programs
  3. Interpreters

Fig. 5.1.5 shows browser architecture.

- The controller receives input from the keyboard or mouse and uses the client programs to access the document. After the document has been accessed, the controller uses one of the interpreters to display the document on the screen. Client program uses protocol such as HTTP, FTP or SMTP. The interpreter can be HTML or Java.

5.1.7 Caching in Web Browser

- Each time a server receives a query for a name that is not in its domain, it needs to search its database for a server IP address. DNA handles this with a mechanism called caching.
- When a server asks for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client.
- If the same or another client asks for the same mapping, it can check its cache memory and resolve the problem.
- To inform the client that the response is coming from the cache memory and not from an authoritative source, the server marks the response as unauthoritative.
- Caching speed up the resolution.
- Problem - if a server caches a mapping for a long time, it may send an outdated mapping to the client.
- Above problem is solved by two methods.
  1. Authoritative server always adds a piece of information to the mapping called time to live (TTL).
  2. DNS requires that each server keeps a TTL counter for each mapping it caches. The cache

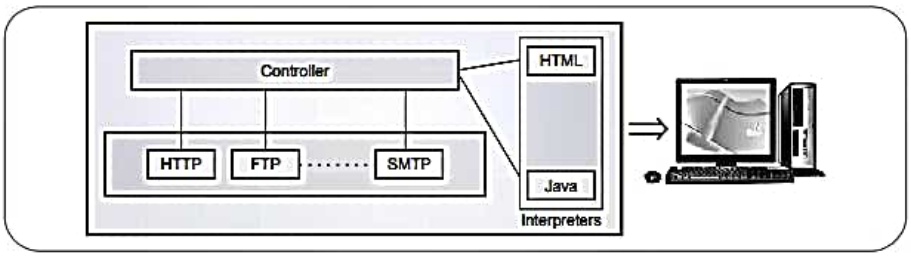


Fig. 5.1.5 Browser architecture

memory must be searched periodically and those mappings with an expired TTL must be purged.

- It satisfies the client request without involving origin server.
- User sets brower i.e. web accesses via cache.
- Brower sends all HTTP request to cache. If the object is in cache, it returns the object otherwise cache request the object from origin server.
- Fig. 5.1.6 shows the caching.

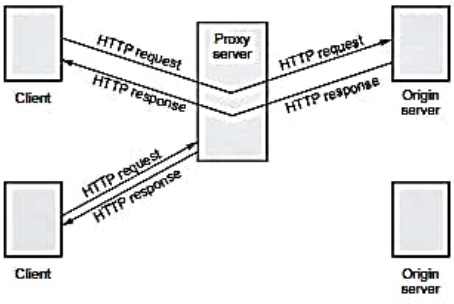


Fig. 5.1.6 Caching

5.1.8 Uniform Resource Locators

- The Uniform Resource Locator (URL) is a standard for specifying any kind of information on the Internet.
- URL has three parts
  1. The protocol
  2. DNS name of the machine where the page is located.
  3. File name containing the page.
- URL is represented as
- The protocol is the client-server program used to retrieve the document.
- Host is the computer on which the information is located.
- The URL can optionally contain the port number of the server.
- File name gives where the information is located.

5.2 HTTP

- The standard web transfer protocol is Hyper Text Transfer Protocol (HTTP).
- The HTTP protocol consists of two fairly distinct items: The set of requests from browsers to servers and the set of responses going back the other way.
- All the newer versions of HTTP support two kinds of requests: Simple requests and full requests. A simple request is just a single GET line naming the page desired, without the protocol version. The response is just the raw page with no headers, no MIME, and no encoding. To see how this works, try making a Telnet connection to port 80 of www.w3.org and then type.
  GET /hypertext/www/TheProject.html
  but without the HTTP/1.0 this time. The page will be returned with no indication of its content type. This mechanism is needed for backward compatibility. Its use will decline as browsers and servers based on full requests become standard.
- Full requests are indicated by the presence of the protocol version on the GET request line. Requests may consist of multiple lines, followed by a blank line to indicate the end of the request. The first line of a full request contains the command (of which GET is but one of the possibilities), the page desired, and the protocol/version. Subsequent lines contain RFC 822 headers.
- Although HTTP was designed for use in the Web, it has been intentionally made more general than necessary with an eye to future object-oriented applications. For this reason, the first word on the full request line is simply the name of the **method** (command) to be executed on the web page (or general object).
- When accessing general objects, additional object-specific methods may also be available. The names are case sensitive, so, GET is a legal method but get is not.

HTTP Transaction

- HTTP uses the services of TCP. HTTP is a stateless protocol.
- The client initilizes the transaction by sending a request message. The server replies by sending a response.

- Fig. 5.2.1 shows HTTP transaction

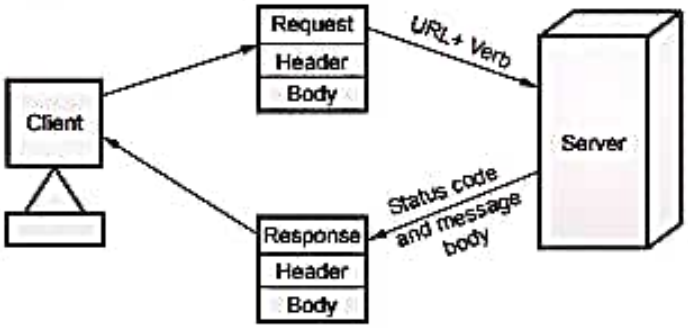


Fig. 5.2.1 HTTP transaction

Message

- HTTP messages are two types
  1. Request 2. Response
- Both message type used same format.
- Request message consists of a request line, headers and a body. Fig. 5.2.2 shows request message.

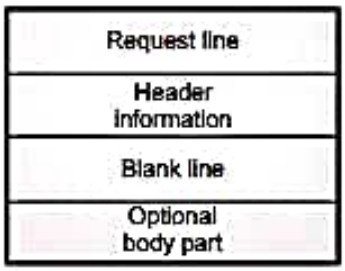


Fig. 5.2.2 Request message

Request line

- Request line defines the
  1. Request type
  2. Resource
  3. HTTP version
- Request type categorizes the request message into several methods for HTTP version 1.1.
- Fig. 5.2.3 shows the request line.

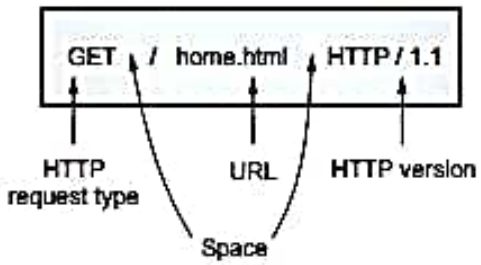


Fig. 5.2.3 Request line

- URL is a standard for specifying any kind of information on the internet. The URL define four things.
  1. Method
  2. Host computer
  3. Port
  4. Path

Fig. 5.2.4 shows the URL.

Fig. 5.2.4 (a) URL

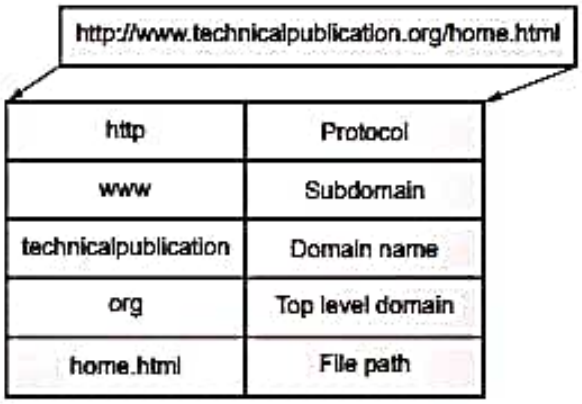


Fig. 5.2.4 (b) URL example

- The method is the prototocol used to retrieve the document. Several different protocols can retrieve a document, among them are FTP and HTTP.
- The host is the computer where the information is located, although the name of the computer can be alias. Web pages are usually stored in computers and computers are given alias names that usually begin with the character www.
- The URL can optionally contain the port number of the server.
- Path is the path name of the file where the information is located.
- The request type field in a request message defines several kinds of messages referred to as methods.

Sr. No.	Method	Purposes
1.	GET	Used when the client wants to retrieve a document from the server. Server responds with the contents of the document.
2.	HEAD	Used when client wants some information about a document but not the document itself.
3.	POST	Used by the client to provide some information to the server i.e. input to the server.

- Fig. 5.2.1 shows HTTP transaction

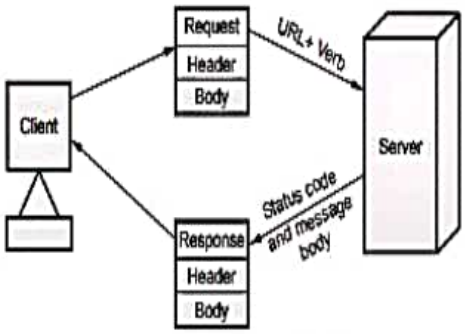


Fig. 5.2.1 HTTP transaction

Message

- HTTP messages are two types
  1. Request 2. Response
- Both message type used same format.
- Request message consists of a request line, headers and a body. Fig. 5.2.2 shows request message.

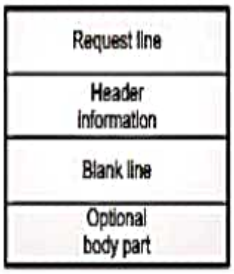


Fig. 5.2.2 Request message

Request line

- Request line defines the
  1. Request type
  2. Resource
  3. HTTP version
- Request type categorizes the request message into several methods for HTTP version 1.1.
- Fig. 5.2.3 shows the request line.

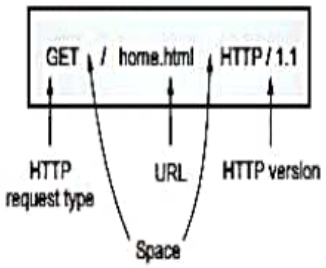


Fig. 5.2.3 Request line

- URL is a standard for specifying any kind of information on the internet. The URL define four things.
  1. Method
  2. Host computer
  3. Port
  4. Path

Fig. 5.2.4 shows the URL.

Fig. 5.2.4 (a) URL

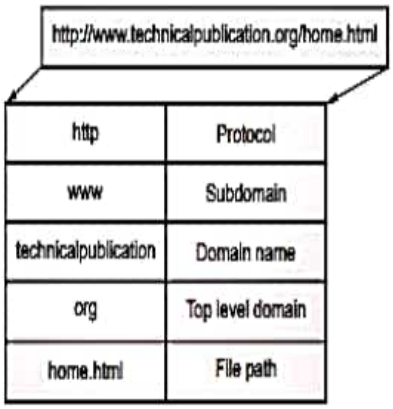


Fig. 5.2.4 (b) URL example

- The method is the prototocol used to retrieve the document. Several different protocols can retrieve a document, among them are FTP and HTTP.
- The host is the computer where the information is located, although the name of the computer can be alias. Web pages are usually stored in computers and computers are given alias names that usually begin with the character www.
- The URL can optionally contain the port number of the server.
- Path is the path name of the file where the information is located.
- The request type field in a request message defines several kinds of messages referred to as methods.

Sr. No.	Method	Purposes
1.	GET	Used when the client wants to retrieve a document from the server. Server responds with the contents of the document.
2.	HEAD	Used when client wants some information about a document but not the document itself.
3.	POST	Used by the client to provide some information to the server i.e. input to the server.

- The header exchange additional information between the client and the server.
- A header line belongs to one of four categories : general header, request header, response header and entity header.
- Fig. 5.2.6 shows the header format.

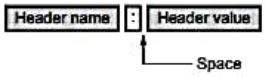


Fig. 5.2.6 Header format

- *General header* includes general information about the message. Request and a response both contains general header.
- *Response header* can be present only in a response message. It specifies the servers configuration and special information about the request.
- Request header can be present only in a request message. It specifies the clients configuration and the client preferred document format.
- *Entity header* gives information about the body of the document. It is mostly present in response messages, some request message, such as POST and PUT methods, that contain a body also use this type of header.
- Fig. 5.2.7 shows the headers.

Status line	HTTP/1.1 300 OK
General Headers	Date : Wed, 8 Oct 2014 13:00:13 GMT
	Connection : close
Response Headers	Server : Apache /1.3.27
	Accept-Ranges : bytes
Entity Headers	Content-Type : text/html
	Content-Length : 200
	Last-Modified : 2 Oct 2014 13:00:13 GMT
Blank Line	
Message Body	<html>
	<head>
	<title> Welcome to the India <title>
	<head>
	<body>

Fig. 5.2.7 Response message header

5.2.1 Persistent and Non-persistent Connection

- HTTP connections are of two types
  1. Persistent HTTP
  2. Non-persistent HTTP

Non-persistent connections

- In this type of connection, one TCP connection is made for each request / response.
- Suppose the page consists of a base HTTP file and ten JPEG images and that all 11 of these objects reside on the same server.
- Suppose the URL for the base HTML file is

  www.vtubooks.com / ITDept / home.index

The sequence of events are as follows :

1. The HTTP client initiates a TCP connection to the server www.vtubook.com on port number 80. It is default port number for HTTP.
2. HTTP client sends an HTTP request message to the server via the socket. Request message includes the path name/ITDept/home.index.
3. HTTP server receives the request message via the socket.
4. HTTP server tells TCP to close the TCP connection.
5. HTTP client receives the response message. The TCP connection terminates.
6. The first four steps are then repeated for each of the referenced JPEG objets.

- As the brower receives the web pages, it displays the page to the user.

Round Trip Time (RTT)

- RTT is the time it takes for a small packet to travel from client to server and then back to the client.
- RTT includes packet propagation delays, packet queuing delays in intermediate routers and switches and packet processing delays.
- Fig. 5.2.8 shows operation when user clicks on a hyperlink.
- Browser to initiate TCP connection between the browser and the web server. It requires three way handshake.
- The client sends a small TCP segment to the server.

- The header exchange additional information between the client and the server.
- A header line belongs to one of four categories : general header, request header, response header and entity header.
- Fig. 5.2.6 shows the header format.

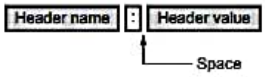


Fig. 5.2.6 Header format

- *General header* includes general information about the message. Request and a response both contains general header.
- *Response header* can be present only in a response message. It specifies the servers configuration and special information about the request.
- Request header can be present only in a request message. It specifies the clients configuration and the client preferred document format.
- *Entity header* gives information about the body of the document. It is mostly present in response messages, some request message, such as POST and PUT methods, that contain a body also use this type of header.
- Fig. 5.2.7 shows the headers.

Status line	HTTP/1.1 300 OK
General Headers	Date : Wed, 8 Oct 2014 13:00:13 GMT
	Connection : close
Response Headers	Server : Apache /1.3.27
	Accept-Ranges : bytes
Entity Headers	Content-Type : text/html
	Content-Length : 200
	Last-Modified : 2 Oct 2014 13:00:13 GMT
Blank Line	
Message Body	<html>
	<head>
	<title> Welcome to the India <title>
	<head>
	<body>

Fig. 5.2.7 Response message header

5.2.1 Persistent and Non-persistent Connection

- HTTP connections are of two types
  1. Persistent HTTP
  2. Non-persistent HTTP

Non-persistent connections

- In this type of connection, one TCP connection is made for each request / response.
- Suppose the page consists of a base HTTP file and ten JPEG images and that all 11 of these objects reside on the same server.
- Suppose the URL for the base HTML file is

  www.vtubooks.com / ITDept / home.index

The sequence of events are as follows :

1. The HTTP client initiates a TCP connection to the server www.vtubook.com on port number 80. It is default port number for HTTP.
2. HTTP client sends an HTTP request message to the server via the socket. Request message includes the path name/ITDept/home.index.
3. HTTP server receives the request message via the socket.
4. HTTP server tells TCP to close the TCP connection.
5. HTTP client receives the response message. The TCP connection terminates.
6. The first four steps are then repeated for each of the referenced JPEG objets.

- As the brower receives the web pages, it displays the page to the user.

Round Trip Time (RTT)

- RTT is the time it takes for a small packet to travel from client to server and then back to the client.
- RTT includes packet propagation delays, packet queuing delays in intermediate routers and switches and packet processing delays.
- Fig. 5.2.8 shows operation when user clicks on a hyperlink.
- Browser to initiate TCP connection between the browser and the web server. It requires three way handshake.
- The client sends a small TCP segment to the server.

- To use proxy server, the client must be configured to access the proxy instead of the target server.

5.2.2 Difference between Persistent and Non-persistent

Sr. No.	Persistent HTTP	Non-persistent HTTP
1.	Persistent version is 1.1.	Non-persistent HTTP version is 1.0.
2.	It uses one RTT.	It uses two RTT.
3.	TCP connection is not closed.	TCP connection is closed after every request-response.
4.	Client make multiple request over the same TCP connection.	Client make multiple request over the multiple TCP connection.
5.	It is default mode.	It is not default mode.
6.	Request methods are GET, HEAD, POST, PUT, DELETE, TRACE and OPTIONS.	Request methods used are GET, POST and HEAD.

5.3 File Transfer Protocol (FTP)

- Many network system provides computers with the ability to access files on remote machines. Some designer provides remote file access to lower overall cost. In such architectures, a single centralized file server provides secondary storage for a set of in expensive computers that have no local disk storage. e.g. the diskless machines can be portable devices used for chores such as inventory such machine communicates with a file server over a high speed wireless network. Some designs use remote storage to archive data. Some designs emphasize the ability to share data across multiple programs, multiple users, or multiple sites. The file sharing comes in two distinct forms.

  a) On-line access

  b) Whole-file copying

- On-line access means allowing multiple programs to access a single file concurrently. Changes to the file takes effect immediately and are available to all programs that access the file. Whole-file copying means that whenever a program wants to access a file, it obtains local copy. Copying is often used for read-only data, but if the file must be modified, the program makes changes to the local copy and transfers the modified file back to the original site. The remote file is integrated with local files, and that the entire file system provides transparent access to shared files. The alternative to integrated, transparent on-line access is file transfer. Accessing remote data with a transfer mechanism is a two step process, the user first obtains a local copy of file and then operates on the copy. Most transfer mechanisms operate outside the local file system. A user must invoke a special purpose client program to transfer files. Advantage of whole-file copying lies in the efficiency of operations-once a program has obtained a copy of a remote file, it can manipulate the copy efficiently.
- File transfer is among the most frequently used TCP/IP applications and it accounts for much network traffic. File transfer software evolved into a current standard known as the File Transfer Protocol (FTP). FTP is designed for distributing files to a number of users. FTP uses a client-server system, in which files are stored at a central computer and transferred between that computer and other, widely distributed computers. The central computer runs FTP server software and widely distributed computer runs FTP client software. FTP is interactive. The FTP program accepts a sequence of commands. To interact with a remote computer, a user must identify the computer and allow FTP to establish contact. FTP uses TCP/IP software to contact the computer. FTP provides 58 separate commands, an average user only needs to understand the three basic commands to connect to a remote computer, retrieve a copy of a file and exit the FTP program. Following are the list of commands.

Sr. No.	Command	Purpose
1.	open	Connect to a remote computer
2.	get	a file from the computer
3.	bye	Terminate the connection and leave the program

Table 5.3.1

These 3 commands are used for FTP clients for file transfer and terminates the connection after down loading or up loading the file. When user transfer a file by either uploading or downloading-user use one of two modes. User may need to select the mode. The modes is as follows.

1) ASCII mode

2) Binary (Image) mode

- ASCII mode is used for transferring a text files including HTML files. Different computer systems use different characters to indicate the ends of lines. In ASCII mode, the FTP software automatically adjusts line endings for the system to which the file is transferred. In binary mode, transferring of files consists of anything but unformatted text. In this mode, the FTP software does not make any changes to the contents of the file during transfer. Use binary mode when transferring graphic files, audio files, video files, program or any other kind of file other than plain text. Choosing between binary and ASCII transfer can be difficult. When unsure about the content of file, enter the FTP command binary before transferring the file. FTP uses the client-server approach. A user invokes an FTP program on the computer, instructs it to contact a remote computer and then requests the transfer of one or more files. The local FTP program becomes a client that uses TCP to connect on FTP server program on the remote computer. Each time the user requests a file transfer, the client and server programs co-operate to send copy of the data across the Internet. Fig. 5.3.1 shows the FTP connection.
- The FTP server locates the file that the user requested and uses TCP to send a copy of the entire contents of the file across the Internet to the client. As the client program receives data, it writes the data into a file on the user's local disk. After the file transfer completes the client and server programs terminate the TCP connection used for the transfer. FTP data transfer causes more traffic on the Internet than any other application.

Detail steps of FTP

- FTP client contacts FTP server at port 21 specifying TCP as transport protocol.
- Client obtain authorization over control connection.
- Client browse remote directory by sending commands over control connection.
- When server receives a command for a file transfer, the server open a TCP data connection to client.
- After transfering one file, server closes connection.
- Server opens a second TCP data connection to transfer another file.
- FTP server maintains state i.e. current directory, earlier authentication.
- Fig. 5.3.2 shows the FTP data connection

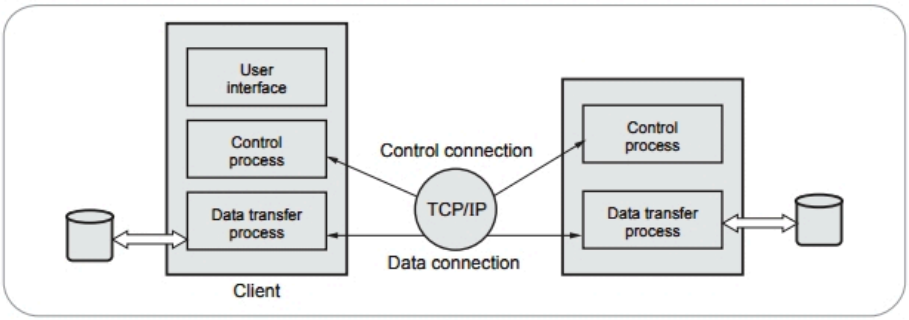


Fig. 5.3.1 FTP

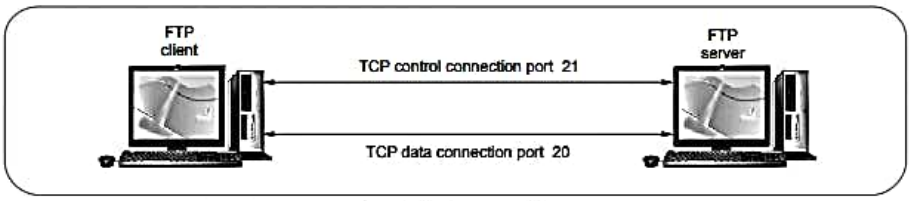


Fig. 5.3.2 Data connection

FTP commands

Sr. No.	Command	Meaning
1.	cd	Changes the working directory on the remote host
2.	close	Closes the FTP connection
3.	quit	Quits FTP
4.	pwd	Displays the current working directory on the remote host
5.	dir or ls	Provides a directory listing of the current working directory
6.	help	Displays a list of all client FTP commands
7.	remotehelp	Displays a list of all server FTP commands
8.	type	Allows the user to specify the file type
9.	struct	Specifies the files structure

5.3.1 Trivial File Transfer Protocol (TFTP)

- It is a UDP-based file transfer program which is frequently used to allow diskless hosts to boot over the network. TFTP is implemented by the tftp client program and by the tftp server program. As TFTP has no user authentication, it may be possible for unwanted file transfer to occur. It is a significant threat that TFTP may be used to steal password files.
- TFTP is a simple protocol to transfer files. It is implemented on top of the Internet User Datagram Protocol (UDP or Datagram). The design of a TFTP is small and easy to implement, therefore, lacks most of the features of a regular FTP. TFTP can only read and write files (or mail) from/to a remote server. It cannot list directories, and currently it has no provisions for user authentication.
- In TFTP, any transfer always begins with a request to read or write a file, which serves to request a connection. When the server grants the request, the connection is opened and the file is sent in fixed length blocks of 512 bytes. Each data packet contains one block of data, and it must be acknowledged by an acknowledgement packet before sending the next packet. A data packet of less than 512 bytes signals causes termination of a transfer. If a packet is lost in the network, the intended recipient will timeout and may retransmit his last packet (which may be data or an acknowledgment), thereby causing the sender of the lost packet to retransmit that lost packet. The sender has to keep just one packet on hand for retransmission, because the lock step acknowledgement guarantees that all older packets have been received. Notice that both machines involved in a transfer are considered senders and receivers. One sends data and receives acknowledgements, the other sends acknowledgements and receives data. Three modes of transfer currently supported by TFTP are netascii (that it is 8 bit ascii) octet (raw 8 bit bytes), mail, netascii characters sent to a user rather than a file. Also additional modes can be defined by pairs of cooperating hosts.

5.3.2 Difference between FTP and TFTP

Sr. No.	FTP	TFTP
1.	FTP uses two connections	TFTP uses one connection
2.	Provides many commands	Provides only five commands
3.	Uses TCP	Uses UDP

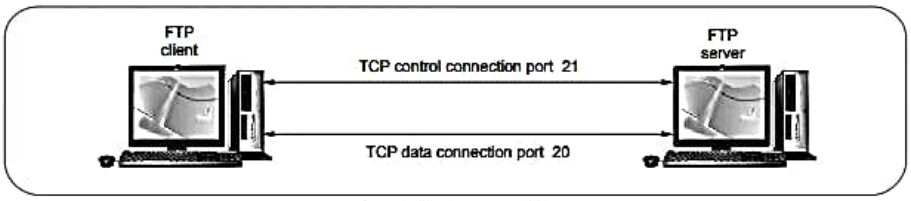


Fig. 5.3.2 Data connection

FTP commands

Sr. No.	Command	Meaning
1.	cd	Changes the working directory on the remote host
2.	close	Closes the FTP connection
3.	quit	Quits FTP
4.	pwd	Displays the current working directory on the remote host
5.	dir or ls	Provides a directory listing of the current working directory
6.	help	Displays a list of all client FTP commands
7.	remotehelp	Displays a list of all server FTP commands
8.	type	Allows the user to specify the file type
9.	struct	Specifies the files structure

5.3.1 Trivial File Transfer Protocol (TFTP)

- It is a UDP-based file transfer program which is frequently used to allow diskless hosts to boot over the network. TFTP is implemented by the tftp client program and by the tftp server program. As TFTP has no user authentication, it may be possible for unwanted file transfer to occur. It is a significant threat that TFTP may be used to steal password files.
- TFTP is a simple protocol to transfer files. It is implemented on top of the Internet User Datagram Protocol (UDP or Datagram). The design of a TFTP is small and easy to implement, therefore, lacks most of the features of a regular FTP. TFTP can only read and write files (or mail) from/to a remote server. It cannot list directories, and currently it has no provisions for user authentication.
- In TFTP, any transfer always begins with a request to read or write a file, which serves to request a connection. When the server grants the request, the connection is opened and the file is sent in fixed length blocks of 512 bytes. Each data packet contains one block of data, and it must be acknowledged by an acknowledgement packet before sending the next packet. A data packet of less than 512 bytes signals causes termination of a transfer. If a packet is lost in the network, the intended recipient will timeout and may retransmit his last packet (which may be data or an acknowledgment), thereby causing the sender of the lost packet to retransmit that lost packet. The sender has to keep just one packet on hand for retransmission, because the lock step acknowledgement guarantees that all older packets have been received. Notice that both machines involved in a transfer are considered senders and receivers. One sends data and receives acknowledgements, the other sends acknowledgements and receives data. Three modes of transfer currently supported by TFTP are netascii (that it is 8 bit ascii) octet (raw 8 bit bytes), mail, netascii characters sent to a user rather than a file. Also additional modes can be defined by pairs of cooperating hosts.

5.3.2 Difference between FTP and TFTP

Sr. No.	FTP	TFTP
1.	FTP uses two connections	TFTP uses one connection
2.	Provides many commands	Provides only five commands
3.	Uses TCP	Uses UDP

- Fig. 5.4.1 shows the high-level view of the internet e-mail system.
- Mail server handles incoming and outgoing mails.
- The Post Office Protocol (POP) servers store incoming mail while SMTP servers relay outgoing mails.
- The Internet Service Provider (ISP) probably runs both an SMTP server and POP server for its customers.

Following are the ways to access the e-mail.

1. Web based e-mail service.
2. E-mail through a LAN.
3. Unix shell account.
4. Using mail client.

Components

Three major components are

1. User agents.
2. Mail servers.
3. SMTP.

Fig. 5.4.2 shows the components of an e-mail system.

5.4.1 E-mail Addressing

- To send e-mail to some one, the Internet e-mail address must be known to sender. E-mail addresses look like this : @hotmail.com.
- The e-mail address has two main parts, joined by @. In this example, vilas is the username. Username can contain numbers, underscores, periods and some other special characters. Commas, spaces and parentheses are not allowed.
- Hotmail.com is the host or domain name. E-mail address is case insensitive. **Vilas@hotmail.com** works just the same as **vilas@hotmail.com**. E-mail addresses do not have punctuation marks around them.

5.4.2 Message Headers

The message headers include the addresses of the receiver and the sender. Each header consists of the type of header, a colon, and the content of the header. Following is the sample of the complete header for a message.

Table shows the list of standard header.

```
Received:from del2..net.in(del2.vsnl.net.in [202.54.15.30])
by giaspn01.vsnl.net.in (8.9.0/8.9.0) with ESMTP id
MAA22885
for<siitpune@giaspn01.vsnl.net.in>;wed,19 jul 2000
    12:42:33+0530 (IST)
Received: from oemcomputer ([202.54.109.165])
by del2.vsnl.net.in (8.9.2/8.9.2)with SMTP id MAA12595
for<siitpune@giaspn01.vsnl.net.in>;wed, 19 Jul 2000
12:47:52-0500 (GMT)
Reply-To: <kanohar@del2.vsnl.net.in>
From:"SachinMahadik" <kanohar@del2.vsnl.net.in>
To: <siitpune@giaspn01.vsnl.net.in>
Subject: admission
Date: Wed, 19 Jul 2000 12:43:31 +530
Message-ID:<LPBBKDKDNBJBIDPNDOLHOECOCBAA.kano
har@del2.vsnl.net.in>
MIME-version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
```

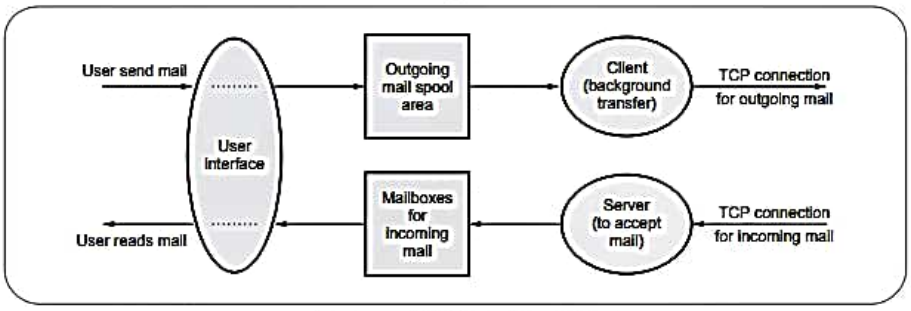


Fig. 5.4.2 Component of e-mail system

- Fig. 5.4.1 shows the high-level view of the internet e-mail system.
- Mail server handles incoming and outgoing mails.
- The Post Office Protocol (POP) servers store incoming mail while SMTP servers relay outgoing mails.
- The Internet Service Provider (ISP) probably runs both an SMTP server and POP server for its customers.

Following are the ways to access the e-mail.

1. Web based e-mail service.
2. E-mail through a LAN.
3. Unix shell account.
4. Using mail client.

Components

Three major components are

1. User agents.
2. Mail servers.
3. SMTP.

Fig. 5.4.2 shows the components of an e-mail system.

5.4.1 E-mail Addressing

- To send e-mail to some one, the Internet e-mail address must be known to sender. E-mail addresses look like this : @hotmail.com.
- The e-mail address has two main parts, joined by @. In this example, vilas is the username. Username can contain numbers, underscores, periods and some other special characters. Commas, spaces and parentheses are not allowed.
- Hotmail.com is the host or domain name. E-mail address is case insensitive. **Vilas@hotmail.com** works just the same as **vilas@hotmail.com**. E-mail addresses do not have punctuation marks around them.

5.4.2 Message Headers

The message headers include the addresses of the receiver and the sender. Each header consists of the type of header, a colon, and the content of the header. Following is the sample of the complete header for a message.

Table shows the list of standard header.

```
Received:from del2..net.in(del2.vsnl.net.in [202.54.15.30])
by giaspn01.vsnl.net.in (8.9.0/8.9.0) with ESMTP id
MAA22885
for<siitpune@giaspn01.vsnl.net.in>;wed,19 jul 2000
    12:42:33+0530 (IST)
Received: from oemcomputer ([202.54.109.165])
by del2.vsnl.net.in (8.9.2/8.9.2)with SMTP id MAA12595
for<siitpune@giaspn01.vsnl.net.in>;wed, 19 Jul 2000
12:47:52-0500 (GMT)
Reply-To: <kanohar@del2.vsnl.net.in>
From:"SachinMahadik" <kanohar@del2.vsnl.net.in>
To: <siitpune@giaspn01.vsnl.net.in>
Subject: admission
Date: Wed, 19 Jul 2000 12:43:31 +530
Message-ID:<LPBBKDKDNBJBIDPNDOLHOECOCBAA.kano
har@del2.vsnl.net.in>
MIME-version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
```

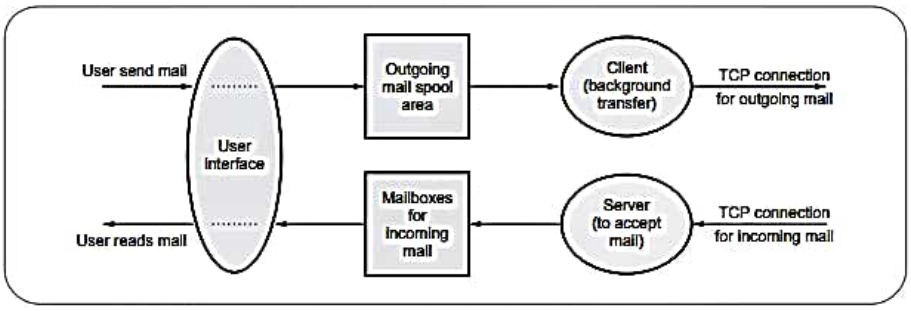


Fig. 5.4.2 Component of e-mail system

2. Transfer : It is moving messages from the originator to the receiver.
3. Reporting : It inform the originator what happened to the message. Whether, email is delivered or not delivered.
4. Displaying : Display is required for reading the email.
5. Disposition is the last step and related what the receiver does with the message after receiving it. It may be read and save or delete or forward the message.

5.4.5 User Agent and Message Transfer Agent

E-mail system consists of two subsystems.

1. User agent
2. Message transfer agent.

1. User Agent (UA)

- User agent is an interface between user and network application.
- It allow user to read and send e-mail. The user agents are local program that provide a command based, menu based or graphical method for interacting with the e-mail system.
- To send an e-mail message, a user must provide the data and the destination address. The destination address should be in proper format and the user agent can deal with destination address. Details of e-mail address, we already studied in email addressing section.
- Most e-mail system support mailing lists, so that a user can send the same message to a list of people with a single command.
- For reading e-mail, the user agent will look at the user's mail box for incoming e-mail before displaying anything on the screen. It display total number of new mail.

2. Message transfer agent

- Message Transfer Agent (MTA) move the messages from the source to the destination. MTA are system program that run in the background and move e-mail through the system.
- After writing the mail, user click of send icon. MTA activates at this time, MTA checks the destination address and transfer the mail to proper destination on the network.
- MTA use different types of protocol for moving the message from source to destination.

1. It must handle temporary failures, if a destination machine is temporarily unavailable, it must spool the message on the local machine for later delivery.
2. MTA must distinguish between local and remote destinations.
3. It may have to deliver copies of a message to several machines.
4. It may allow mixing text, voice and video in a message as well as appending documents and files to a message.

- MTA works in background, while the user usually interacts directly with a user agent.

5.4.6 Simple Mail Transfer Protocol (SMTP)

- SMTP is application layer protocol of TCP/IP model.
- SMTP transfers message from sender's mail servers to the recipients mail servers.
- SMTP interacts with the local mail system and not the user.
- SMTP uses a TCP socket on port 25 to transfer e-mail reliably from client to server.
- E-mail is temporarily stored on the local and eventually transfered directly to receiving server.
- Client / Server interaction follows and commond/reponse paradigm.

a] Commands are plain ASCII text.

b] Responses are a status code and an optional phase.

c] Command and response lines terminated with CRLF.

- Mail client application interacts with a local server to initiate the delivery of an e-mail message.
- There is an input queue and an output queue at the interface between the local mail system and the client and the server parts of the .
- The client is concerned with initiating the transfer of mail to another system while server is concerned with receiving mail. Before the e-mail message can be transferred, the application process must be set

up a TCP connection to the local SMTP server. The local mail system retains a mailbox for each user into which the user can deposit or retrieve mail. Mail handling system must use a unique addressing system.

- Addressing system used by SMTP consists of two parts : A local part and a global part. The local part is the user name and is unique only within that local mail system. Global part of the address is the domain name. Domain name is identity of the host, must be unique within the total internet.
- SMTP uses different types of component. They are MIME and POP.

Scenario : Alice sends message to Bob

1. Alice uses User Agent (UA) to compose message and send to bob@technical.org.
2. Alice's UA sends message to her mail server, message placed in message queue.
3. Client side of SMTP opens TCP connection with Bob's mail server.
4. SMTP client sends Alice's message over the TCP connection.
5. Bob's mail server places the message in Bob's mailbox.
6. Bob invokes his user agent to read message.

- SMTP uses commands and responses to transfer messages between an MTA client and an MTA server.
- Each command or reply is terminated by a two character end of line token.
- Commands are sent from the client to the server. SMTP defines 14 commands.

SMTP commands consist of human readable ASCII strings.

SMTP commands are,

i) **HELO :** Initiate a mail transaction, identifying the sender to the recipient.

ii) **MAIL FROM :** Tells the remote SMTP that a new mail transaction is beginning.

iii) **RCPT TO :** The sending SMTP sends a RCPT command for each intended receiver.

iv) **DATA :** If accepted, the sender transfers the actual message. End of message is indicated by sending a " • " on a line by itself.

v) **QUIT :** Terminate the connection.

Sample SMTP Interaction

- Following are messages exchanged between an SMTP client (C) and an SMTP server (S).
- The host name of the client is iresh.fr and the host name of the server is sinhgad.edu.

S : 220 sinhgad.edu

C : HELO iresh.fr

S : 250 Hello iresh.fr, pleased to meet you

C : MAIL FROM : <rupali@iresh.fr>

S : 250 rupali@iresh.fr ... sender ok

C : RCPT TO : < rakshita@sinhgad.edu>

S : 250 rakshita@sinhgad.edu ..... Recipient ok

C : DATA

S : 354 Enter Mail, end with "." on a line by itself

C : Do you like Apple ?

C : What about school ?

C : .

S : 250 message accepted for delivery

C : QUIT

S : 221 sinhgad.edu closing connection

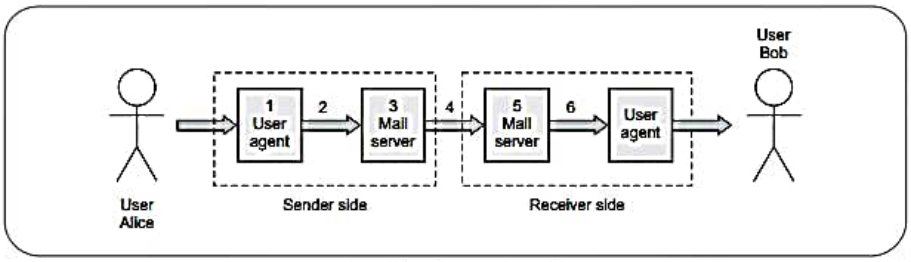


Fig. 5.4.4 Message Scenario

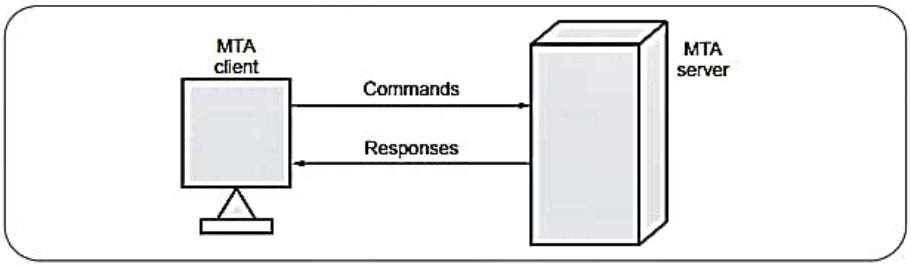


Fig. 5.4.5 Command / Response

5.4.7 Multipurpose Internet Mail Extensions

- MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP.
- MIME defined by IETF to allow transmission of non-ASCII data via e-mail.
- It allows arbitary data to be encoded in ASCII for normal transmission.
- All media types that are sent or received over the world wide web (www) are encoded using different MIME types.
- Messages sent using MIME encoding include information that describes the type of data and the encoding that was used.
- RFC822 specifies the exact format for mail header lines as well as their semantic interpretations.
- Fig. 5.4.6 shows the working of MIME.
- MIME define five headers.

1. MIME - Version
2. Content - Type
3. Content - Transfer - Encoding
4. Content - Id
5. Content - Description

Mail Message Header

- From : iresh@e-mail.com
- TO : rupali@sinhgad.edu
- MIME - Version : 1.0
- Content - Type : image/gif
- Content - Transfer - Encoding : base64

..... data for the image .....

....

....

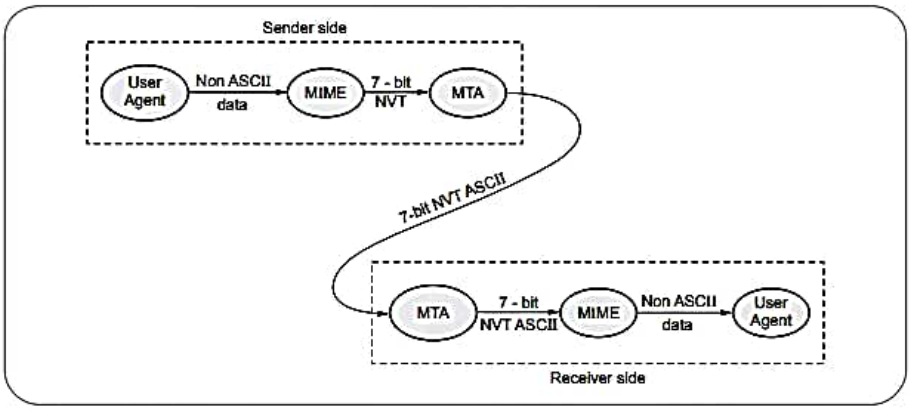


Fig. 5.4.6 MIME

MIME Types and SubTypes

- Each MIME content - type must contain two identifiers:
  - Content type
  - Content subtype
- There are seven standardized content-types that can appear in a MIME

Content - type declaration

Type	Subtype	Description
Text	Plain	Unformatted text.
Multipart	Mixed	Body contains ordered parts of different data types.
	Parallel	Same as above, but no order.
	Digest	Similar to mixed, but the default is message.
	Alternative	Parts are different versions of the same message.
Video	MPEG	Video is in MPEG format.
Audio	Basic	Single channel encoding of voice at 8kHz. (Sound file)
Image	JPEG	Image is in JPEG format.
	GIF	Image is in GIF.
Message	Partial and external body	An entire e-mail message or an external reference to a message.
Application	Postscript	Adobe postscript.
	Octet stream	General binary data.

Content - Transfer Encoding

- This header defines the method to encode the messages into 0 and 1 for transport.

Content-Transfer-Encoding : < Type >

The five types of encoding is listed below.

Type	Description
7-bit	ASCII characters and short lines.
8-bit	Non-ASCII characters and short lines.
Binary	Non-ASCII characters with unlimited length lines.
Base 64	6-bit blocks of data are encoded into 8-bit ASCII characters.
Quoted printable	Non-ASCII characters are encoded as an equal sign followed by an ASCII code.

5.4.8 Post Office Protocol (POP)

- Post Office Protocol 3 (POP3) is used to transfer e-mail messages from a mail server to mail client software.
- Fig. 5.4.7 shows working of POP3.

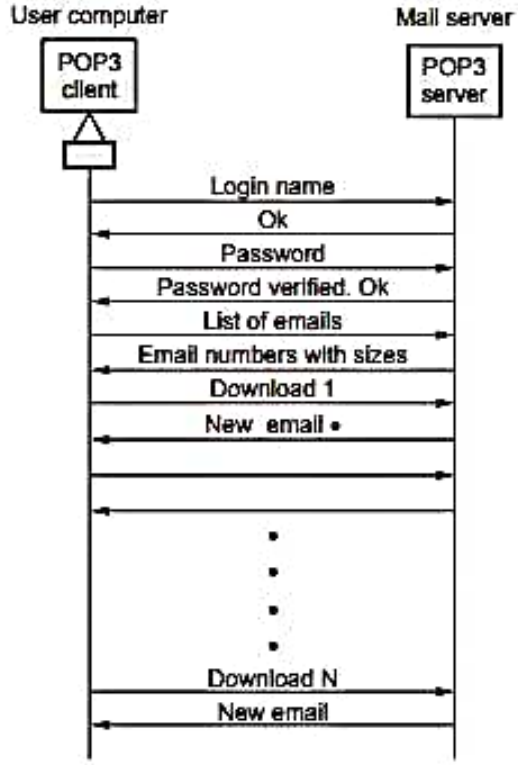


Fig. 5.4.7 POP3

- POP3 begins when the user agent opens a TCP connection to the mail server on port 110.
- After TCP connection established, POP3 progresses three phases :
  - i) Authorization
  - ii) Transaction
  - iii) Update
- In authorization phase, user agent sends a user name and a password to authenticate the user downloading the mail.
- In transaction phase, the user agent retrieves messages. In this phase, user agent can also mark messages for deletion, remove deletion marks.
- In update phase, it occurs after the client has issued the quit command, ending the POP3 session.
- POP3 has two modes : Delete mode and the keep mode.
- In the delete mode, mail is deleted from the mailbox after each retrieval.
- In the keep mode, the mail remains in the mailbox after retrieval.

Limitations of POP3

1. POP3 does not allow the user to organize mail on the server, the user cannot have different folders on the server.
2. POP3 does not allow the user to partially check the contents of the e-mail before downloading.

5.4.9 IMAP

- IMAP is the Internet Mail Access Protocol. IMAP4 is more powerful and more complex. IMAP is similar to SMTP.

Status line	HTTP / 1.1 300 ok
General headers	Date : Wed , 8 Oct 2014 13:00:13 GMT
	Connection : close
Entity headers	Server : Apache / 1.3.27
	Accept-range : bytes
	Content-type : text / html
	Content-length : 200
	Last-modified : 2 Oct 2014 13:00:13 GMT
Blank line	
Message body	<html> <head> <title> Welcome to the India <title> <head> <body>

- IMAP allows users to store their email on remote server.
- It was designed to help the user who uses multiple computers.
- IMAP does not copy e-mail to the user's personal machine because the user may have several.
- An IMAP client connects to a server by using TCP.
- IMAP supports the following modes for accessing e-mail messages :

  i) Offline mode ii) Online mode

  iii) Disconnected mode

Offline mode : A client periodically connects to the server to download e-mail messages. After downloading, messages are deleted from the server. POP3 support this mode.

Online mode : Client process e-mail messages on the server. The e-mail messages are stored on the server itself but are processed by an application on the client's end.

Disconnected mode : In this mode, both offline and online modes are supported.

IMAP4 provides the following extra functions :

1. User can check the e-mail header prior to downloading.
2. User can partially download e-mail.
3. A user can create, delete or rename mailboxes on the mail server.
4. A user can create a hierarchy of mailboxes in a folder for e-mail storage.
5. User can search the contents of the e-mail for a specific string of characters.

- The IMAP protocol provides commands to allow users to create folders and move messages from one folder to another.

Fig. 5.4.8 shows state transition diagram.

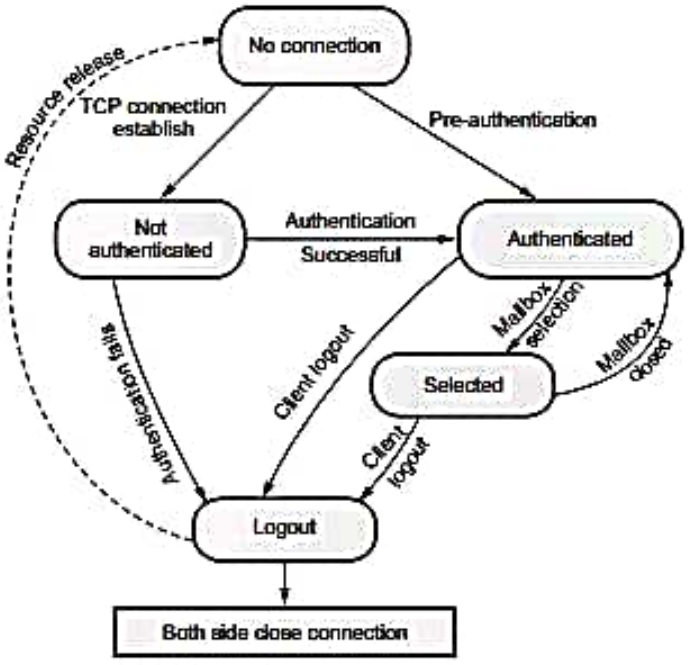


Fig. 5.4.8 IMAP state diagram

1. **Not authenticated :** Client provides authentication information to the server.
2. **Authenticated :** Server verify the information and client is now allowed to perform operations on a mailbox.
3. **Selected :** Client is allowed to access manipulated individual messages within the mailbox.
4. **Logout :** Client send logout command for closing session.

5.5 DNS

- **Goal :** Assign meaningful high-level names to a large set of machines and handle the mapping of those names to a machine's IP address.
- The DNS is a distributed database that resides on multiple machines on the internet and used to convert between names and address and to provide e-mail routing information.
- DNS provides the protocol that allows the client and servers to communicate with each other.
- Domain names are case insensitive so **com** and **COM** mean the same thing.
- The **DNS** protocol runs over **UDP** and uses port 53.
- The **DNS** is specified in **RFC 1034** and **RFC 1035.**
- The **DNS** protocol is the application layer protocol.
- A full domain name is a sequence of labels separated by dots (.).
- The **DNS** name space is hierarchical and it is similar to the unix file system.

Originally, the internet was small and mapping between names and addresses was accomplished using a centrally-maintained file called *hosts.txt*. To add a name or change an address required contacting the central administrator, updating the table, and distributing it to all the other sites. This solution worked at first because most sites had only a few machines, and the table didn't require frequent changes. **The centrally-maintained table suffered from several drawbacks :**

1. The name space was *flat*, and no two machines could use the same machine name.
2. As the internet grew, changes to the database took days to weeks to take effect.
3. The central site became congested with the increase in the number of sites retrieving copies of the current table.
4. The internet grew at an astonishing rate.

The Domain Name System (DNS) is a hierarchical, distributed naming system designed to cope with the problem of explosive growth :

1. It is *hierarchical* because the name space is partitioned into *subdomains*.
2. It is distributed because management of the name space is delegated to local sites. Local sites have complete control (and responsibility) for their part of the name space. DNS queries are handled by servers called *name servers*.
3. It does more than just map machine names to internet addresses. For example, it allows a site to associate multiple machines with a single, mailbox name.

In the DNS, the name space is structured as a tree, with *domain names* referring to nodes in the tree. The tree has a *root*, and a *fully-qualified* domain name is identified by the *components* of the path from the domain name to the root.

Services provided by DNS :

- **Host aliasing :** A host with complicated hostname can have one or more alias names. DNS can be invoked by an application to obtain the canonical hostname for a supplied alias hostname as well as the IP address of the host.
- **Mail server aliasing :** DNS can be invoked by a mail application to obtain the hostname for a supplied alias hostname as well as the IP address of the host.
- **Load distribution :** DNS is also used to perform load distribution among replicated servers.

5.5.1 Components of DNS

DNS includes following components

1. Domain 2. Domain name
3. Name server 4. Name resolver
5. Name cache 6. Zone

1) For example, vtubooks.com is the site for technical publications. Here com is the domain.
2) Domain name is defined by the DNS as being the sequence of names and domain. For example, vtubooks.com could be domain name.
3) In name server, software (program) that maps names to addresses. It does this by mapping domain names to IP addresses.
4) Name resolver is a software that functions as a client interacting with a name server.

5) Name cache is the storage used by the name resolver to store information frequently used.

6) Zone is a contiguous part of a domain.

5.5.2 DNS in the Internet

DNS is divided into three different sections in the internet i.e. Generic domain, Country domain and Inverse domain.

- Fig. 5.5.1 shows the DNS in the internet.

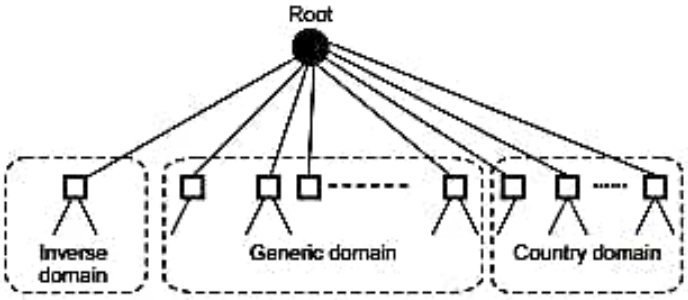


Fig. 5.5.1 DNS in the Internet

Generic Domains

- Each node in the tree defines a domain, which is an index to the domain name space database.
- Generic domain labels are as follows

Sr. No.	Label	Description
1.	com	Commercial organization
2.	edu	Educational organization
3.	gov	Government Institutions
4.	int	International organizations
5.	mil	Military group
6.	net	Network support centers
7.	org	Nonprofit organization

- Fig. 5.5.2 shows the generic domains

Country Domains

- It uses two character country abbreviations at first level. Second level labels can be more specific, national destinations. For India, the country domain is in. (See Fig. 5.5.3)

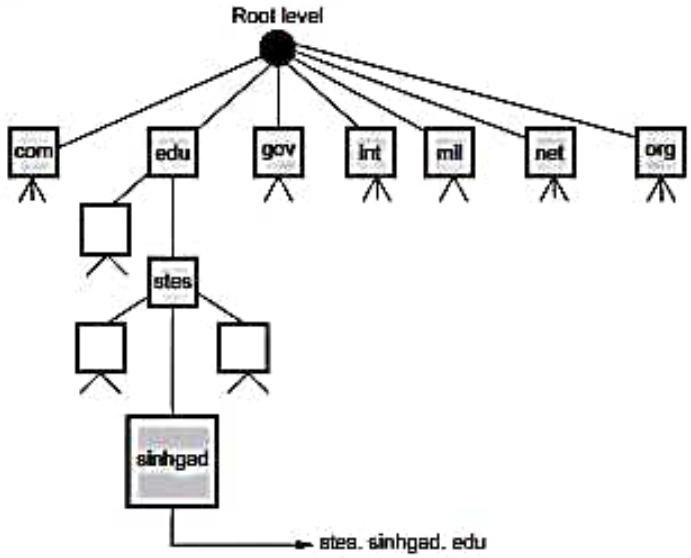


Fig. 5.5.2 Generic domains

- Fig. 5.5.3 shows country domains.

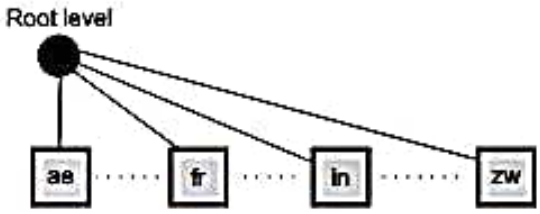


Fig. 5.5.3 Country domains

Inverse Domain

- Used to map an address to a name.
- Example : When a client send a request to the server for doing a particular task, server finds the list of authorized client. The list contains only IP address of the client.
- Server send a query to the inverse DNS server and ask for a mapping of address to name for authorized client list.
- The above query is called an inverse or pointer query.
- The pointer query is handled by the first level node called arpa. The second level is also one single node named in-addr. The rest of the domain defines IP addresses.

Fig. 5.5.4 shows inverse domain.

5.5.3 Name Spaces

- Name spaces are of two types : Flat name spaces and Hierarchical names.
- The name assigned to machines must be carefully selected from a name space with complete control over the binding between the names and IP addresses.

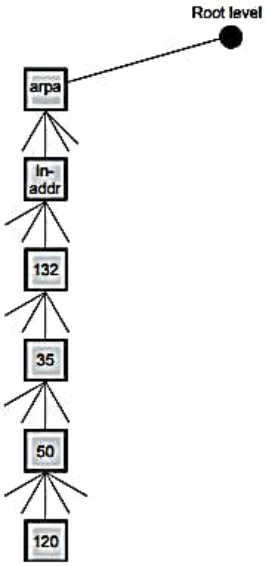


Fig. 5.5.4 Inverse domain

i) Flat name spaces :

- The original set of machines on the Internet used flat namespaces.
- These namespaces consisted of sequence of characters with no further structure.
- A name is assigned to an address.
- **Advantage :**
  1. Names were convenient and short.
- **Disadvantages :**
  1. Flat name spaces cannot generalize to large sets of machines because of the single set of identifiers.
  2. Single central name authority was overloaded.
  3. Frequent name-address binding changes were costly and cumbersome.

ii) Hierarchical names

- The partitioning of a namespace must be defined in such a way that it :
  - Supports efficient name mapping.
  - Guarantees autonomous control of name assignment.
- Hierarchical namespaces provides a simple yet flexible naming structure.
- The namespace is partitioned at the top level.
- Authority for names in each partition are passed to each designated agent.
- The names are designed in an inverted-tree structure with the root at the top.
- The tree can have only 128 levels.

The top level domains are divided into three areas :

1. Arpa is a special domain used for the address-to-name mappings.
2. The 3 character domains are called the generic domains.
3. The 2 character domains are based on the counter codes found in ISO 3166. These are called the country domains.

- Fig. 5.5.5 shows the hierarchy of DNS.

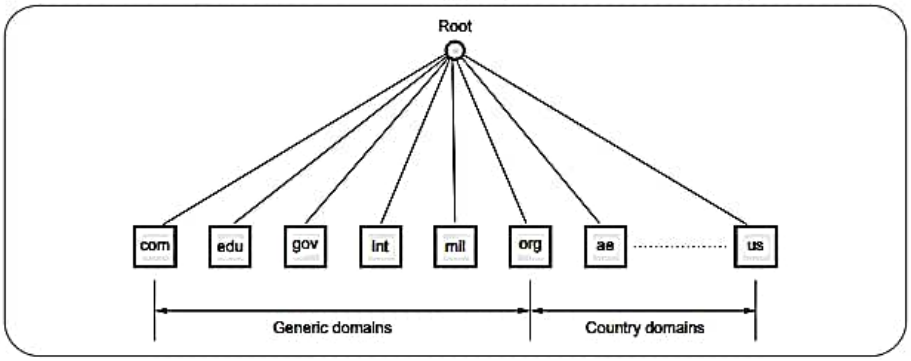


Fig. 5.5.5 Hierarchy of DNS

5.5.4 Domain Name Space

- In DNS, names are defined in an inverted tree structure with the root at the top. The tree can have only 128 levels : Level 0 to Level 127.
- Each node in the tree has a label, which is a string with a maximum of 63 characters. The root label is a null string , i.e. empty string.
- Each node in the tree has a domain name, a full domain name is a sequence of labels separated by dots(.). Fig. 5.5.6 shows the domain names and labels.

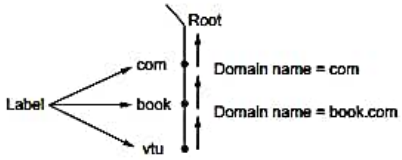


Fig. 5.5.6 Domain names and label

- In fully qualified domain name, label is terminated by a null string. Fully Qualified Domain Name (FQDN) contains the full name of host. All labels are part of FQDN.
- Partially Qulified Domain Name (PQDN) : In this label is not terminated by a null string. It always start from node. A domain name does not include all the levels between the host and the root node. For example, vtu.book.com.

Hierarchy of Name Servers

- To distribute the information among many computers, DNS servers are used. Creates many domains as there are first level nodes. Fig. 5.5.7 shows hierarchy of name servers.
- **Zone** : Server have some authority and also responsible for operation. Server creates database, which is called zone file. Server maintain all the information about node of that domain.
- Fig. 5.5.8 shows domain with zone.

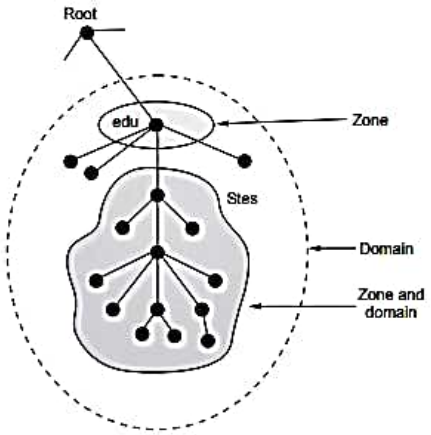


Fig. 5.5.8 Domain and zone

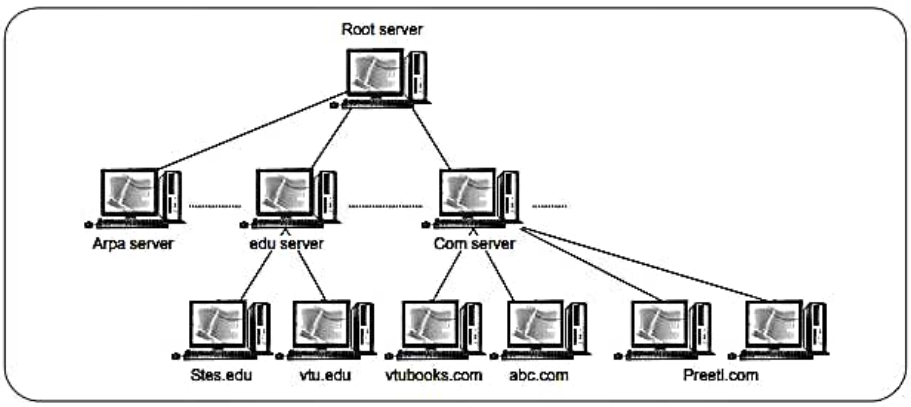


Fig. 5.5.7 Hierarchy of name server

- Domain and zone are same if server accepts responsibillity for a domain and does not divide the domain into **subdomian.**
- Domain and zone are different, if a server divides its domain into subdomains and delegates part of its authority to other server.
- **Root server :** If zone consists of the full tree then that zone server is called root server. Root server do not maintain any information about domains.
- DNS uses two types of servers :

1. Primary server 2. Secondary server

- **Primary server :** This server keeps a file about the zone for which it is responsible and have authority. It performs operation on zone file like create, update and maintaining.
- **Secondary server :** It loads all information from the primary server. Secondary server can not perform any operation on zone file.

5.5.5 Resolution

- DNS is designed as a client server application. A host that needs to map an address to a name or a name to an address calls a DNS client named a **resolver.**

Working :

- Name resolving must also include the type of answer desired (specifying the protocol family is optional).
- The DNS partitions the entire set of names by class (for mapping to multiple protocol suites).
- Naming items is required since one cannot distinguish the names of subdomains from the names of individual objects or their types.

Mapping Domain Names to Addresses :

a) The DNS also includes an efficient, reliable, general purpose, distributed system for mapping names to addresses using an independent co-operative system called name servers.

b) Names Servers - are server programs that translate names-to-addresses (maps DN => IP addresses) and usually executes on a dedicated processor.

c) Name Resolvers - client software that uses one or more name servers in getting a mapped name.

d) Domain name servers are arranged in a conceptual tree structure that corresponds to the naming hierarchy.

Recursive Resolution

- A client request complete translation.
- If the server is authority for the domain name, it checks its database and responds.
- If the server is not authority, it sends the request to another server and waits for the response.
- When the query is finally resolved, the response travel back until it finally reaches the requesting client. This is called recursive resolution.
- Fig. 5.5.9 shows the recursive resolution.

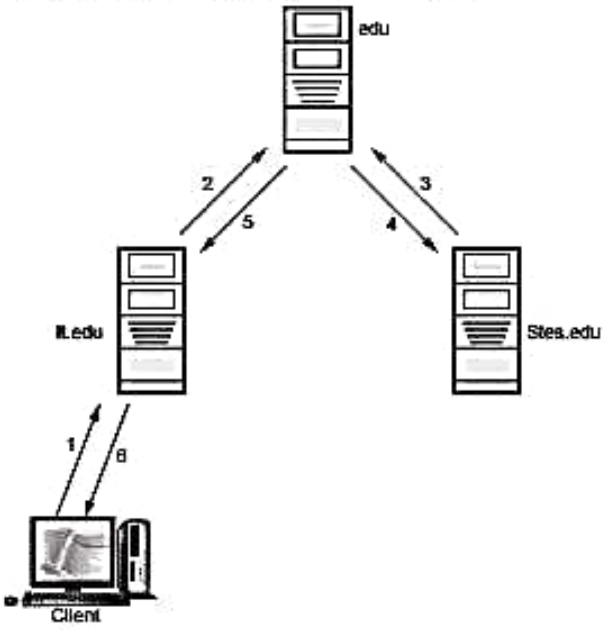


Fig. 5.5.9 Recursive resolution

Iterative Resolution

- Only a single resolution is made and returned (not recursive).
- Client must now explicitly contact different name servers if further resolution is needed.
- If the server is an authority for the name, it sends the answer. If it is not, it returns the IP address of the server that it thinks can resolve the query. The client is responsible for repeating the query to this second server. This process is called iterative resolution because the client repeats the same query to multiple servers.
- Fig. 5.5.10 shows iterative resolution.

- Domain and zone are same if server accepts responsibillity for a domain and does not divide the domain into **subdomian.**
- Domain and zone are different, if a server divides its domain into subdomains and delegates part of its authority to other server.
- **Root server :** If zone consists of the full tree then that zone server is called root server. Root server do not maintain any information about domains.
- DNS uses two types of servers :

1. Primary server 2. Secondary server

- **Primary server :** This server keeps a file about the zone for which it is responsible and have authority. It performs operation on zone file like create, update and maintaining.
- **Secondary server :** It loads all information from the primary server. Secondary server can not perform any operation on zone file.

5.5.5 Resolution

- DNS is designed as a client server application. A host that needs to map an address to a name or a name to an address calls a DNS client named a **resolver.**

Working :

- Name resolving must also include the type of answer desired (specifying the protocol family is optional).
- The DNS partitions the entire set of names by class (for mapping to multiple protocol suites).
- Naming items is required since one cannot distinguish the names of subdomains from the names of individual objects or their types.

Mapping Domain Names to Addresses :

a) The DNS also includes an efficient, reliable, general purpose, distributed system for mapping names to addresses using an independent co-operative system called name servers.

b) Names Servers - are server programs that translate names-to-addresses (maps DN => IP addresses) and usually executes on a dedicated processor.

c) Name Resolvers - client software that uses one or more name servers in getting a mapped name.

d) Domain name servers are arranged in a conceptual tree structure that corresponds to the naming hierarchy.

Recursive Resolution

- A client request complete translation.
- If the server is authority for the domain name, it checks its database and responds.
- If the server is not authority, it sends the request to another server and waits for the response.
- When the query is finally resolved, the response travel back until it finally reaches the requesting client. This is called recursive resolution.
- Fig. 5.5.9 shows the recursive resolution.

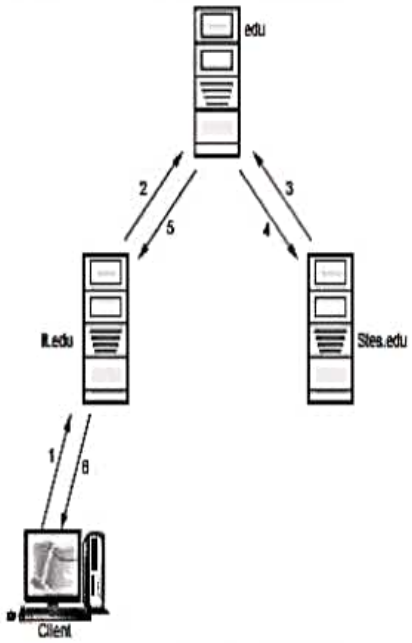


Fig. 5.5.9 Recursive resolution

Iterative Resolution

- Only a single resolution is made and returned (not recursive).
- Client must now explicitly contact different name servers if further resolution is needed.
- If the server is an authority for the name, it sends the answer. If it is not, it returns the IP address of the server that it thinks can resolve the query. The client is responsible for repeating the query to this second server. This process is called iterative resolution because the client repeats the same query to multiple servers.
- Fig. 5.5.10 shows iterative resolution.

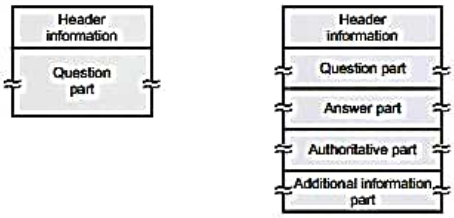


Fig. 5.5.11 Query and response message

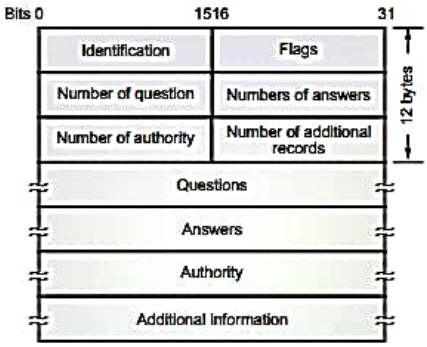


Fig. 5.5.12 General format of DNS

- Number of answer record contains the number of answer records in the answer section of the response message.
- Number of authority record contains the number of authority records in the authoritative section of the response message.
- Number of additional records contains the number of additional records in the additional section of the response message. The message has a fixed 12-byte header followed by 4 variable length fields. The identification field is set by client and returned by the server. It lets the client, match responses to requests.
- Fig. 5.5.13 flag fields in DNS header.
- The flags field is divided into 8 parts.

QR = 0 For message is a query
= 1 It is response
Opcode = 0 Standard query
= 1 Inverse query
= 2 Server status request
AA = Authoritative answer
TC = Truncated
RD = Recursive query
RA = Recursion available
r code = Return code

- RD field is 1-bit and can be set in a query and is then returned in the response. This flag tells the name server to handle the query itself, called a recursive query.
- RA is a 1-bit field and set to 1 in the response if the server support recursion. There is a 3-bit field that must be zero.
- r code is a 4-bit field. The common value are 0 for no error and 3 for name error. A name error is returned only from an authoritative name server and means the domain name specified in the query does not exist.
- The next four 16-bit fields specify the number of entries in the four variable length fields that complete the record.

5.5.7 Resource Records

- Different types of resource records are used in DNS. An IP address has a type of A and PTR means pointer query.
- There are about 20 different types of resource records available. Some PR are listed below.

1) A = It defines an IP address. It is stored as a 32-bit binary value.
2) CNAME = "Canonical name". It is represented as a domain name.
3) HINFO = Host information, two arbitrary character strings specifying the CPU and operating system (OS).

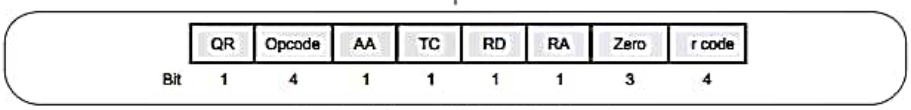


Fig. 5.5.13 Flags field in the DNS header

4) MX = Mail exchange records. It provide domain willing to accept e-mail.

5) PTR = Pointer record used for pointer queries. The IP address is represented as a domain name in the in-addr.arpa domain.

6) NS = Name Server record. These specify the authoritative name server for a domain. They are represented as domain names.

A) Configuration of DNS :

The DNS server can be configured manually by editing files in the default WINNT installation path \% SYSTEM ROOT %\ SYSTEM 32 \ DNS. Administration is identical to administration in traditional DNS. These files can be modified using a text editor. The DNS service must then be stopped and restarted.

5.5.8 Name Servers

- When a resolver has a query about a domain name, it passes the query to one of the local name servers. If the domain is remote and no information about the requested domain is available locally, the name server sends a query message to the top level name server for the domain requested.
- Fig. 5.5.14 shows the eight steps for resolving the remote name.

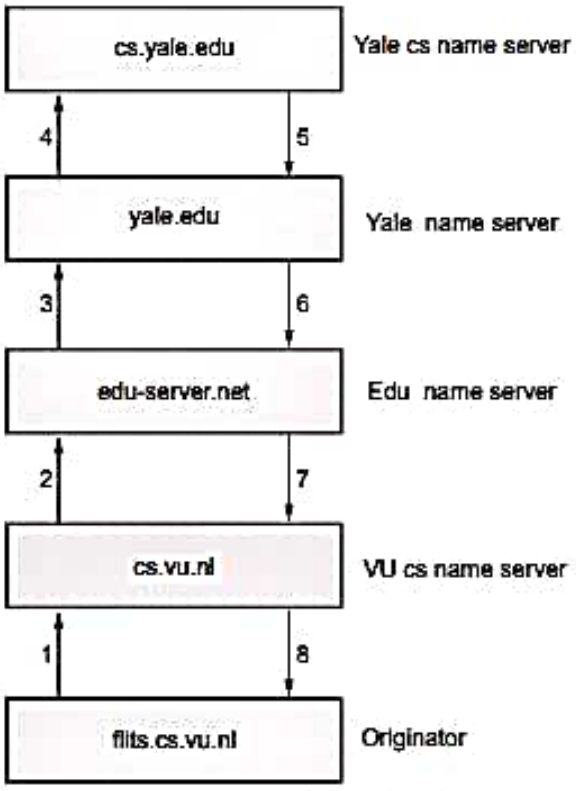


Fig. 5.5.14 Remote name resolve

- A resolver on flits.cs.vu.nl wants to know the IP address of the host linda.cs.yale.edu.

Steps

1. It sends a query to the local name server cs.vu.nl. This query contains the domain name, sought, the type (A) and the class (IN).
2. and 3. Suppose the local name server has never had a query for this domain before and knows nothing about it. It may ask a few other nearby name servers, but if none of them know, it sends a UDP packet to the server for edu given in its database, edu-server.net. This server knows all its children, so it forwards the request to the name server for yale.edu.
4. This forwards the request to cs.yale.edu, which must have the authoritative resource records.
5. to 8. Each request is from a client to a server, the resource record requested works its way back in these steps.

5.5.9 LDAP

- LDAP is Lightweight Directory Access Protocol. It provides X-500 features. LDAP is an application-level protocol that is implemented directly on top of TCP.
- It stores entries, which is similar to objects. Each entry must have a distinguished name, which un-equally identifies the entry. Entries can also have attributes.
- LDAP provides binary, string and time types. It allows the defination of object classes with attribute name of types. Entries are organized into a directory information tree, according to their distinguished names.
- LDAP defines a network protocol for carrying out data defination and manipulation.
- LDAP has been widely adopted, particularly for internet directory services. It provides secured access to directory data through authentication.

5.5.10 Dynamic Domain Name System (DDNS)

- DDNS is a service that maps internet domain names to IP addresses. DDNS serves a similar purpose to DNS : DDNS allows anyone hosting a Web or FTP server to advertise a public name to prospective users.

- Unlike DNS that only works with static IP addresses, DDNS works with dynamic IP addresses, such as those assigned by an ISP or other DHCP server. DDNS is popular with home networkers, who typically receive dynamic, frequently-changing IP addresses from their service provider.
- To use DDNS, one simply signs up with a provider and installs network software on their host to monitor its IP address.
- Compared to ordinary DNS, the disadvantage of DDNS is that additional host software, a new potential failure point on the network, must be maintained.

5.6 DHCP

- BOOTP is a static configuration protocol. Each client has a permanent network connection.
- When a client requests its IP address, the BOOTP server consults a table that matches the physical address of the client with its IP address. The binding is predefined.
- If the client moves from one physical network to another then it creates problem. Wireless networking and portable computer i.e. laptops and notebooks may move from one network to another.
- BOOTP cannot handle these situations because the binding between the physical and IP addresses is static and fixed in a table until changed by the system administrator.

DHCP

- DHCP provides static and dynamic address allocation that can be manual or automatic.
- DHCP does not require an administrator to add an entry for each computer to the database that a server uses. DHCP provides a mechanism that allows a computer to join a new network and obtain an IP address without manual intervention. The DHCP work like **plug and play networking**.
- DHCP is in wide use because it provides a mechanism for assigning temporary IP network address to hosts. This capability is used extensively by Internet service providers to maximum the usage of their limited IP addresses space.
- DHCP has a pool of available IP addresses. When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available IP addresses (unused IP addresses) and assigns an IP address for a negotiable period of time.
- An administrator can configure a DHCP server to have two types of addresses: permanent addresses that are assigned to server computers, and a pool of addresses to be allocated on demand. When a computer boots and send a request to DHCP, the DHCP server consults its database to find configuration information.
- DHCP uses a same technique as BOOTP : each computer waits a random time before transmitting or retransmitting a request. When a host wishes to obtain an IP address the host broadcasts a DHCP discover message in its physical network. The server in the network may respond with a DHCP offer message that provides an IP address and other configuration information.
- When a computer discovers a DHCP server, the computer saved the server's address in a cache on permanent storage. Once it obtains an IP address, the computer saves the IP address in a cache.

5.6.1 DHCP Message Format

Fig. 5.6.1 shows the DHCP message format.

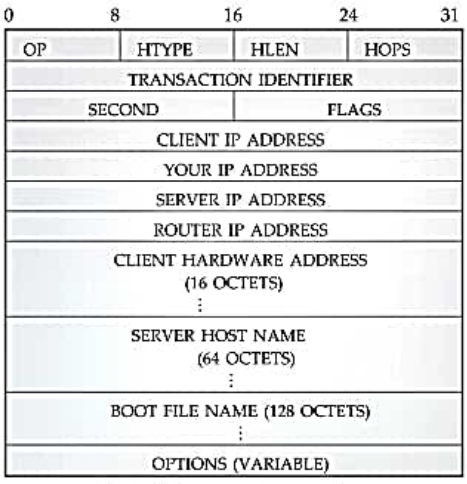


Fig. 5.6.1 The DHCP message format

- **OP field** - Specifies whether the message is a request or a response.

- **HTYPE** - It specifies the network hardware type.
- **HLEN** - Specifies length of a hardware address.
- **HOPS** - Specifies how many servers forwarded the request.
- **TRANSACTION IDENTIFIER** - This field provides a value that a client can use to determine if an incoming response matches its request.
- **CLIENT IP ADDRESS** - Computer fills this field in a request.
- **YOUR IP ADDRESS** - Server uses this field to supply the value if computer does not know its address.
- **SERVER IP ADDRESS and SERVER HOST NAME** - Use by server to give the computer information about the location of a computer that runs server.
- **ROUTER IP ADDRESS FIELD** - Contains then IP address of default router.
- **FLAGS and OPTIONS FIELD** - Use to encode additional information. To distinguish among various messages that a client uses to discover servers or request an address or that a server uses to acknowledge.

5.6.2 Working of DHCP

- A DHCP infrastructure consists of the following elements :

1. **DHCP servers :** Computers that offer dynamic configuration of IPv4 addresses and related configuration parameters to DHCP clients.
2. **DHCP clients :** Network nodes that support the ability to communicate with a DHCP server to obtain a dynamically leased IPv4 address and related configuration parameters.
3. **DHCP relay agents :** Network nodes, typically routers that listen for broadcast and unicast DHCP message and relay them between DHCP servers and DHCP clients. Without DHCP relay agents, you would have to install a DHCP server on each subnet that contains DHCP clients.

- Each time a DHCP client starts, it requests IPv4 addressing information from a DHCP server, including; IPv4 address, subnet mask, additional configuration parameters, such as a default gateway address, DNS server addresses, a DNS domain name, etc.
- When a DHCP server receives a request, it selects an available IPv4 address from a pool of addresses defined in its database and offers it to the DHCP client. If the client accepts the offer, the IPv4 addressing information is leased to the client for a specified period of time.
- The DHCP client will typically continue to attempt to contact a DHCP server if a response to its request for an IPv4 address configuration is not receive, either because the DHCP server cannot be reached or because no more IPv4 addresses are available in the pool to lease to the client.
- Users no longer need to acquire IPv4 address configurations from a network administrator to properly configure TCP/IP. When a DHCP client is started, it automatically receives an IPv4 address configurtion that is correct for the attached subnet from a DHCP server.
- When the DHCP client moves to another subnet, it automatically obtains a new IPv4 address configuration for that subnet.
- The DHCP server supplies all of the necessary configuration information to all DHCP clients. As long as the DHCP server has been correctly configured, all DHCP clients of the DHCP server are configured correctly.

5.6.3 DHCP Options and Message Type

- DHCP message is either a boot request (1) or a boot reply (2).
- One option, with the value 53 for the tag subfield, is used to define the type of interaction between client and the server.
- Other options define parameters such as lease time and so on.
- Fig. 5.6.2 shows the option format.

Tag (8-bit)	Length (8-bit)	Value (variable length)

Fig. 5.6.2 DHCP message type

- Type field with corresponding DHCP message is given below

Type field (value)	DHCP message type
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNACK
7	DHCPRELEASE

DHCP clients and servers use the following messages to communicate during the DHCP configuration process :

DHCPDISCOVER (sent from client to server)

DHCPOFFER (sent from server to client)

DHCPREQUEST (sent from client to server)

DHCPACK (sent from server to client)

DHCPNACK (sent from server to client)

DHCPDECLINE (sent from server to client)

DHCPRELEASE (sent from client to server)

5.7 Remote Login

- Client-server model can create a mechanism that allows a user to establish a session on the remote machine and then run its applications. This application is known as *remote login*.
- Remote logging allows the user to log on to a remote computer. After logging on, a user can use the services available on the remote computer and transfer the result back to the local computer.
- TELNET and SSH are the two protocols of the remote login.

5.7.1 TELNET

- TELNET (terminal network) is a protocol that provides "a general, bi-directional, eight-bit byte oriented communications facility". It is a program that supports the TELNET protocol over TCP. Many application protocols are built upon the TELNET protocol.
- A client program running on the user's machine communicates using the Telnet protocol with a server program running on the remote machine. The Telnet client program performs two important functions :

1. Interacting with the user terminal on the local host
2. Exchanging messages with the Telnet server.

- The client connects to port 23 on the remote machine, which is the port number reserved for Telnet servers. The TCP connection persists for the duration of the login session. The client and the server maintain the connection, even when the user interrupts the transfer of data, for example by hitting cntl-C.
- Since Telnet is designed to work over two hosts on different platforms, the protocol assumes that the two hosts run a Network Virtual Terminal (NVT). The TCP connection is set up across these two NVT terminals. The NVT is a very simple character device with a keyboard and a printer, data typed by the user on the keyboard is translated by the client software into NVT format and sent via its NVT terminal to the server, and data received in NVT format from the server is translated by the client into the local machine format and output to the printer.
- **NVT uses two types of set in TELNET :**

1. Data character : It has 8 bit in which lowest bit is set as ASCII and highest order bit is 0.
2. Control character : It uses 8 bit character set in which highest order bit is set and lowest order bit is 1.

- TELNET has the following properties :

1. Client programs are built to use the standard client/server interface without knowing the details of server programs.
2. A client and server can negotiate data format options.
3. Once a connection is established through TELNET, both ends of the connection are treated symmetrically.

Different modes of operation in Telnet

1. **Default Mode :** It is half duplex and has become obsolete. Echoing is done by client.

2. **Character Mode :** Server echoes the character back to screen and it can be delayed if transmission time is low. It also creates overhead for network.
3. **Line Mode :** Line Editing, Line Erasing, Character erasing is done by client. It is full duplex mode.

TELNET

- TELNET is a TCP applications. It provides the ability to perform remote logons to remote hosts. TELNET operates using a client and server. Fig. 5.7.1 shows TELNET client server interaction schematic.
- The client TELNET protocol is accessed through the local Operating System (OS) either by user or by a user at a terminal. It provides services to enable a user to log on to the operating system of a remote machine, to initiate the running of a program on that machine. All the commands and data entered at the user terminal are passed by the local operating system to the client TELNET process which then passes them, using the reliable stream service provided by TCP, to the correspondent server TELNET. The two TELNET protocols communicate with each other using commands that are encoded in a standard format known as network virtual terminal. The character set used for commands is ASCII. All input and output data relating to an interaction is transferred as ASCII strings. If this is different from the local character set being used, the corresponding TELNET will carry out any necessary mapping functions. Thus, the two TELNET protocol entities also perform the role of the presentation layer in an OSI stack.
- Following are the Telnet commands.

Name	Code	Meaning
EOF	236	End of file
ABORT	238	Abort process
EOR	239	End of record
NOP	241	No operation
Go Ahead	249	The GA signal
IAC	255	Data byte 255

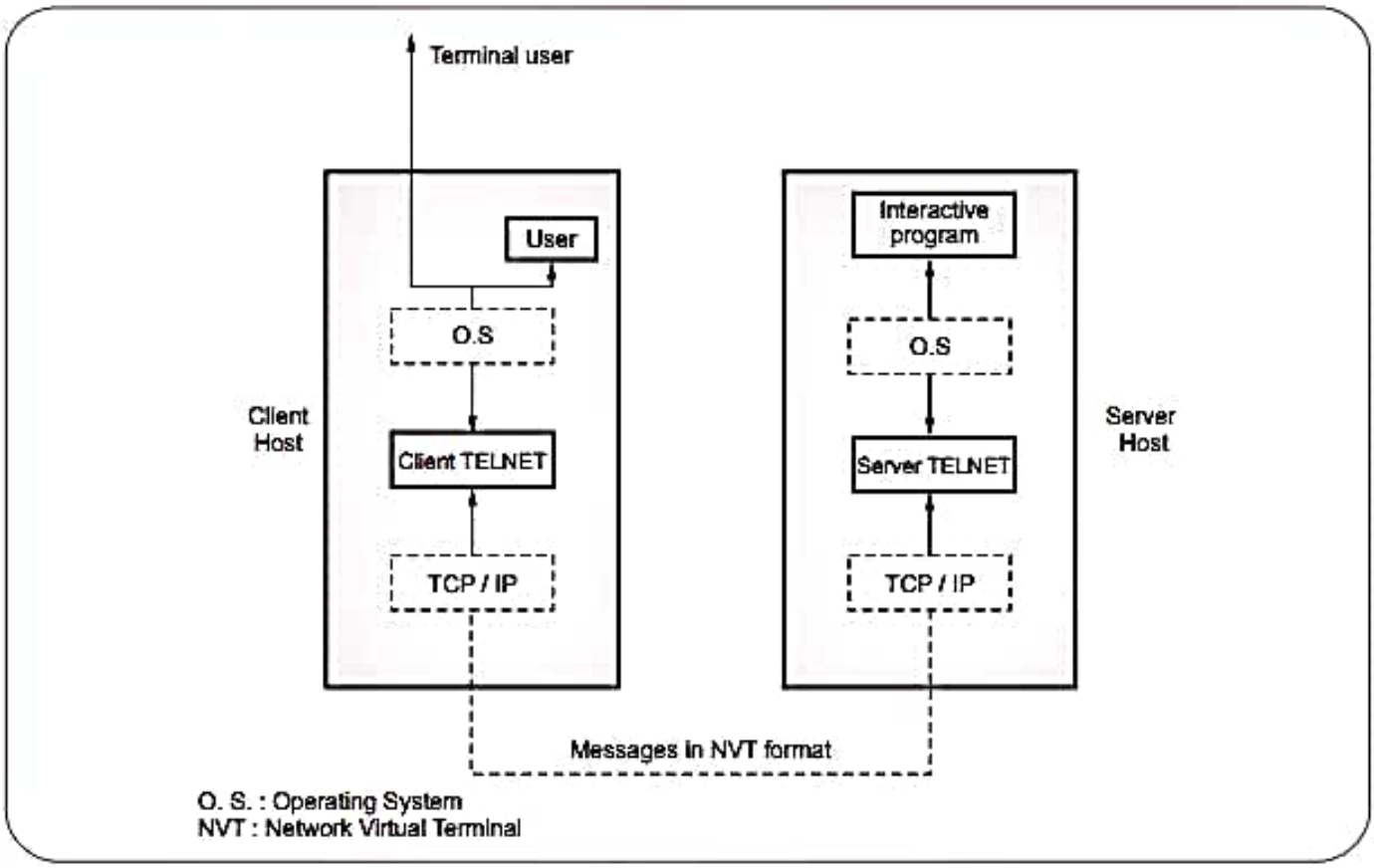


Fig. 5.7.1 TELNET client / server interaction

- Control characters used to control remote server in Telnet are as follows :

1. IP : Interrupt process which is used to interrupt the program.
2. AO : Abort output allows the process to continue without creating output.
3. AYT : Are You there. It determines if the remote server is running after a long silence from server.
4. EC : Erase character. It is used to delete last character.
5. EL : Erase Line. It is used to erase current line in remote host.

5.7.2 Secure Shell Protocol

- Secure Shell (SSH) enhances TELNET in two ways : it provides secure communication, and it provides users with the ability to perform additional independent data transfers over the same connection used for remote login. SSH originated commercially, but it is now a proposed IETF standard.

SSH service is based on

1. A transport layer protocol that provides server authentication, data confidentiality, and data integrity with perfect forward security.
2. A user authentication protocol that authenticates the user to the server.
3. A connection protocol that multiplexes multiple logical communication channels over a single underlying SSH connection.

- SSH does not mandate a specific cryptographic protocol, but uses public key cryptography for authentication and then a choice of several protocols using a session key. SSH uses Port Forwarding. An SSH connection can be used as a secure tunnel, and the user can configure SSH to automatically splice an incoming TCP connection to a new connection across the tunnel.
- SSH is a protocol for secure remote access to a machine over untrusted networks. SSH is a replacement for telnet, rsh, rlogin and can replace ftp. It is not a shell like Unix Bourne shell and C shell.

Reasons to use SSH

1. Designed to be a secure replacement for rsh, rlogin, rcp, rdist, and telnet.
2. Strong authentication.
3. Improved privacy. All communications are automatically and transparently encrypted.
4. Arbitrary TCP/IP ports can be redirected through the encrypted channel in both directions.
5. The software can be installed and used even without root privileges.
6. Optional compression of all data with gzip , which may result in significant speedups on slow connections.

Components of Secure Shell

1. SSHD Server : A program that allows incoming SSH connections to a machine, handling authentication, authorization.
2. Clients : A program that connects to SSH servers and makes requests for service.
3. Session : An ongoing connection between a client and a server. It begins after the client successfully authenticates to a server and ends when the connection terminates.

SSH Architecture

- The user initiates an SSH connection. SSH attempts to connect to port 22 on the remote host. If successful, SSHD on the machine Remote forks off a child SSHD process. This process will handle the SSH connection between the two machines.
- The child SSHD now forks off the command received from the original SSH client. The SSHD child process now encrypts every messages that has to be send to the SSH client. The SSH client decrypts the information and sends it to the user application.
- **For example,** suppose that C1 forms an SSH connection to C2 and specifies that an incoming TCP connection for port 2000 be automatically forwarded across the tunnel to C2, and then spliced to a connection to port 80 on C3. Once the connection has been established and forwarding enabled, whenever a computer at C1's site forms a connection to port 2000 on C1, SSH will

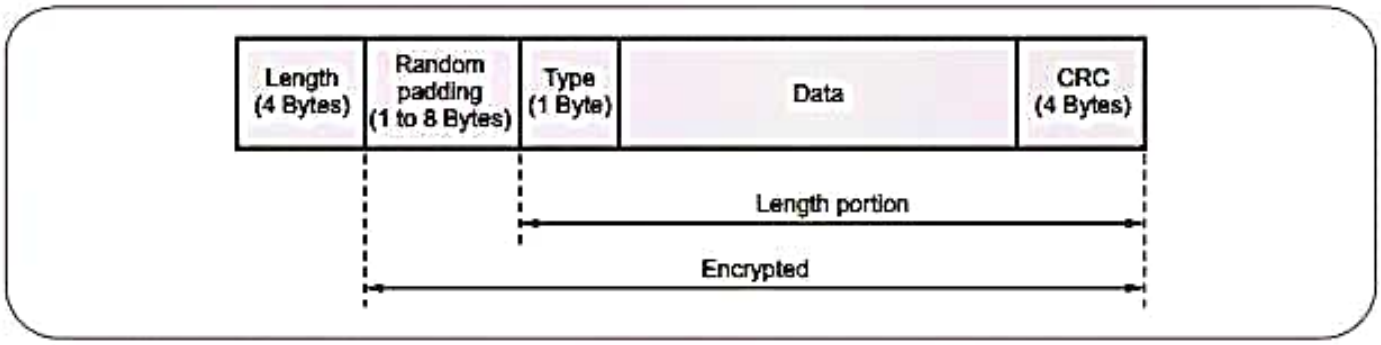


Fig. 5.7.2 SSH packet format

automatically arrange to forward the data to port 80 on C3. Both ends appear to be local : the client at site 1 sees a TCP connection to C1, and the server on C3 sees a TCP connection coming from C2.

- Fig. 5.7.2 shows SSH packet format.

1. **Length :** It indicates the size of the packet, not including the length field or the variable length random padding fields that follows it.
2. **Padding** causes an intrusion to be more difficult.
3. **Type** identifies the type of message.
4. **CRC** is an error detection field.

Working of SSH

- Fig. 5.7.3 shows working of SSH.

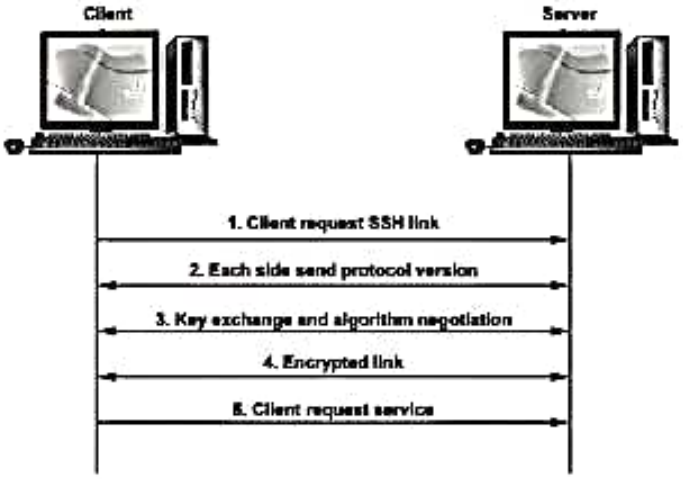


Fig. 5.7.3 SSH protocol working

1. Client contacts server
2. If SSH protocol versions do not agree, no connection
3. Server identifies itself. Server sends host key, server key, check bytes, list of methods. Client looks in its DB for hosts.
4. Client sends a secret key, encrypted using server's public key.
5. Both begin encryption. Server authentication is completed.
6. Client authentication on the server side. Example, password and public-key authentication.

- **Advantages of SSH over TELNET :**

1. SSH provides a secure communication by encrypting and authenticating messages.
2. SSH provides several additional data transfers over the same connection by multiplexing multiple channels that are used for remote login.

Comparison between SSH-1 vs. SSH-2

Sr. No.	SSH-1	SSH-2
1.	All in one protocol	Separate protocols
2.	CRC-32 integrity check	Strong integrity check
3.	One session per connection	Multiple sessions per connection
4.	No password change	Password change
5.	No public-key certificate authentication	Provide public-key certificate authentication

5.8 Two Marks Questions with Answers

Q.1 *Define WWW ?*

Ans. : World Wide Web (WWW) is an internet application that allows users to view web pages and move from one web page to another.

Q.2 *What are the four groups of HTTP Headers ?*

Ans. : The four groups of HTTP headers are: General Headers, Entity Headers, Request Headers, and Response Headers.

Q.3 *What are the four main properties of HTTP ?*

Ans. : The four main properties of HTTP are :

1. Global Uniform Resource Identifier.
2. Request-response exchange.
3. Statelessness.
4. Resource metadata.

Q.4 *Mention the types of HTTP messages.*

Ans. : Types of HTTP messages : Request and Response

Q.5 *What are the transmission modes of FTP ?*

Ans. : Transmission modes of FTP are :

1. **Stream mode :** Default mode and data is delivered from FTP to TCP as a continuous stream of data.
2. **Block mode :** Data is delivered from FTP to TCP in terms of blocks. Each data block follows the three byte header.
3. **Compressed mode :** File is compressed before transmitting if size is big. Run length encoding method is used for compression.

Q.6 *Mention the application of FTP.*

Ans. :

1. Used for remote login and data transfer.
2. FTP provides good security.
3. It is often used to upload web pages and other documents from a private development machine to a public web-hosting server.

Q.7 *What are the basic functions of e-mail ?*

Ans. : Basic functions of e-mail are : Composition, Transfer, Reporting, Displaying, Disposition.

Q.8 *Why email security is necessary ?*

Ans. : Email security is the process of using email encryption to send messages that can only be opened by the intended recipient. Sending a message without secure email encryption is similar to dropping a post card in the mail - it can be read by almost anyone handling the postcard during its journey from sender to receiver. Secure email encryption protects both your online data and customers' sensitive information.

Q.9 *When web pages are sent out, they are prefixed by MIME headers. Why ?*

Ans. : The MIME headers tell the browser what type of file is contained on the Web page and also what type of helper application or plug-in needs to be used to display the content.

Q.10 *State the difference between SMTP and MIME.*

Ans. :

Sr. No	SMTP	MIME
1.	SMTP is protocol used to exchange messages between mail servers.	MIME expands the messaging abilities of SMTP and supports all formats.
2.	SMTP is the most widely used internet application.	MIME allows multimedia and other non-textual formats to be handled reliably throughout the message transport process.

Q.11 *What is DNS ?*

Ans. : DNS is a client/server application that identifies each host on the Internet with a unique user friendly name.

Q.12 *What is the Domain Name System responsible for ?*

Ans. : The Domain Name System converts domain names (of the form "www.vtubooks.com") into IP numbers.

Q.13 *Why do we need a Domain Name System ?*

Ans : IP numbers uniquely identify hosts on the Internet; however they are difficult to remember. We therefore need a more memorable way of identifying hosts. Furthermore, since multiple domains may be hosted by a single computer we need a way of mapping multiple domains to a

single host. Finally, since domains may be hosted on a number of different machines over a period of time we need a method for

changing the IP number representing a host without having to change the information people use to access that host (that is the domain name remains constant but the IP number may change).

Q.14 *List the two types of DNS message.*

Ans. : DNS messages are : Query and Response. The query message consists of the header and the question records. The response message consists of a header, question record, answer record, authoritative record and additional record.

Q.15 *What do you mean by TELNET ?*

Ans. : TELNET is a client/server application that allows a user to log on to a remote machine giving the user access to the remote system.

TELNET is used to connect remote computers and issue commands on those computers.

❑❑❑

SOLVED SAMPLE TEST PAPER - 1

Advanced Computer Network

T.Y. Diploma, Sem - V [Computer Engg./IT] [CO/CM/IF/CW]

Time : 1 Hour] **[Marks : 20**

Instructions :

1) *All questions are compulsory.*
2) *Illustrate your answers with neat sketches wherever necessary.*
3) *Figures to the right indicate full marks.*
4) *Assume suitable data, if necessary.*
5) *Preferably, write the answers in sequential order.*

Q.1 Attempt any FOUR **(8)**

a) *What is subnet masking ?* **(Refer Two Marks Q.15 of Chapter-1)**

b) *What is the main reason for IPv6 being developed ?* **(Refer Two Marks Q.1 of Chapter-2)**

c) *What are the benefits of Open Shortest Path First (OSPF) protocol ?* **(Refer Two Marks Q.8 of Chapter-3)**

d) *What is multicast routing ?* **(Refer Two Marks Q.1 of Chapter-3)**

e) *Why is IPv4 to IPv6 transition is required ?* **(Refer Two Marks Q.5 of Chapter-2)**

f) *What is network address ?* **(Refer Two Marks Q.2 of Chapter-1)**

Q.2 Attempt any THREE **(12)**

a) *What is fragmentation ? Explain.* **(Refer section 1.2.1)**

b) *Draw and explain header format of IPv4.* **(Refer section 1.2)**

c) *Explain difference between distance vector and link state routing.* **(Refer section 3.2.3)**

d) *Describe classful addressing.* **(Refer section 1.1.2)**

e) *Explain autoconfiguration and renumbering of IPv6.* **(Refer section 2.1.2)**

f) *Explain path vector routing.* **(Refer section 3.2.5)**

SOLVED SAMPLE TEST PAPER - 2

Advanced Computer Network

T.Y. Diploma, Sem - V [Computer Engg./IT] [CO/CM/IF/CW]

Time : 1 Hour] **[Maximum Marks : 20**

Instructions :

1) *All questions are compulsory.*
2) *Illustrate your answers with neat sketches wherever necessary.*
3) *Figures to the right indicate full marks.*
4) *Assume suitable data, if necessary.*
5) *Preferably, write the answers in sequential order.*

Q.1 Attempt any FOUR. **(8)**

a) *What is the purpose of TCP push operation ?* **(Refer Two Marks Q.5 of Chapter-4)**

b) *What factors govern the rate at which TCP sends segments ?* **(Refer Two Marks Q.7 of Chapter-4)**

c) *What is Port ?* **(Refer Two Marks Q.9 of Chapter-4)**

d) *State four properties of HTTP.* **(Refer Two Marks Q.3 of Chapter-5)**

e) *What are transmission modes of FTP ?* **(Refer Two Marks Q.5 of Chapter-5)**

f) *What is TELNET ?* **(Refer Two Marks Q.15 of Chapter-5)**

Q.2 Attempt any THREE. **(12)**

a) *Explain TCP congestion control.* **(Refer section 4.2.11)**

b) *Explain SCTP packet format.* **(Refer section 4.3.5)**

c) *Explain TCP connection establishment.* **(Refer section 4.2.5)**

d) *Explain working of FTP.* **(Refer section 5.3)**

e) *Explain components of DNS.* **(Refer section 5.5.1)**

f) *Explain Secure Shell Protocol.* **(Refer section 5.7.2)**

❑❑❑

SOLVED SAMPLE QUESTION PAPER

Advanced Computer Network

T.Y. Diploma, Sem - V [Computer Engg./IT] [CO/CM/IF/CW]

Time : 3 Hours] **[Marks : 70**

Instructions : *1) All questions are compulsory.*

2) Illustrate your answers with neat sketches wherever necessary.

3) Figures to the right indicate full marks.

4) Assume suitable data, if necessary.

5) Preferably, write the answers in sequential order.

Q.1 **Attempt any FIVE of the following** **(10)**

a) What is anycast ? **(Refer Two Marks Q.4 of Chapter 2)**

b) State the IP address classes. **(Refer Two Marks Q.16 of Chapter 1)**

c) Write abbreviation/acronym of following : **(Refer Two Marks Q.1 of Chapter 4)**

i) UDP *ii) TCP* *iii) TFTP*

iv) RTT *v) SCTP*

d) What is TCP ? **(Refer Two Marks Q.4 of Chapter 4)**

e) Define BGP. **(Refer Two Marks Q.6 of Chapter 3)**

f) Define WWW. **(Refer Two Marks Q.1 of Chapter 5)**

g) State main applications of FTP. **(Refer Two Marks Q.6 of Chapter 5)**

Q.2 **Attempt any THREE of the following** **(12)**

a) Explain network address translation. **(Refer section 1.1.5)**

b) What is mobile IP ? List and explain components of mobile IP. **(Refer section 1.1.5)**

c) Explain advantages and disadvantages of VPN. **(Refer section 1.5)**

d) Describe classful addressing. **(Refer section 1.1.2)**

Q.3 **Attempt any THREE of the following** **(12)**

a) Explain difference between static and dynamic routing. **(Refer section 3.1.4)**

b) What is OSPF ? Explain features of OSPF. **(Refer section 3.3.2)**

c) What is count-to-infinity problem ? Explain. **(Refer section 3.2.1.1)**

d) What is PIM ? Explain PIM-DM mode and PIM-SM mode. **(Refer section 3.5.3)**

Q.4 **Attempt any THREE of the following** **(12)**

a) Explain the various fields in the frame format of UDP with a neat diagram. **(Refer section 4.1.1)**

b) Explain UDP services. **(Refer section 4.1.2)**

c) Compare TCP and UDP. **(Refer section 4.2.13)**

d) Explain components of DNS. **(Refer section 5.5)**

e) Explain DHCP frame format. **(Refer section 5.6.1)**

Q.5 Attempt any TWO of the following **(12)**

a) Explain address space allocation of IPv6. **(Refer section 2.1.1)**

b) Draw and explain IPv6 header format. **(Refer section 2.3)**

c) Explain different transition method of IPv4 to IPv6. **(Refer section 2.2)**

Q.6 Attempt any TWO of the following **(12)**

a) Explain ports of UDP. **(Refer section 4.1.3)**

b) Draw the frame format of TCP header and state the function of various field. **(Refer section 4.2.3)**

c) Explain SCTP. **(Refer section 4.3)**

d) Explain working of WWW. **(Refer section 5.1)**

❑❑❑

Books available @

MUMBAI

Student Agencies Pvt. Ltd.
Ph. - 022 - 40496161 / 31

Vidyarthi Sales Agencies
Ph. - 022 - 23829330
022 - 23851416 / 23867279

Bharat Sales
Ph. - 022 - 23821307 / 7580

AHMEDNAGAR

Shripad Granth Bhandar
Ph. - 9922664979

SANGAMNER

Amrut Book Stall
Ph. - 9850663354

NARAYANGAON

Sunil General Stores
Ph. - 9850725770

KOPARGAON

Mauli Books & General Store
Ph. - 9890451467

Kohinoor Book Stall
Ph. - 9371719996

KARAD

Archana Bazar
Ph. - 7588065287

NASHIK

Rahul Book Centre
Ph. - 0253 - 27424287

Maharashtra Pustak Bhandar
Ph. - 0253 - 2317506

New India Book House
Ph. - 9623123458

Anmol Pustakalaya
Ph. - 9822306289

Anmol Books
Ph. - 0253 - 2505501

Om Pustakalaya
Ph. - 9422246809

Pragati Books & Stationers
Ph. - 7721014040

New Om Stationers
& General Stores
Ph. - 0253 - 2378874

Shri Ganesh Book Depot
Ph. - 9890335806

Eakveera Books
Ph. - 9422754746

Yuvraj Books & Stationers
Ph. - 9850725770

New Anand Pustakalaya
Ph. - 9881540440 / 7720054040

JALGAON

Parvati Traders
Ph. - 9422277738