CMR
INSTITUTE OF
TECHNOLOGY

USN | | | | | | | | | | |

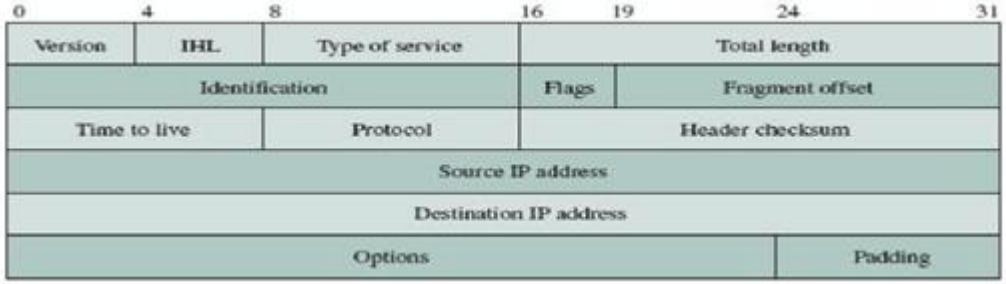
Internal Assesment Test - II

Sub:	**Computer Networks - 2**							Code:	**10CS64**
Date:	09/ 05 / 2017	Duration:	90 mins	Max Marks:	50	Sem:	**VI A & B**	Branch:	**ISE**

1. a) Explain the format of IPv4 basic header format. [6] CO3 L2

Internet Protocol

- It provides best effort, connectionless packet delivery, packets may be lost, out of order, or even duplicated, so it is the responsibility of higher layer protocols to deal with these, if necessary.
- The header is of fixed-length component of 20 bytes plus variable-length consisting of options that can be up to 40 bytes.



Version: This field identifies the current IP version and it is 4.
Internet header length (IHL): It specifies the length of the header in 32-bit words. If no options are used, IHL will have value of 5.
Type of service (TOS): This field specifies the priority of packet based on delay, throughput, reliability and cost. Three bits are used to assign priority levels and four bits are used for specific requirement (i.e. delay, throughput, reliability and cost).

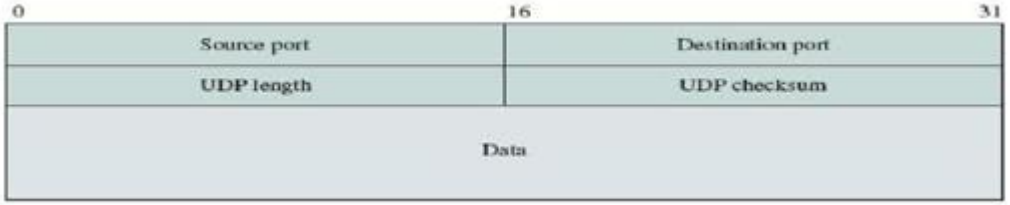
Total length: The total length specifies the number of bytes of the IP packet including header and data, maximum length is 65535 bytes.
Identification, Flags, and Fragment Offset: These fields are used for fragmentation and reassembly.
Time to live (TTL): It specifies the number of hops; the packet is allowed to traverse in the network. Each router along the path to the destination decrements this value by one. If the value reaches zero before the packet reaches the destination, the router discards the packet and sends an error message back to the source.
Protocol: specifies upper-layer protocol that is to receive IP data at the destination.
Examples include TCP (protocol = 6), UDP (protocol = 17), and ICMP (protocol = 1).
Header checksum: verifies the integrity of the IP header of the IP packet.

- IP header uses check bits to detect errors in the **header**
- A checksum is calculated for header contents
- Checksum recalculated at every router, so algorithm selected for ease of implementation in software
- **Source IP address** and **destination IP address:** contain the addresses of the source and destination hosts.
- **Options:** Variable length field allows packet to request special features such as security level, route to be taken by the packet, and timestamp at each router. Detailed descriptions of these options can be found in [RFC 791].
- **Padding:** This field is used to make the header a multiple of 32-bit words.

b) With a neat diagram explain UDP datagram. [4] CO3 L2

UDP is a transport protocol

- UDP provides communication between processes
- UDP uses IP to deliver datagrams to the right host
- Connectionless
- No session is established.



Does not provide guaranteed delivery

- No sequence numbers
- No acknowledgements
- No flow control
- No error control
- Reliability is the responsibility of the application. Uses Port numbers as endpoints to communicate

a) Explain IP address classification & Subnet addressing [6] CO4 L2

Each host on Internet has unique 32 bit IP address
Each address has two parts: netid and hostid
netid unique & administered by

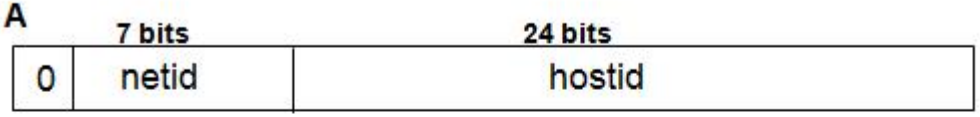
American Registry for Internet Numbers (ARIN)
Reseaux IP Europeens (RIPE)
Asia Pacific Network Information Centre (APNIC)

Facilitates routing
A separate address is required for each physical connection of a host to a network; "multi-homed" hosts
Dotted-Decimal Notation:

int1.int2.int3.int4 where intj = integer value of jth octet
IP address of 10000000 10000111 01000100 00000101
is 128.135.68.5 in dotted-decimal notation

Classful Addresses

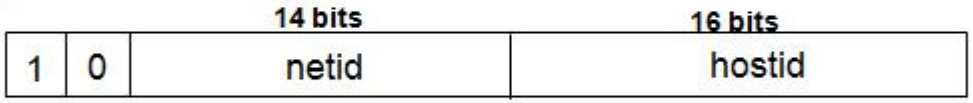
Class A



- 126 networks with up to 16 million hosts

1.0.0.0 to 127.255.255.255

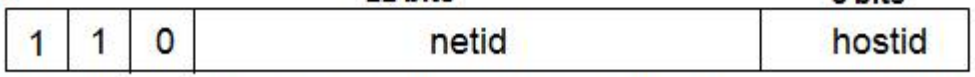
Class B



- 16,382 networks with up to 64,000 hosts

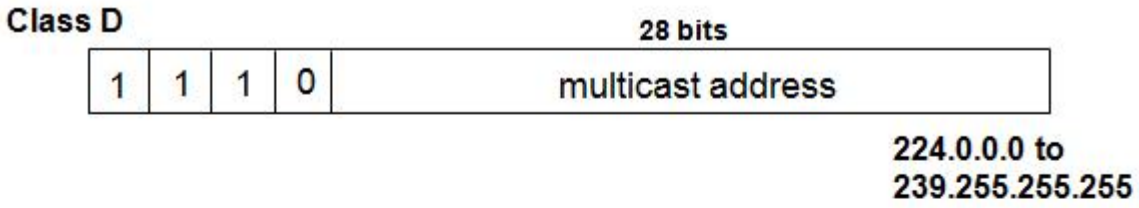
128.0.0.0 to 191.255.255.255

Class C



- 2 million networks with up to 254 hosts

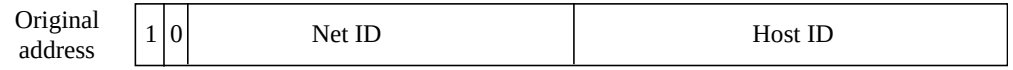
192.0.0.0 to 223.255.255.255



- Up to 250 million multicast groups at the same time
- Permanent group addresses
  - All systems in LAN; All routers in LAN;
  - All OSPF routers on LAN; All designated OSPF routers on a LAN, etc.
- Temporary groups addresses created as needed
- Special multicast routers

Subnetting:

- Subnet addressing introduces another hierarchical level
- Transparent to remote networks
- Simplifies management of multiplicity of LANs
- Masking used to find subnet number



- Organization has Class B address (16 host ID bits) with network ID: 150.100.0.0
- Create subnets with up to 100 hosts each
  - 7 bits sufficient for each subnet
  - 16-7=9 bits for subnet ID
- Apply subnet mask to IP addresses to find corresponding subnet
  - Example: Find subnet for 150.100.12.176
  - IP add = 10010110 01100100 00001100 10110000
  - Mask = 11111111 11111111 11111111 10000000
  - AND = 10010110 01100100 00001100 10000000
  - Subnet = 150.100.12.128

Subnet address used by routers within organization

b) A host in an organization has an IP address 150.32.64.34 and subnet mask 255.255.240.0. What is the address of the subnet? What is the range of IP address that a host can have on this subnet. **[4] CO4 L3**

A host in an organization has an Ip address 150.32.64.34 and a subnet mask 255.255.240.0. What is the address of this subnet? What is the range of Ip address that a host can have on this subnet?

Soln,

Ip Address : 150.32.64.34

⇓

10010110 00100000 01000000 00100010

Subnet Mask : 255.255.240.0

⇓

11111111 11111111 11110000 00000000

To find subnet : Do AND operation for Ip Address & subnet mask.

So, 10010110 00100000 01000000 00100010
11111111 11111111 11110000 00000000

10010110 00100000 01000000 00000000

∴ Range of Ip address starts from,

→ From : 10010110 00100000 01000000 00000001

To : 10010110 00100000 0100 1111 11111110

3. What are the elements of network security? Explain the threats to network security. [10] CO5 L2

ThreatstoNetworkSecurity

Internet infrastructure attacksare broadly classifiedinto four categories,as follows:

DNS hacking attacks Routingtable poisoningattacks

Packetmistreatmentattacks Denialof serviceattacks

Among these threats,the first threeattacks arerelated to networkinfrastructure; denial-of-service attacksare related to endsystems.

DNSHackingAttacks

In the normal modeof operation,hosts send UDP queriesto the DNS server.

DNS servers reply with aproper answer, or direct thequeries to smarter servers.

ADNShackingattackmayresultinthelackofdataauthenticityandintegrityandcanappearinanyofthefollowingforms:

An information-levelattack forces aserver to respondwith something other thanthe correct answer.With cache poisoning, a hacker tricksa remote nameserver into cachingthe answer for a third-partydomain by providingmalicious information for the domain's authorizedservers. Hackers canthen redirect traffic to apreselected site.

DNSHackingAttacks

In a masqueradingattack, the adversary posesas atrusted entity to obtainsecret information. Inthis guise,theattacker can stopany message frombeing transmitted further or canchange the contentor redirectthe packet to bogus servers. Thisaction is alsoknown asaman-in-the-middleattack.

The attacker normally sendsqueries to eachhost and receives in replythe DNShost name. In aninformationleakageattack, the attacker sendsqueries to allhostsand identifieswhich IP addresses arenot used.Later on, the intruder can usethoseIP addressesto make other types of attacks.

DNSHackingAttacks

Once a domain nameis selected, ithas tobe registered. Various tools areavailableto registerdomain names over the Internet.

Ifthe tools are notsmart enough,aninvader mightobtain secure information anduse it tohighjack thedomain later. In thedomainhighjackingattack, whenever auser enters a domain address, heor she isforced toenter theattacker's Web site. Thiscan be veryirritating andcan cause agreat loss of Internet usageability

RoutingTablePoisoningAttacks

A routing table poisoning attack isthe undesired modification of routing tables.Anattacker cando this bymaliciously modifying the routinginformation update packetssent by routers.

This is a challengingand important problem,as arouting table is thebasis of routinginthe Internet.

Any false entry ina routing tablecould leadto significant consequences, suchas congestion, an overwhelmedhost, looping, illegal accessto data, andnetwork partition.

Two typesof routing table poisoningattacksare:

1.linkattack

2.routerattack.

RoutingTablePoisoningAttacks

LinkAttack

A link attackoccurs when ahacker gets accessto a linkand thereby intercepts, interrupts,or modifiesrouting messages on packets.

Link attacks act similarly onboth the link-stateand thedistance-vector protocols. Ifan attacker succeedsin placing anattackin a link-state routing protocol,a router maysend incorrect updates about its neighborsorremain silenteven if the link stateof its neighbor has changed.

The attack througha link canbeso severe that the attacker can program a routerto either droppackets from avictim or readdress packets to a victim, resulting in alower throughputof the network.

Sometimes, a routercan stop anintended packet frombeing forwarded further. However,since more thanone path toany destination exists, thepacket ultimately reachesits destination.

RoutingTablePoisoningAttacks

RouterAttacks

Router attacks may affectthe link-state protocolor even the distance-vector protocol.

If link-stateprotocol routers are attacked,they become malicious. Theymay add a non-existing linkto a routing table, delete anexisting link, oreven changethe cost ofa link.

This attack may causea router tosimply ignorethe updates sent byits neighbors, leadingto aserious impact on the operabilityof the networktraffic flow.

In the distance-vector protocol, an attackermay cause routers to sendwrong updatesabout anynode in the network, thereby misleadinga router andresulting in network problems.

RoutingTablePoisoningAttacks

Most unprotected routers have no wayto validate updates. Therefore, both link-stateand distance-vectorrouter attacks are veryeffective.

In the distance-vector protocol,for example,a malicious router can sendwrong information inthe formof a distance vector to allits neighbors.

A neighbor may notbe able todetect thiskind of attackand thus proceeds toupdate itsrouting table, based on wrong distance vectors.

The error can in turn bepropagated to agreat portionof the network beforebeing detected.

Packet-MistreatmentAttacks

A packet-mistreatment attack can occur duringany data transmission. A hackermaycapture certaindata packets and mistreat them.This type ofattack isvery difficult to detect.

The attack mayresult in congestion, lower throughput,and denial-of-service attacks.

Similartorouting tablepoisoning attacks, packet-mistreatment attacks canalso besub classifiedinto link attacks and routerattacks.

The link attack causes interruption, modification,or replication ofdata packets.

Arouter attack canmisroute allpackets, which mayresult in congestion ordenialof service

Packet-MistreatmentAttacks

Someexamplesofapacket-mistreatmentattack:

Interruption. If anattacker intercepts packets,they maynot be allowed tobepropagated totheir destinations, resulting in a lowerthroughput of thenetwork. Thiskind ofattack cannot be detected easily, as evenin normaloperations, routers can dropsomepackets forvarious reasons.

Modification. Attackers may succeed inaccessing the content of apacket while intransit andchange its content. They can thenchange the addressof thepacket or even change its data.

Packet-MistreatmentAttacks

Replication. An attacker mighttrap a packetand replayit. This kind ofattack canbe detectedby using the sequence number for eachpacket.

Pingofdeath. An attacker maysend aping message, which is largeand therefore mustbe fragmentedfor transport. The receiverthen starts toreassemble the fragments as theping fragmentsarrive. The totalpacket length becomes toolarge and mightcause asystem crash.

Maliciousmisroutingofpackets. A hacker may attacka router and changeitsrouting table, resulting inmisrouting of data packets,causing a denialof service.

Denial-of-ServiceAttacks

A denial-of-service attackis a type ofsecurity breach that prohibits a userfrom accessingnormallyprovidedservices:

The denial of servicedoes not resultin informationtheft or any kind of information loss butcan nonethelessbe very dangerous, as itcan cost thetarget persona largeamount of time andmoney. Denial-of-service attacksaffect the destination rather thanadatapacket or router.

denial-of-service attack affects aspecific network service, such as e-mail or DNS. For example, suchan attackmay overwhelm the DNSserver in variousways andmakeit inoperable.

Denial-of-ServiceAttacks

One way of initiatingDenial-of-serviceattack isby causing buffer overflow. Insertingan executablecode inside memory can potentiallycause a bufferoverflow.

Denial-of-serviceattacks are easy togenerate but maybe difficult to detect.Theytake importantservers out of action for few hours,thereby denying serviceto allusers.

Severalother situationscan also causethis kind ofattack, such as UDPflood, TCP flood,and ICMPflood. Inall these attacks, the hacker’smain aim isto overwhelmvictims and disrupt services providedto them.

Denial-of-ServiceAttacks

Denial-of-serviceattacksareoftwotypes:

1.Single-source. An attacker sends alarge numberof packets to atarget systemto overwhelmand disable it. These packets aredesigned such thattheir realsources cannot be identified.

2.Distributed. In thistype of attack,a largenumber of hosts are used tofloodunwanted trafficto a single target. The target cannot thenbe accessible toother usersinthe network, as it is processingthe floodof traffic.

4.Explain the following: **[10] CO5 L2**

a) DNS message format with a neat diagram

DNS has two types of messages: query and response. Both types have the same format. The query message consists of a header and the question records; the response message consisits of a header, question records, answer records, authoritative records, and additional records.

Header

Both query and response messages have the same header format with some fields set to zero for the query messages. the header is 12 byte and its format is as follows:

Identification	**flags**
Number of question records	Number of answer records(All os in query message
Number of authoritative records(All os in query message)	Number of additional records(All os in query message)

The header fields are as follows:

- **Identification.** 16 bit field used by the client to match the response with the query. The client uses ientification number each time it sends a query. the server duplicates this number in response.
- **Flags.** 16 bit field consisting of other subfields as shown below.
  1. QR (query/response). If set (1) means message is a response , if 0 it means message type is query.
  2. OpCode. 4-bit defines type of query or response (0-standard, 1-inverse, 2-server status required).
  3. AA (authoritative answer). (1-bit and used inly in response message. Set (1)-means Authoritative server).
  4. TC (truncated) . if set means value of 1, means messgae was more than 512 bytes and is truncated.
  5. RD (recursion desired). A 1-bit field, when set means client desires reursive answer. It is repeated in both request and response.
  6. RA (recursion available). 1-bit, and it is set only in response message to indiacate that recursion is available.
  7. Reserved. A 3-bit subfield set to 000.

8. rCode. A 4-bit field which shows the status of error in the response. Of course, only an authoritative server can make such judgement.

Values of rCode:

1. 0 - No error
2. 1 - Format error.
3. 2 - Problem at name server.
4. 3 - Domain reference problem.
5. 4 - Quert type not supported.
6. 5 - Administratively prohibited.
7. 6-15 - Reserved

- Number of Question Records. This is a16-bit field consisting of number of queries in question section of message.
- Number of Answer Records. This is a 16-bit field containing the number of answer records in the answer section of response message. Its value is 0in the query message.
- Number of authoritative records. A sixteen bit field which tells the number of authoritative records in the authoritative section of the response message. Its value is zero in the query message.
- Number of additional records. This is a 16 bit fieldcontaining the number of additional recordsin the additional section of the response message.

Question Section

This is a section consisting of one or more question records. It is present on both query and response messsages

Answer Section

This is section consisting of one or more resource records. It is present only in response messages. This section includes answer from the server to the client (resolver).

Authoritative Section

This section is also contained only in response messages of DNS, and gives information about domain names regarding authoritative servers for the query.

Additional Information Section

This section provides additional information to help the resolver and present only in response part of DNS message format.

This was discussion about the format of DNS message. We discussed about various sections of Domain Name System message format like header, question section, answer

section, authoritative section, and Additional information section of Domain Name System (DNS) messages.

b) Remote login protocols

- TELNET Protocol TELNET (terminal network) is a TCP/IP standard for establishing a connection to a remote system. TELNET allows a user to log in to a remote machine across the Internet by first making a TCP connection and then pass the detail of the application from the user to the remote machine..
- Logging to Remote Servers With TELNET, an application program on the user's machine becomes the client. The user's keyboard and its monitor also attach directly to the remote server. The remotelogging operation is based on timesharing, whereby an authorized user has a login name and a password. TELNET has the following properties. •
- Client programs are built to use the standard client/server interfaces without knowing the details of server programs.
- A client and a server can negotiate data format options. • Once a connection is established through TELNET, both ends of the connection are treated symmetrically. When a user logs in to a remote server, the client's terminal driver accepts the keystrokes and interprets them as characters by its operating system. Characters are typically transformed to a universal character set called network virtual terminal (NVT), which uses 7-bit USASCII representation for data. The client then establishes a TCP connection to the server.
- Texts in the NVT format are transmitted using a TCP session and are delivered to the operating system of the remote server. The server converts the characters back from NVT to the local client machine's format. Secure Shell (SSH) Protocol Secure Shell (SSH), another remote login protocol, is based on UNIX programs. SSH uses TCP for communications but is more powerful and flexible than TELNET and allows the user to more easily execute a single command on a remote client.
- SSH has the following advantages over TELNET. • SSH provides a secure communication by encrypting and authenticating messages. SSH provides several additional data transfers over the same connection by multiplexing multiple channels that are used for remote login.
- SSH security is implemented by using public-key encryption between the client and remote servers. When a user establishes a connection to a remote server, the data being transmitted remains confidential even if an intruder obtains a copy of the packets sent over an SSH connection.

- SSH also implements an authentication process on messages so that a server can find out and verify the host attempting to form a connection. Normally, SSH requires users to enter a private password. The advantage of port forwarding is that application data can be passed between two sites the client and the second server without requiring a second client and server the first server as a client and the second server.

5a) Define the network management. Explain the SNMP with SNMP messages. [5]
CO5 L2

SNMP Message Types

There are five types of messages exchanged in SNMP. They are referred to by Protocol Data Unit (PDU) type.

PDU Type	Name	Description
0	get-request	Get one or more variables .(manager to element)
1	get-next-request	Get next variable after one or more specified variables. (manager to element)
2	set-request	Set one or more variables. (manager to element)
3	get-response	Return value of one or More variables. (element to manager)
4	trap	Notify manager of an event. (element to manager)

b) Explain the Diffie-Hillman exchange for key generation. [5]
CO5 L2

Diffie-HellmanKey-ExchangeProtocol

In theDiffie-Hellmankey-exchangeprotocol, two end users can agree ona shared secretcodewithoutany information shared in advance.Thus, intruders wouldnot beable to access the transmittedcommunication between the two users or discoverthe shared secretcode.

This protocolis normally used for virtualprivate networks (VPNs)

The essenceof this protocol fortwo users,1 and 2,is as follows. Suppose thatuser 1 selectsa primea, a random integer numberx1, and a generatorgand createsy1 {1,2,…..,a-1}such that,

In practice, the twoend users agreeonaandgahead of time. User 2performs the samefunctionand createsy2:

User 1 then sendsy1to user 2. Now,user 1forms itskey, k1, using the information itspartner sent as

User 2 forms itskey,k2, using the information itspartner sent as

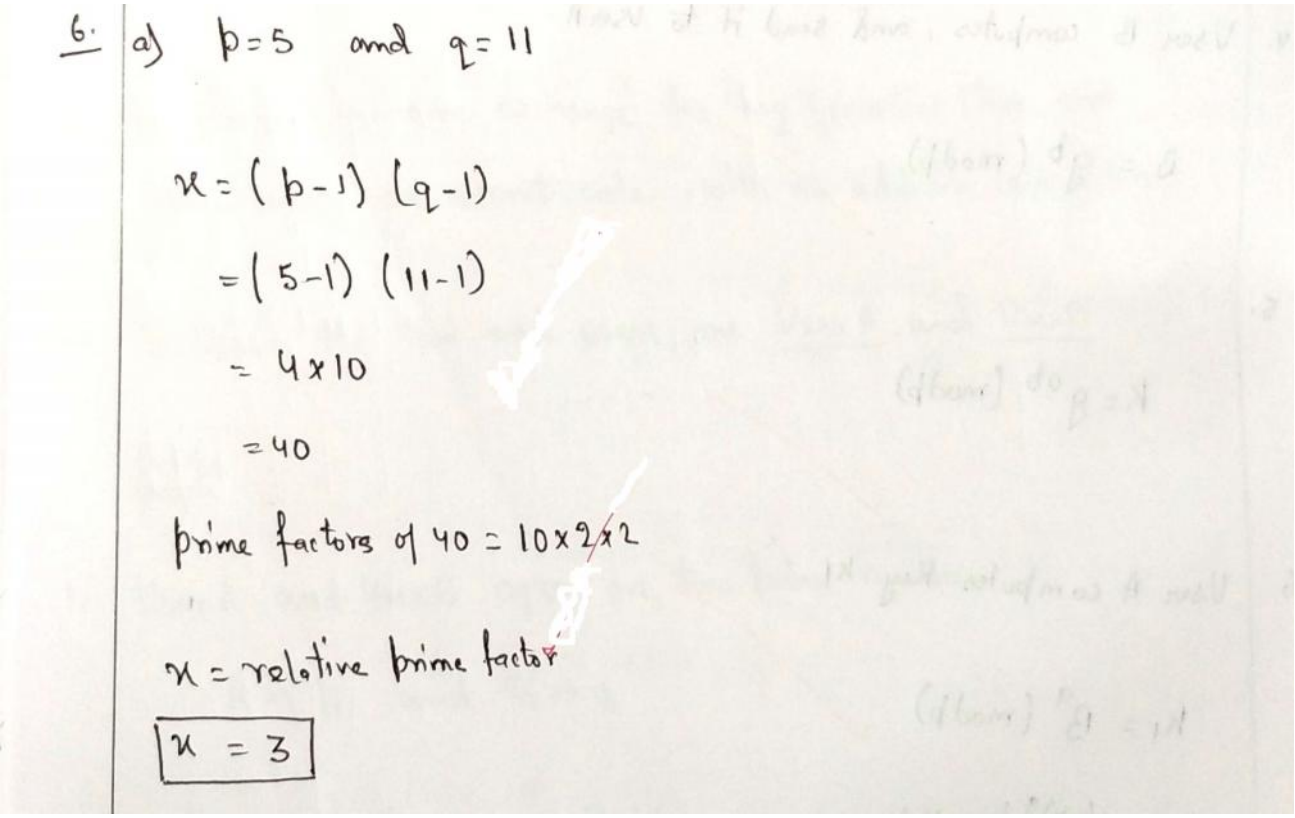
It can easily beproved that thetwo keysk1andk2are equal. Therefore, the twousers can nowencrypt their messages, each using itsown key createdby theother one's information.

6 Apply RSA and do the following: [10] CO5 L3

a) Suppose p=5 and q=11. Find e and d.

b) Encrypt the following and to get the cipher texts p1=18, p2=19 and p3=1

c) Decrypt the cipher texts obtained above



6. a) $p=5$ and $q=11$

$x = (p-1)(q-1)$

$= (5-1)(11-1)$

$= 4 \times 10$

$= 40$

prime factors of $40 = 10 \times 2 \times 2$

x = relative prime factor

$x = 3$

for y:

$1 = x * y \bmod (p-1)(q-1)$

$1 = 3 * y \bmod 40$

$\therefore \boxed{y = 27}$

b) $p1 = 18$, $p2 = 19$, $p3 = 1$

to encrypt the cipher text, we have

$$c = m^x \bmod n$$

where,

$n = p * q = 5 \times 11 = 55$

for $p1 = 18$

$c_1 = 18^x \bmod 55$

$= 18^3 \bmod 55$

$= 18^3 \,\%\, 55$

$= 5832 \,\%\, 55$

$= 2$

for $p2 = 19$

$c_2 = 19^x \bmod 55$

$= 19^3 \bmod 55$

$= 19^3 \,\%\, 55$

$= 6859 \,\%\, 55$

$= 39$

for $p3 = 1$

$c_3 = 1^3 \bmod 55$

$= 1 \,\%\, 55$

$= 1$

c) decrypt of cipher texts can be obtained from

$$m = c^d \bmod n$$

⇒ for $c_1 = 3$

$m_1 = 2^{27} \bmod 55$

$= 2^{27} \,\%\, 55$

$= 134217728 \,\%\, 55 = \underline{\underline{18}}$

⇒ for $c_2 = 2$

$m_2 = 39^{27} \bmod 55$

$= 39^{27} \,\%\, 55$

$= 9.093 \times 10^{42} \,\%\, 55 = \underline{\underline{19}}$

⇒ for $c_3 = 1$

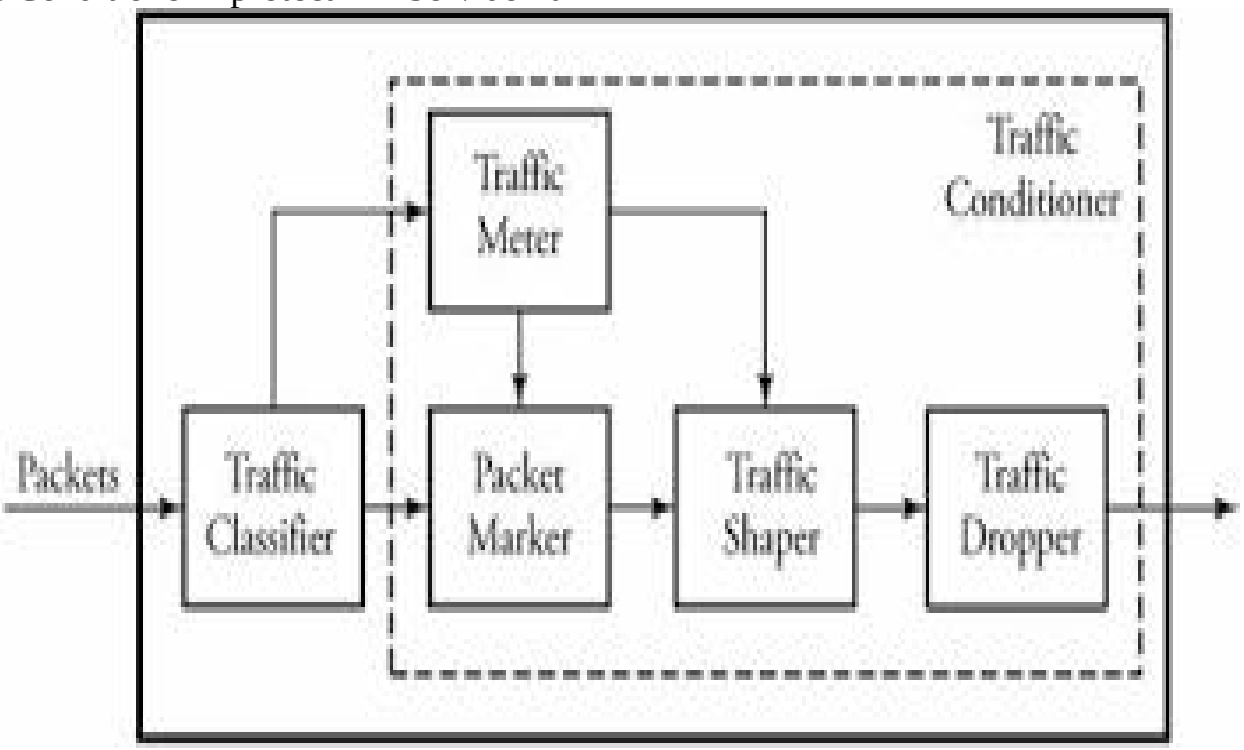
$m_3 = 1^{27} \,\%\, 55$

$= 1 \,\%\, 55$

$= \underline{\underline{1}}$

7. a) Explain the overview of differentiated services operation with a neat diagram.
[6] CO5 L2

It provides a simpler and more scalable QOS.
DS minimizes the amount of storage needed in a router by processing traffic flows in an aggregate manner, moving all the complex procedures from the core to the edge of the network.
Traffic Conditioner – protect DiffServ domain



Traffic conditioner includes 4 components :

Traffic meter – measures the traffic to make sure that packets do not exceed their traffic profiles.
Traffic marker – marks or unmarks packets inorder to keep track of their situations in the DS node.
Traffic shaper – delays any packet that is not complaint with the traffic profile.
Traffic dropper – discards any packet that violates its traffic profile.
Bandwidth broker – to manage the traffic - it operates in its own domain and maintains contact with other bandwidth brokers at neighboring domains.
Service Level Agreement(SLA) – It includes Traffic conditioning Agreement(TCA). SLA indicates the type of forwarding service and TCA presents all the traffic parameters that a customer receives.
SLA can be static or dynamic.
Static SLA – long term agreement
Dynamic SLA – uses bandwidth broker that allows users to make changes more frequently.
To establish traffic-policing scheme, a service provider uses,

Traffic classifier – routes packets to specific outputs based on the values found inside multiple fields of a packet header.
Traffic conditioner – detects and responds if any packet has violated any of the rules specified in the TCA.

DiffServ Field(8 bits)-to replace the IPv4 TOS field and the IPv6 traffic class field.
6 bits – used as differentiated services code point (DSCP) to specify its PHB.
2 bits – unused and ignored by the DS node

b) Explain VPN and its types based on tunnelling. [4]
CO5 L2

Tunneling

Tunneling can also beformed at network-and transport-layer protocols, where equallayers are involved,such asIP-in-IP tunnels.

A packet with alink-layer header, network-layerheader, and transport-layer header isa result of three packet encapsulation acts inwhich:

The payload has been encapsulated inthe transport-layer "segment,".

The result has been in turnencapsulated inthe network-layer "datagram,"

Finally that result has been encapsulatedin the link-layer."

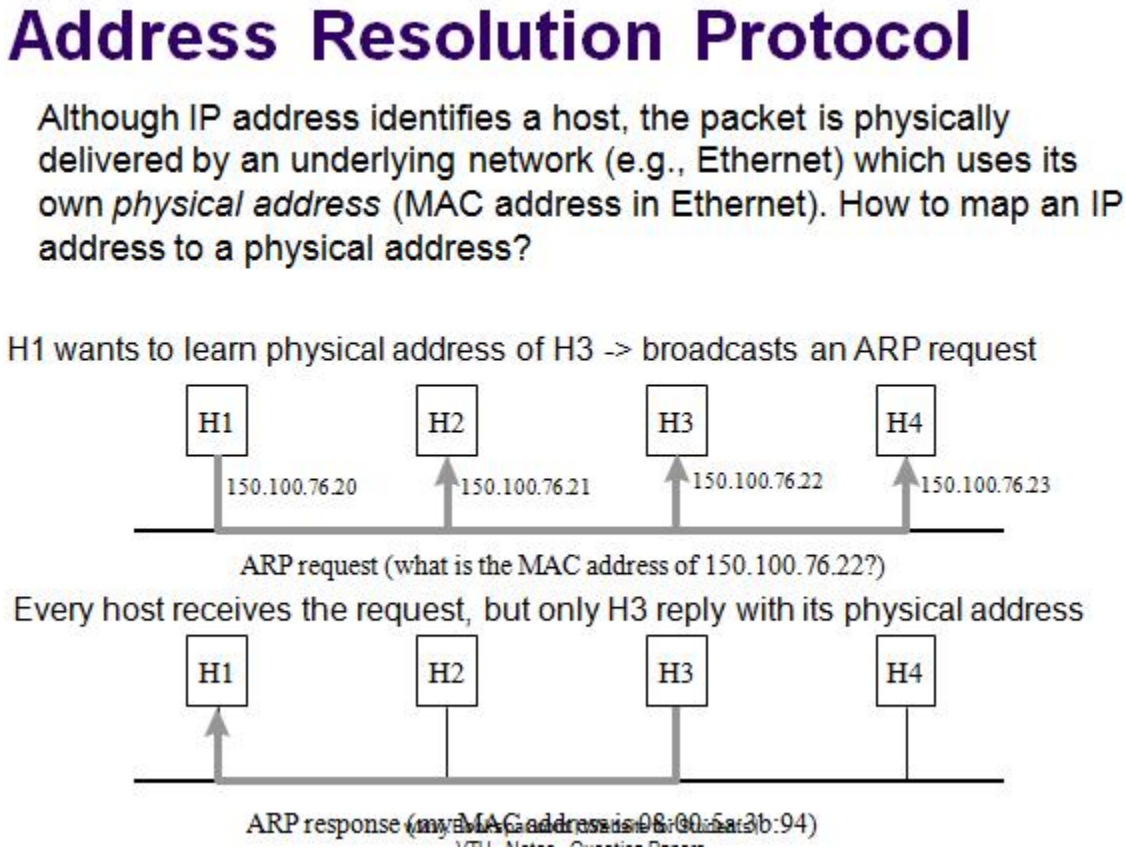
t

Two hosts are connectedthrough the Internetby using a**tunnel**:

The router adjacentto host 1prepares packets withIP1 and UDP1 headers (thelink-layer header isnot shown forsimplicity) and payload1.
IP1 implies thesource and destinationaddresses are host1 and host 2, respectively
When the packetreaches the beginningof the tunnel,R3 encapsulates the packetinto a newpacket with IP2addressing.
IP2 implies thesource and destinationaddresses inside the tunnel are R3to R6, respectively
IP1, UDP1, and payload1collectively shown bypayload2 are considered asthe payload ofthe newpacket.
We assumethat there isno change requiredon the transport-layer header, andthus, UDP1 canalso beused for the encapsulatingpacket.
The transport-layerheader could also beencapsulated and thus the newlycreated packet coulduse itsown transport protocol.
Tunneling protocols, such asthe**Point-to-PointProtocol(PPP)orthePoint-to-PointTunnelingProtocol(PPTP),** are encapsulating protocolsthat allow an organization to establish secure connectionsfrom one pointto another while using publicresources.
A PPP connectionis a serial connectionbetween a user and an Internetservice provider.

8. Explain the following:

a) Address Resolution protocol **[5] CO4 L2**



b) Write a note on structure of management information.

[5] CO5 L2

The Structure of Management Information (SMI), described in detail in RFC 1155, is a framework that describes the basic types of information that can be manipulated by SNMP. It provides a skeleton that specifies the basic format and hierarchy of management data but does not describe the objects that can be managed. Rather, it describes the building blocks from which managed objects are constructed.

A fundamental concept of SNMP is the notion of *object identifiers*. An object identifier (OID) is a tag that allows a management entity to refer unambiguously to a particular object. Object identifiers are allocated in a tree fashion. The value of the object identifier is a sequence of integers that refer to a particular traversal of the object tree. ``Object identifier hierarchy'', shows a portion of the object identifier hierarchy.

The root of the OID tree has no label. Currently, there are three children of the root, ccitt(0), iso(1), and joint-iso-ccitt(2). The ISO node has many children, one of which is org(3), which is allocated

for international organizations. Under org(3) is the U.S. Department of Defense, dod(6), which has the child internet(1).

The name *{ iso org dod internet }* is a symbolic representation for the integer series *1.3.6.1*. Both refer to the object identifier of the Internet subtree. In practice, *1.3.6.1* can simply be referred to as ``internet''. The terms *{ iso org dod internet }*, *1.3.6.1*, and *internet* are all different ways of identifying the same object. In SNMP PDUs, only the numeric sequences are used.