20-21

2 a) Given that,

MTU = 1500

Total datagram = 5000 - 20
= 4980 bytes

Data per fragement = 1500 - 20
= 1480 (It's divisible by 8)

The number of fragment = 4980 ÷ 1480
= 3.36

So, here required four fragment 3 full sized one final smaller fragment

Data size and offset values

Fragment #	Data size	offset	More fragment MF
1	1480	0/8 = 0	1 (set)
2	1480	1480/8 = 185	1 (set)
3	1480	2960/8 = 370	1 (Set)
4	(4980 - 4440) 540 Remaining	4440/8 = 555	0 (no set)

3a) Given that

IP 172.30.0.0/16

i) 11111111 11111111 00000000 00000000

255. 255. 0. 0

Subnet Mask: 255.255.0.0

ii) Find the number of address in each subnet

$2^{32-16} = 2^{16} = 65536$

20-21

3a) given that

IP 172.30.0.0/16

It wants to create 256 subnet so, $\log_2(256) = 8$

additional bit for subneting

new prefix = 16+8 = 24

(i) 11111111 11111111 11111111 00000000

255. 255. 255. 0

Subnet MASK = 255.255.255.0

ii) number of address each subnet

$2^{32-24} = 2^8 = 256$

Usable host 254

iii) Subnet 10

Network address 172.30.9.0

First host address 172.30.9.1

Last host address 172.30.9.254

Broadcast address 172.30.9.255

iv) subnet 256

Network address 172.30.255.0

First host " 172.30.255.1

Last " " 172.30.255.254

Broadcast " 172.30.255.255

b) Symmetric key encryption

Symmetric encryption is a method in which the same key is used for both encryption and dycryption. The sender and receiver must share this secret key securely in advance

Example: AES, DES.

AES → encrypting large file or data streams

Compare Symmetric and Asymmetric Encryption

Symmetric	Asymmetric
One shared secret key for both encrypt & decrypt	Tow keys: public key (encrypt) and private key (decrypt)
Very fast, suitable for bulk data	Slower, due to complex math
Hard to share the secret key securely	Easier: public key is openly shared
Example: AES, DES, 3DES	Example: RSA, ECC

20=

c) Advantages of IPV6

1. Larger address space: IPV6 uses 16-bit address providing a virtually unlimited number of IP addresses compared to IPV4's 32 bit space
2. Built-in security (IPSec): IPV6 was design with mandatory IPsec support, improving confidentially and authentication

Disadvantages of IPV6

1. Compatibility Issues: IPV6 is not backword-compatible with IPV4, requiring tunneling, dual stack or translation mechanisms.

2. Deployment cost: upgrading hardware, software and training administrators increases the cost and complexity of migration.

20-21

4 a) Given that

Total length $= (00A0)_{16}$

$= 160_{10}$

HLEN = value = 5

Header length = 5 x 4 = 20 bytes

Payload = Total length - Header length

= 160 - 20 = 140

$$\text{Efficiency} = \frac{140}{160} \times 100\%$$

$$= 87.5\%$$

4 b) NAT (Network Address translation) is a technique used in routers to translate private IP addresses inside a local network into a public IP address for communication over the internet. It allows multiple internal hosts to access external networks using a single public IPv4 address.

How NAT helps in address depletion

~~1. Conserves public IPV4 address~~

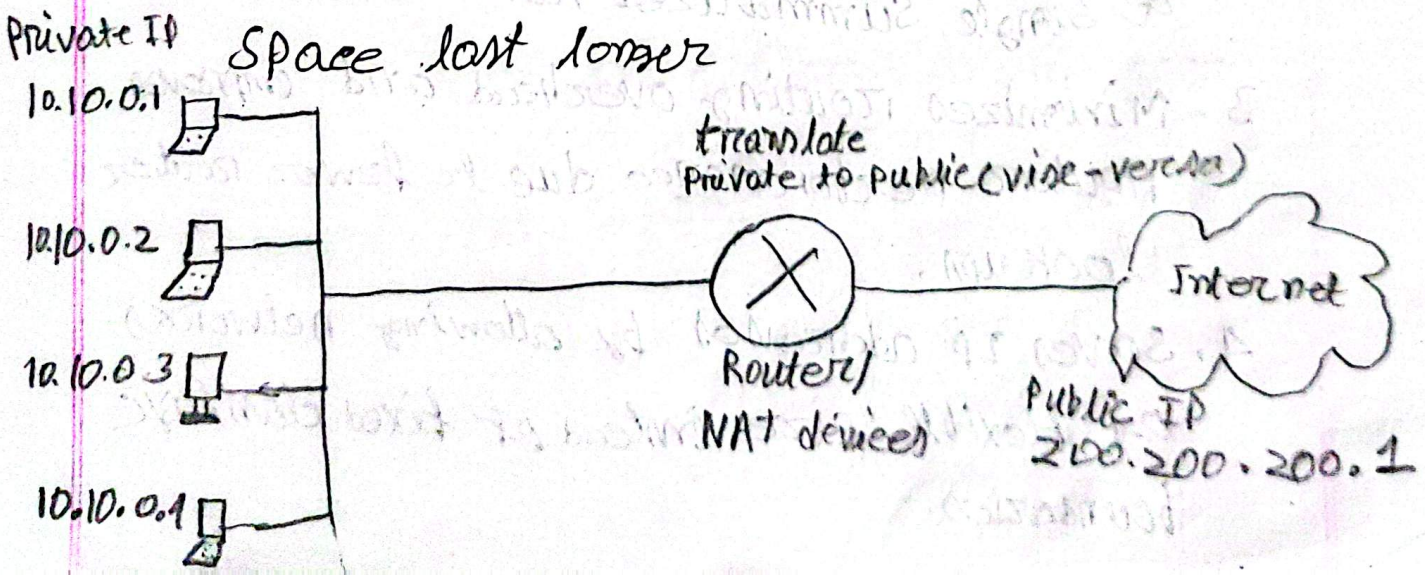
1. NAT lets many devices in a private network use private IP addresses, which do not require public registration.

2. When these ~~dir~~devices access the internet, NAT changes their private addresses to one shared public IP

3. Because of sharing, an organization doesn't need a separate public IP for every computer or device.

4. This greatly reduced the number of public IPV4 addresses that are needed in the world

5. In this way, NAT helps ~~sto~~slow down IPV4 address depletion and makes the limited address space last longer



20-21

5. b) CIDR (classless Inter-Domain Routing)

CIDR is an IP addressing method that replaces the old classful addressing. It represents addresses using network prefixes (192.168.1.0/24) instead of fixed classes (A, B, C). CIDR allows network of variable size using variable-length subnet masking

CIDR contributes to address aggregation in these ways:

1. Combines multiple continuous networks into one lager block (called Supernetting)
   Example: several /24 networks can be aggregated into one /22 block.
2. Reduces the number of routing table entries because mutiple routes become a single summarized route
3. Minimizes routing overhead and improves router performance due to fewer router look ups.
4. Saves IP addresses by allowing networks of flexible size instead of fixed class A/B/C boundaries.

Final 19-20

3 a) Given that

Network address : 192.168.10.0

Subnet mask : 255.255.255.252

i) subnet mask binary

11111111. 11111111. 11111111. 1111 1100

No of subnets $= 2^6 = 64$

ii) Per subnet ~~ho~~ usable host $= 2^2 - 2 = 2$

Total ~~ho~~ no_of_host $= 2 \times 64 = 128$

iii) The valid subnets

Here subnet block size $= 2^2 = 4$

192.168.10.0

192.168.10.4

192.168.10.8

.

.

.

192.168.10.252

(iv)

Meaning	Subnet1	Subnet2	Subnet3	Subnet4	Subnet5	Subnet6
subnet address	192.168.10.0	192.168.10.4	192.168.10.8	192.168.10.12	 16	 20
First valid host	192.168.10.1	192.168.10.5	 9	192.168.10.13	... 17	 21
Last valid host	192.168.10.2	192.168.10.6	 10	 14	... 18	... 22
Broadcast address	192.168.10.3	192.168.10.7	... 11	... 15	... 19	... 23

10-20

4c) Given that

MTU = 1200

Total datagram = 4000 - 20

= 3980

Maximum pay load Per fragment = 1200-20

= 1180

1180 is not divisible by 8

then, 1180 ÷ 8 = 147.5 → floor

= 147 X 8

= 1176

The number of fragment need = 3980 ÷ 1176

= 3.38

So, Here required 4 fragment 3 full size+

one final smaller fragment

Data size and offset value

Fragment	Payload bytes	Total Data Size	Offset	MF
1	1176	1176+20 = 1196	0/8 = 0	1 (Set)
2	1176	= 1196	1176/8 = 147	1
3	1176	1196	2352/8 = 294	1
4	452	452+20 = 472	3528/8 = 441	0

Final - 2018-19

2(a) Same as 19-20 4(c) Just change MTU = 1400

3a) Given that,

Network address : 192.168.10.0

Subnet mask : 255.255.255.224

i) Subnet mask convert to binary

11111111. 11111111. 11111111. 1110 0000

Total subnet mask $= 2^3$

$= 8$

ii) Each subnet total host $= 2^5 - 2$

$= 30$

Total no. of host $= 8 \times 30$

$= 240$ Ans

iii) The valid subnets

192.168.10.0

192.168.10.32

192.168.10.64

192.168.10.96

192.168.10.128

192.168.10.160

192.168.10.192

192.168.10.224

(iv)

Meaning	Subnet address	First Valid host	Last Valid host	Broadcast Address
Subnet 1	192.168.10.0	192.168.10.1	192.168.10.30	192.168.10.31
Subnet 2	192.168.10.32	192.168.10.33	192.168.10.62	192.168.10.63
Subnet 3	192.168.10.64	192.168.10.65	192.168.10.94	192.168.10.95
Subnet 4	192.168.10.96	192.168.10.97	192.168.10.126	192.168.10.127
Subnet 5	192.168.10.128	192.168.10.129	192.168.10.158	192.168.10.159
Subnet 6	192.168.10.160	192.168.10.161	192.168.10.190	192.168.10.191

4a) It's same as 20-21 4(a)

4c)

Type of address used in the LAN

Inside the LAN, hosts use private IP address (eg., 192.168.x.x, 10.x.x.x). These private are not routable on Internet. The NAT device itself has one public IP address used for all external communication.

The NAT device functions

(i) outgoing traffic

1. A LAN device send a packet, ~~Reference~~ using private IP address
2. The NAT router receives the packet, replaces the private source IP with its public IP.

3. NAT assigns a unique port ~~Alber~~ number to the connection and creates a mapping. This technique is called port address translation - PAT

4. The packet is sent to the internet using the NAT's public IP Address

(b) ii) Incoming traffic

1. When a reply comes back from the internet NAT checks its mapping table.
2. NAT identifies the correct internal private host based on the public port number
3. NAT forwards the packet to the correct LAN device

i) Issue that may appear

- External devices cannot initiate connections to private hosts
- Port exhaustion may occur if many connections are active.
- Some application embed private IPs in the payload, causing translation problems

- Measured NAT: uses to solve the issues
  - Port Forwarding: allows selected services to be reachable from outside.
  - PAT: uses different port numbers to allow many devices to share one public IP.
  - ALG: rewrites embedded private IPs for special protocols
  - Stateful inspection: keeps track of all active sessions for security and correct routing