DI

NE UNIVERSITY

[redacted]

Instruction to Candidate

1. Candidate has to confirm seat number, subject and centre number printed on Bar code and write it on attendance sheet.
   विद्यार्थ्याने प्रथम वार कोडवरील आसन क्रमांक, विषय व केंद्र क्रमांक तपासून योग्य असल्याची खात्री करावी आणि उपस्थिती पत्रकावर नोंदवावी.
2. Paste Bar Code in prescribed space.
   उत्तरपत्रिकेवरील विहित जागेतच वार कोड लावावा.
3. Do not write anything on Bar code sticker, otherwise it will be treated as unfairmeans.
   वार कोड स्टिकरवर काहीही लिहू नये, अन्यथा परीक्षा गैरप्रकार समजला जाईल.

Q. No.	Examiner		Moderator	
1	—			
2	9	2		
3	1	0		
4	—			
5	1	0		
6	—			
7	1	0		
8				
9				
10				
11				
12				
Total in Figure	0	4	2	
Total in Words	Fourty two			
Signature				

Supplements attached		
Main Answer Book	No. of Supplements	Total
1 +	0	= 1

Specific remarks of Centre conductor regarding malpractice (in Red Ink)

Total	Marks in Figure	Marks in Words	Sign
Examiner	42	Fourty two	
Moderator			

१. विद्यार्थ्याने उत्तरपत्रिकेच्या मुखपृष्ठावर दिलेल्या सूचना उत्तरपत्रिकेवर आणि उपस्थिती पत्रकावर विहित जागेत आसन क्रमांक अंकात व अक्षरात बिनचूक लिहून स्वाक्षरी करावी.

२. उत्तरपत्रिकेवर फक्त निळ्या अथवा काळ्या शाईचा उपयोग करावा, अन्यथा उत्तरपत्रिकेचे मूल्यमापन केले जाणार नाही.

३. उत्तरपत्रिकेच्या पृष्ठक्रमांक ३ पासून लिहिण्यास प्रारंभ करावा.

४. संबंधित प्रश्नाचे अथवा उपप्रश्नाचे उत्तर जेथून सुरू होते तेथेच समासात प्रश्न क्रमांक, उपप्रश्न क्रमांक अचूक व स्पष्ट लिहावा, यासाठी वेगळ्या शाईचा उपयोग करु नये.

५. प्रत्येक पानाच्या दोन्ही बाजूस लिहावे, उत्तरपत्रिका किंवा पुरवणी उत्तरपत्रिकेचे कोणतेही पान फाडू नये, फाडल्यास परीक्षा गैरप्रकार समजून पुढील कार्यवाही करण्यात येईल.

६. पेपर संपण्यापूर्वी १० मिनिटे अगोदर इशारा घंटा होईल, त्यानंतर विद्यार्थ्याने उत्तरपत्रिका व पुरवणी उत्तरपत्रिकेवर होलोक्राफ्ट स्टिकर विहित जागेवरच लावावा.

Candidate shall fill all information about seat numbe paper etc. in prescribed space and sign on the answ book and attendance sheet.

Candidate shall use blue or black ink only. Otherwi answer book will not be evaluated.

Candidate shall start writing answers from page No of the answer book.

Candidate shall mention question number, su question number correctly at the beginning of the sam and shall not use ink other than blue or black.

Candidate shall write on both sides of pages. Shall n tear off any page, it will be treated as unfair means

Warning bell will be given before 10 minutes of t concluding time. Candidate shall paste Hollocra sticker at appropriate space on the answer book an supplements.

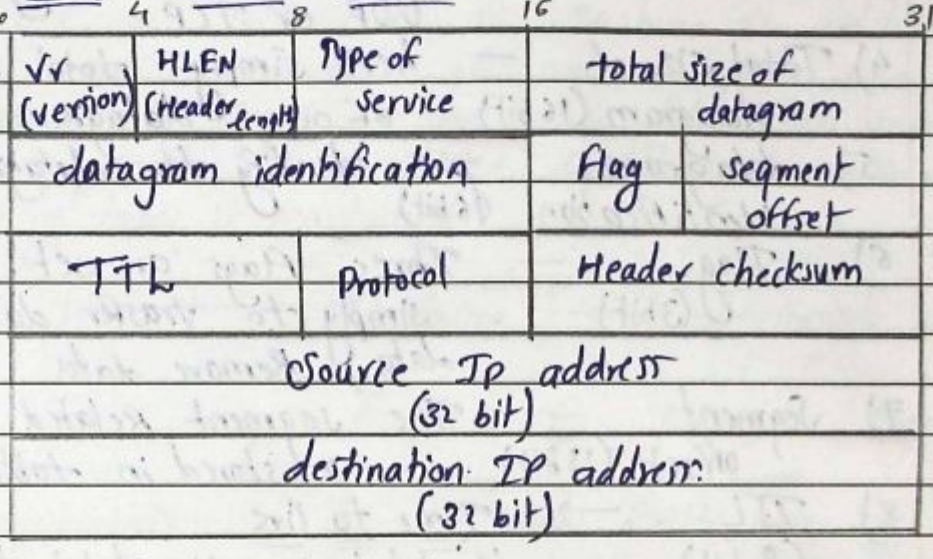
Examiner and Moderator has to write marks on given appropriate places only. Examiner should gi assessment tick(✓) or (x) in the margin.

Q. No.	Examiner	Moderator	Verification	Revaluatio
1	—			
2	12			
3	10			
4	—			
5	10			
6	~~10~~			
7	10			
8				
9				
10				
11				
12				
Total	42			

Q.2) ——→ ?

·a) ——→ ?

→ * IPV4 header Format:-



as we know in network layer to identify various devices uniquely we give each a IP adress by adding IP header to it.

The above figure shows header Format of IPV4 which contain several identifiers which can be explained in detail as follows:-

1) Vr — it gives version used in header (4 bit) either IPV4 or IPV6 (32 bit) (128 bit)

2) H.LEN — it define the length of header (4. bit)

प्र. क्र./ Q. No.

Q-2) → ?

a) → (continue)

→ 3) Type of service (8 bit) – it gives the type of service used while trasnfering info UDP or TCP

4) Total size of datagram (16 bit) – here simply total size of our datagram given

5) datagram identification (16 bit) – identify the datagram

6) Flag (3 bit) – Three flags are set. here simply to trasfer data add. data, Remove data

7) Segment offset (13 bit) – The segment Related info is stored in table or offset

8) TTL (8 bit) → Time to live – it determine the total time given to the packet for trasfer it is discarded if it passes time to live.

9) protocol (8 bit) → it determine which protocol is used.

10) Header Checksum (16 bit) → Check for errors in datagram & found then send back packet to source by using ICMP

11) Source IP adress (32 bit) – IP adress of source (Unique)

12) destination IP adress (32 bit) – IP adress of destination (unique)

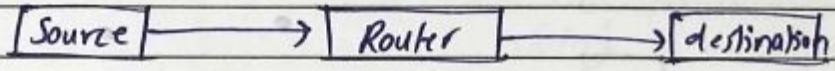
क्र./ Q. No.

Q.2) ⟶ ?.

c) ⟶ ?.

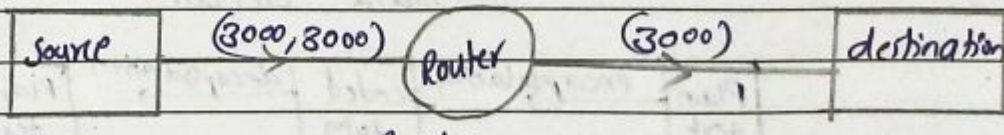
⟶

Their are many functions of Network layer as we know it is host to host delivery mech or user to destination or machine to machine. here no involvment of nodes it their like in data link layer here the data from source is passed to Router & Router to destination Routing table is maintained.



Their are various functions of Network layer:-

1) Fragmentation:- As we know Router have Fixed storage limit if source send more data than Router can receive data will overflow, So segmentation is followed where equal size segment are made & send over the Router So fragmentation is function of Network layer



. 6000 packets

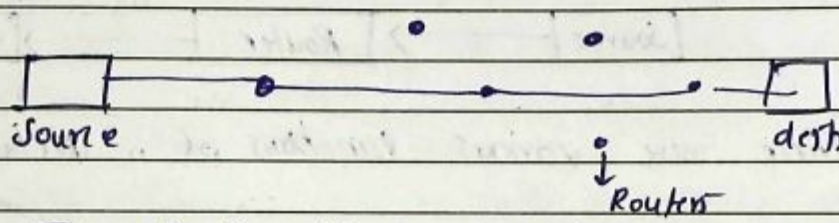
. Router 3000 capacity

प्र. क्र./ Q. No.

Q7) → ?

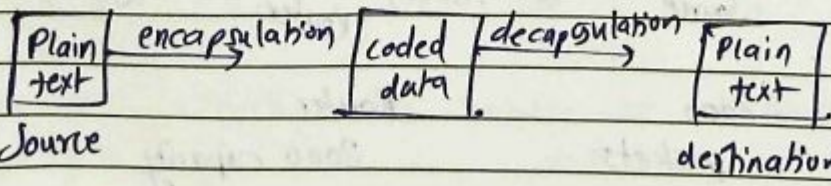
c) → (continue)

→ 2) Routing – here the shortest Path is found in Network layer by Routing through Routers for which Routing table is maintained. Its function is to find Optimal path from source to destination



For Routing it use Dijeskra or Bellman for algorithm & RIP & OSPF protoco it ignor other networks & Routers on way.

3) Packetising :– here we make packets by encapsulating the data then at destination end this packet from cipher text are converted back to plain text. here multiplex & demultiplexing of data occcur.



Q.2) → ?

c) → (continue)

→ Their are also other similar small functions of Network layer which are:-

1) congestion control – control sender from continuously sending data which will lead to Network conjet (Network will get fulfilled with data)

2) Flow control – The flow of data is limited so source & destination should match their capacity.

3) error control – Through using various protocol error on controlled by Network layer.

4) Forwarding – Forward the data to destination

5) analysing – it analysis overall Network for precautions & provide security at some extent.

———•———

प्र. क्र./ Q. No.

Q.3) → ?

→

a) → ?

→	TCP	UDP
1)	The full form of TCP is transmission controlt protocol	The full form of UDP is User datagram protocol.
2)	is Reliable	it is not Reliable.
3)	dom not provide broad casting service	provide pr brodcasting services.
4)	connection oriented	Connection less
5)	it gives gure guareehly of data Reachability	does not guarcenly data Reached to destination.
6)	most of protocol in Application layer prefer TCP	less preferd only prefered for RTP as braad casting.
7)	it support byte stream	it support msg stream
8)	Used in → HTTP → JMTP → IMAP	Used in → RTP
9)	error control, conjection control	No error control, conjetion co
10)	here packet are called Segment	here packet are called datagram

Q3) → ?

b) →

→ The RTP is transport layer protocol mainly used for multimedia services like video conferencing, as it is mainly used for broadcasting.

RTP is just the subpart of UDP which is also connection less & not so Reliable as Real time sending of datagram is done

Multimedia	} User inteface
RTP	
Socket	
UDP	} kernel interface
IP	
ethernet	

The RTP simply have its own header for data where the data is not made pass connection to connection it is send in broad casting manner.

We will get more about RTP by understanding its header (Refer fig. RTP header)

1) V → (2 bits) V in RTP header tell about the version of RTP header used

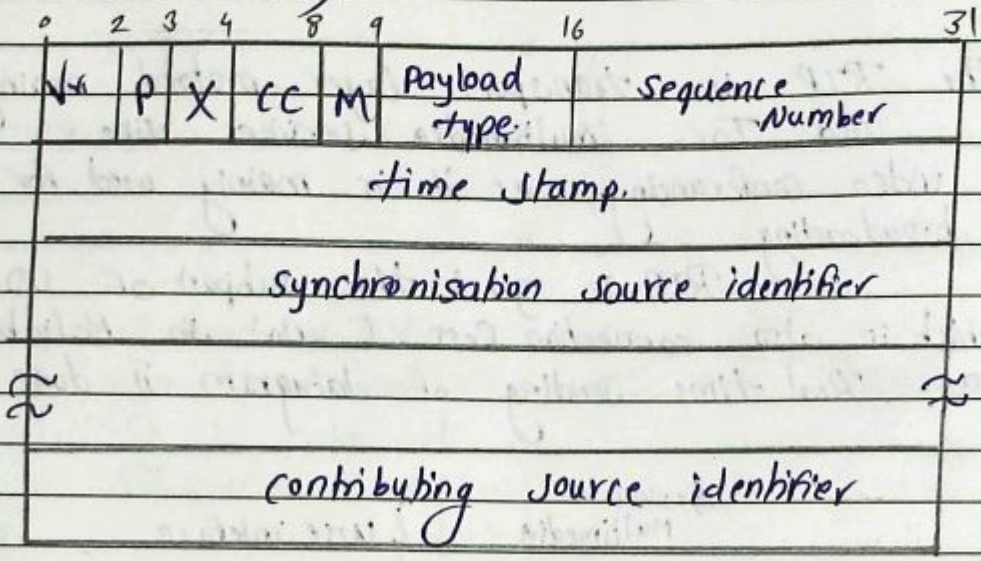
2) P → (1 bit) P means Padded in multiple of 4 bytes

प्र. क्र./ Q. No.

Q.3) →

b) → ? (continue)

→



3) X → extension used (1 bit)

4) CC → source identifier (4 bit)

5) Payload type → it identify the type of payload (7 bit)

6) Sequence Number → Unique sequence number is their for each packet/datagr (16 bit)

7) Synchronization Source identificer → find the source where datagram started beginn 16 (32 bit)

8) Time stamp (32 bit) → total time taken by a datagram to reach destin

9) contributing source identifier (32 bit) → find the source where the data needed to be sent or contributed.

प्र./ Q. No.

Q~~6~~) ⟶ ?.

Q.5) ⟶ ?

a) → ?

→ • DHCP ⟶ Dynamic Host control protocol

We know previously BOOTP was used to give adress to the particular name from our domain . ~~but~~ their the fixed Host adress where used and stored in Static table in where the problem arrised if devise want to change its Network.

So if devise want to shift between Netwo The tmparory adress is given to it by a help o DHCP – dynamic Host control protocol.

it has two approaches to give the devise the ip adress it need. as follows :-

1) if a device ark for static address the permonent adress is given to it & manual the network administrator store this information about the devise & adress in Static table. which is quite time consuming & also taking lot of effort of Network administrator & have disadvantage tha if the Network is changed then their occcurs error.

So to overcome this the dynamic IP adress concept was introduced.

Q. No.

Q.5) → ?

a) → (continue) →

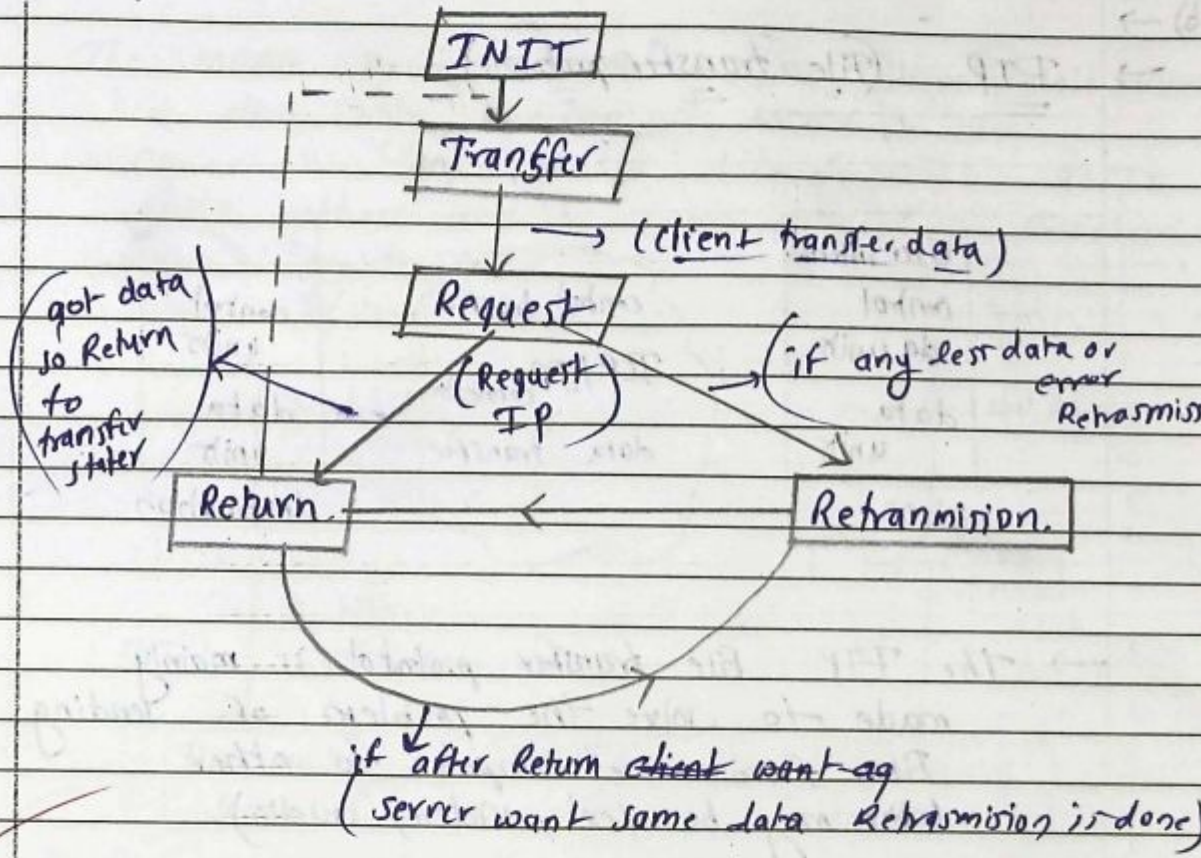
→ 2) Now here if we change Network the device ask for adress to Network, Network chack For the address in static table if it contain address give it to that device
→ BOOTP method.
But if their exist no address then the Network give it random addre From pool containing dynamic addresses

For a limited time, so dynamic addres is used for certain time only after the certain time end the device need to ask again for dynamic address from pool. So this is just temporary address for which also a table is maintained, dynomic Host table.
After ending of time this tempor adress go back into the pool of addresses.

INIT → to begin transfer
transfer → go to other network
Request → Request IP adress
Return → if have fixed IP.
Retrasmission → The IP selected from pool & temporily given to it.

(continue)

Q-7) a) → DHCP State client diagram.



here the device come to other network
then Request IP
if IP already then Return
if No. ip then temporary IP is given

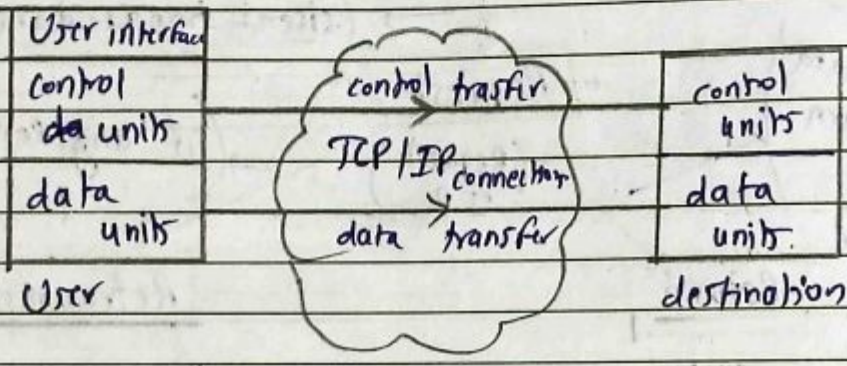
प्र. क्र./ Q. No.

Q.5) → 2

1) → (~~continue~~)

b) →

→ FTP (File transfer protocol.)



→ The FTP file transfer protocol is mainly made to solve the problem of sending File from one computer to other (file may be text, video, audio)

→ FTP uses TCP so it is reliable, connection or can error control, conjection control & most important it quareenty packet transfer

→ here the control transfer & data transfer 2 TC connections are established

→ The control connection work from start to end of process

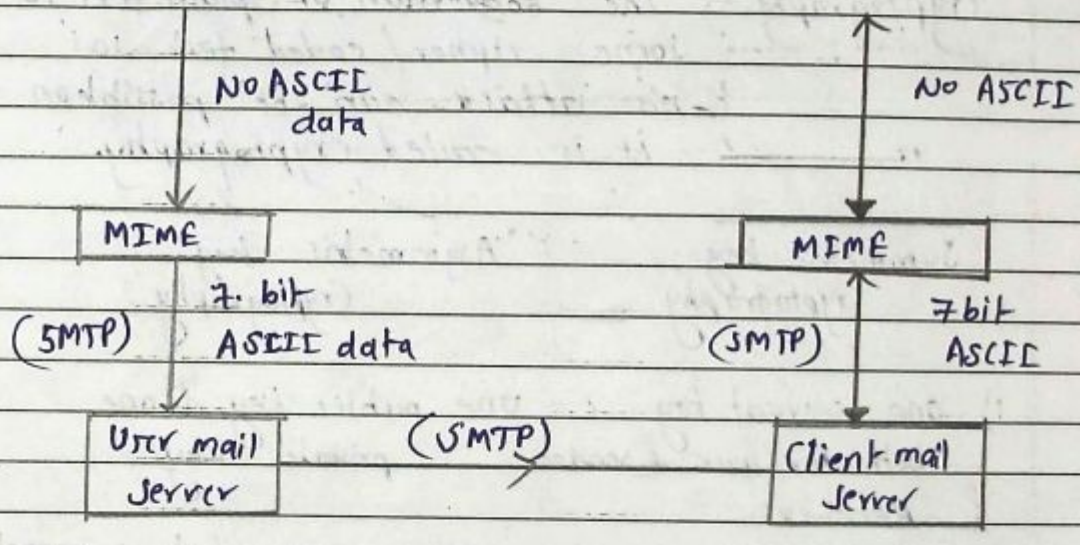
→ but the data connection send data & immidiately close connection.

Q.5) → ?

b) (continue)

→ MIME

The MIME Refer to multi purpose Internet Mail exten here the only function of MIME is to Convert No - ASCII data to 7 bit ASCII data then send it from sender to Receiver Server by SMTP.



Simply here at MIME the encapsulation of various data as images, video audio is done then the data encapsulated then from user mail server to client mail server the data in 7-bit ASCII send by using Simple mail transfer protocol then again at server end the 7 bit ASCII is converted to original data and used by it. the Client.

The function of MIME is limited to conversion of NO ASCII → 7 bit ASCII (charac

प्र. क्र./ Q. No.

Q. 7) → ?.

b) → (~~continue~~) → ?

→ Their are 2 types of cryptography used to keep data security.

① symmetric key
② Asymmetric key.

Cryptography – The conversion of plain text to some cipher/coded text so no attack can be possible on it is called cryptography.

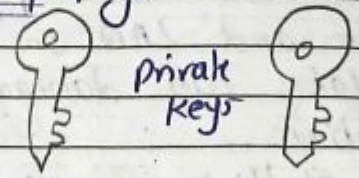
Symmetric key Cryptography	Asymmetric key Cryptography
1) one secreat key both for ~~user~~ & sender & Receiver	one public key & one private key
2) Fast process	Slow compored to symmetric
3) used for small data	Used For larger data.
4) Key may get lost in network	~~Ke~~ Private key is always with user so no lost
5) only who have private key can make changes.	anyone can store data using public key

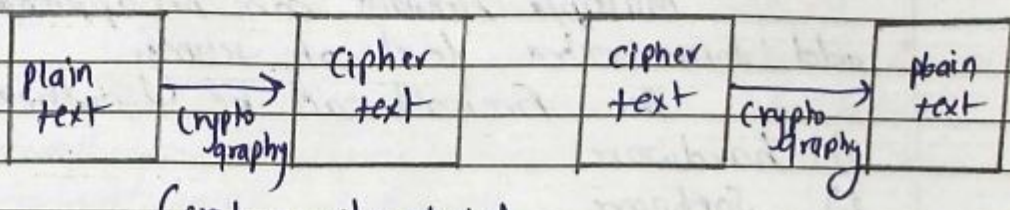
Q. No.

2.7) → ?

b) → (continue)

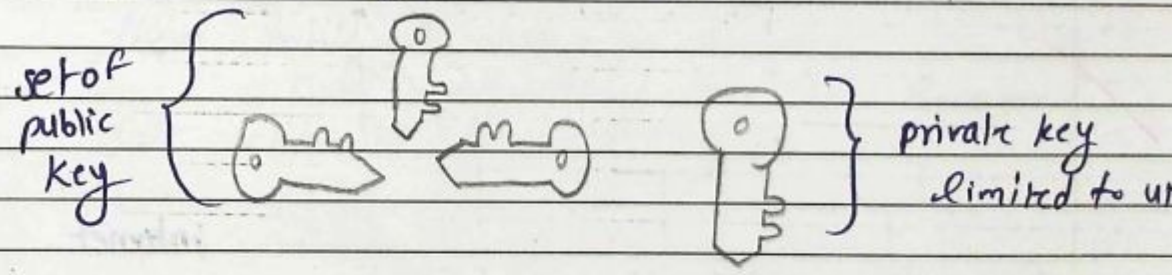
→ → Symmetric key cryptography.

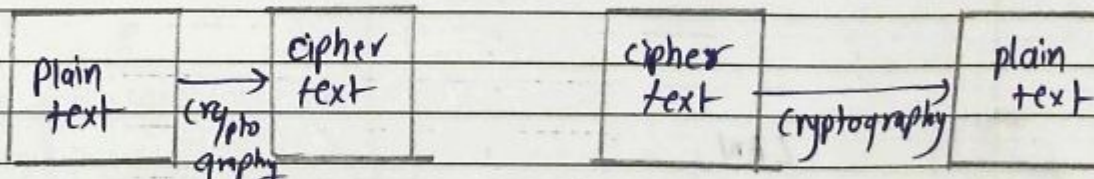




(or by cryptanalysis)

→ asymmetric key cryptography





4

प्र. क्र./ Q. No.

Q.7) → ?

c) → ?.

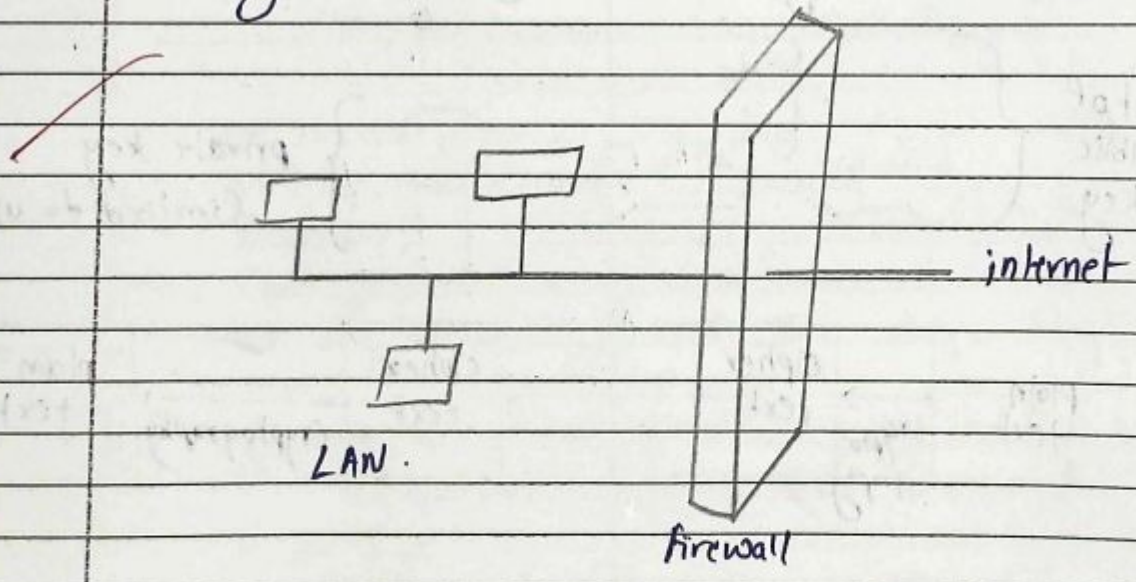
→ The firewall is simply applied between internet and LAN so no internet commands or data can damage our important information.

Multiple firewalls can be applied to add some extra level of security.

The firewall can be either:-

1) hardware
2) software

main aspect of firewall is to give security to our LAN.



the firewall check the incoming data make it flow through it & penetrate and go to find for viruses & threats

Q7) → ?

c) → (continue)

→ The firewall also make data error resolve somehi but definetly to check data going through and analysing it checking for viruses Ih it is main function of firewall.

if the user or some human gave firewal info then it can be broken so to break firewall the information is just enough ≥ disadvantage of ~~of~~ firewall.

and talking about adrantage it have many advantage as it increase our device duration make them secure & keep them stable & always performing.

Our confidential data is Remained safe with us.

4

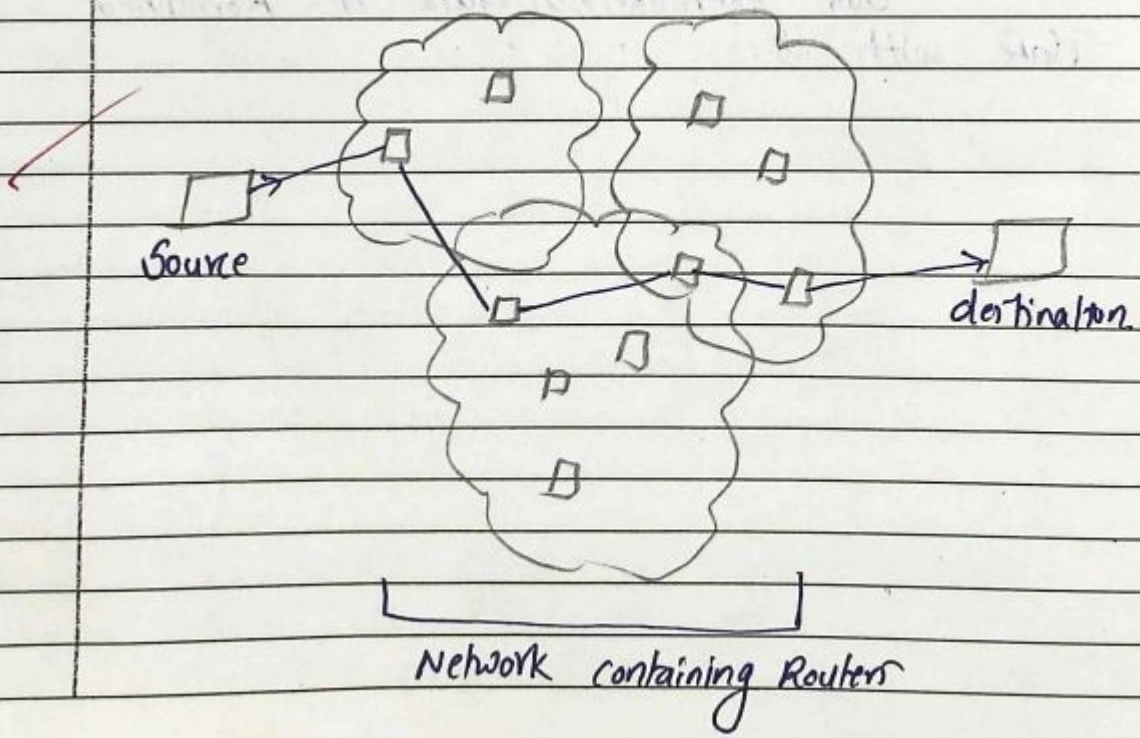
प्र. क्र./ Q. No.

Q.2) → ?

b) → ?

→ OSPF → Open Shortest path First
- it is a Network layer protocol.
- it is protocol used in Link State Routing which Follow the dijestras algorithm to Find shortest path from Router to Router.

OSPF the node copy is maintained while traversing through router and then the small info is send to all nodes of the network & similarly the procedure continues to follow & find shortest path where the path should be predecided in Networks



प्र./ Q. No.

Q.2) → ?

b) → (continue)

→ The OSPF → here it mainly is simple to implent unlike RIP which have complex algorithm & complex calculation.

here only the neighboring node distance from working node is taken in consideration of finding OSPF is largely used on work scale today in day to day computer examples.

The OSPF & BGP are used in Link State Routing where as RIPv6 & RIPv4 used in distance vector Routing.

All are used to find the optimal path from source to destination.

3/

प्र. क्र./ Q. No. Q-3) → ?

c) → ?

→ as we know UDP header formatis

0	16	31
Source port No		destination port No
Header(datagram) length		Header Checksum
data (optional)		

here we have given,

Source port no → the port No of source from where UDP is comming

destination port no → port No of destination where UDP is going

Checksum → to calculate error

Header length → total length of datagram in header.

given 06 32 000D 001C E2 17.

Source port NO :- 06 ~~000D~~

destination port NO :- ~~32~~ ~~001C~~ 000D

total length of datagram :- ~~16 bit~~ / ~~E2 17~~. D

Q7) → ?

a) → ?

→ The IP sec simply tell us about the security provided to IP address as we know IP Header contain a lot of data like

1) type of service
2) total size
3) daqtaqram type
4) Flag.
5) TTL
6) Protocol
7) Source IP address
8) destination IP address

So this is confidential information we need to protect from the Active as well as passive attack as in UDP & TCP both IP segment are used with header while transfer we will give IPsec the Right to Remove its own vulnerability or encoding the IP adress so that it can not be identified by attacker

simply we can encode the IP address of source & destination in cipher text by cryptography with the help of cryptanalysis by cryptanalyst so we can use it secretely from souce to destination

– Providing security to IP address is efficient to save our confidential data.