National University
Of Computer and Emerging Sciences

Assignment-03

In partial
fulfillment of the requirements
for the course of

FA2024-CS3001

Computer Networks

By:

Maryam Masood
22i-1169
BSCS-C

Question:01

(a) Number and Range of Addresses:

Number of Addresses

$2^{32-21} = 2^{11} = 2048$ addresses

Range of Addresses

Starting address : 200.100.50.0

Ending address : First + Total − 1 =

200.100.50.0 + 2048 − 1 = 200.100.57.255

Range : 200.100.50.0 to 200.100.57.255

(b) Range of Address for each Organization

1) Three organizations, each req 400 addresses

$2^9 = 512$ requires /23 subnets.

2) Two organizations, each req 150 addresses.

$2^8 = 256$ requires /24 subnets.

3) Four organizations, each req 30 addresses

$2^5 = 32$ requires /27 subnets.

Org 1 : 200.100.50.0 — 200.100.51.255

Org 2 : 200.100.52.0 — 200.100.53.255

Org 3 : 200.100.54.0 — 200.100.55.255

Org 4 : 200.100.56.0 — 200.100.56.255

Org 5 : 200.100.57.0 — 200.100.57.255

Org 6 : 200.100.58.0 — 200.100.58.31

Org 7 : 200.100.58.32 — 200.100.58.63

Org 8 : 200.100.58.64 — 200.100.58.95

Org 9 : 200.100.58.96 — 200.100.58.127

Unallocated addresses

200.100.58.128 to 200.100.

2048 - (512×3 + 256×2 + 32×4)

= 384 addresses

(c)

ISB Block: 200.100.50.0/21

Allocated Subnets

Three /23: 200.100.50.0/23
200.100.52.0/23
200.100.54.0/23

Two /24: 200.100.56.0/24
200.100.57.0/24

Four /27: 200.100.58.0/27
200.100.58.32/27
200.100.58.64/27
200.100.58.96/27

Unallocated Block: 200.100.58.128/26
200.100.59.0/24

Forwarding Table

Subnet	Destination
200.100.50.0/23	Org 1
200.100.52.0/23	Org 2
200.100.54.0/23	Org 3
200.100.56.0/24	Org 4
200.100.57.0/24	Org 5
200.100.58.0/27	Org 6
200.100.58.32/27	Org 7

Subnet	Destination
200.100.58.64/27	org8
200.100.58.96/27	org9
200.100.58.128/26	Unallocated

Question:02

Block A: 72.15.40.0/26

72.15.40.0 to 72.15.40.63

$2^{32-26} = 64$ addresses

Block b: 72.15.40.64/26

72.15.40.64 to 72.15.40.127

64 addresses

Block c: 72.15.40.128/25

72.15.40.128 to 72.15.40.255

128 addresses.

Block d:

72.15.41.0 to 72.15.41.255

256 addresses

Step 1:

Block a and Block b are contiguous (no gaps).

When two /26 blocks are combined, they form a larger block with a shorter prefix:

Combined Range: 72.15.40.0 to 72.15.40.127

New prefix: /25

72.15.40.0/25

Step 2:

72.15.40.0/25 covers 72.15.40.0 to 72.15.40.127

Block c (72.15.40.128/25) covers 72.15.40.128 to 72.15.40.255

These two blocks are also contiguous.

Combined range: 72.15.40.0 to 72.15.40.255

New prefix: /24

72.15.40.0/24

Step 3:

72.15.40.0/24 covers 72.15.40.0 to 72.15.40.255

72.15.40.0

72.15.41.0/24 (Block d) covers 72.15.41.0 to 72.15.41.255

These two blocks are also contiguous.

Combined range: 72.15.40.0 to 72.15.41.255

New prefix: /23

72.15.40.0/23

Final Block: 72.15.40.0/23

Question: 03

Challenges:

1) Addressability: NAT hides private IPs, preventing direct connections between peers.
2) Port Mapping: Dynamic and unpredictable port mappings make locating peers difficult.

3) Symmetric NAT: Restrictive NAT types block most direct connections.
4) Traffic Blocking: NAT restricts unsolicited incoming traffic.
5) Protocol Issues: NAT often struggles with non-standard P2P protocols.

Strategies:

1) STUN: Discovers public IP/port mappings.
2) TURN: Relays traffic via a server when direct connections fail
3) ICE: Combines STUN and TURN to find the best path.
4) Hole Punching: Establishes direct connections using a third-party server.
5) Keep-Alive: Maintains NAT mappings by sending periodic packets.
6) Port Forwarding: Configures NAT manually for specific traffic.

Key Terms:

NAT traversal: Methods to establish connections through NAT.

Hole Punching: Exploits NAT behaviour for direct links.

Relay Server: An intermediary for NAT-restricted connections

ICE Candidate: Potential connection paths in the ICE framework.

Question:04

The prefix 203.0.113.128/26 represents the address range from 203.0.113.128 to 203.0.113.191

⇒ Example IP: 203.0.113.130.

The prefix 203.0.113.0/26 represents the address range from 203.0.113.0 to 203.0.113.63. It contains $2^{32-26} = 64$ ip addresses.

To divide this into five subnets of equal size:

1) Each subnet must have the same number of IP addresses.
2) The closest power of 2 greater than or equal to 5 is 8 (2^3)
3) Each subnet must have a block size of 64/8 = 8 addresses
4) The subnet mask will change to /29 (since $2^{32-29} = 8$)

Subnets for Five Blocks

1) 203.0.113.0/29
   Range: 203.0.113.0 to 203.0.113.7
2) 203.0.113.8/29
   Range: 203.0.113.8 to 203.0.113.15
3) 203.0.113.16/29
   Range: 203.0.113.16 to 203.0.113.23
4) 203.0.113.24/29
   Range: 203.0.113.24 to 203.0.113.31
5) 203.0.113.32/29
   Range: 203.0.113.32 to 203.0.113.39

Remaining addresses in the range from 203.0.113.40 to 203.0.113.63 can be used for future allocation.

Question:05

Subnet 1: $50+2=52 \rightarrow 2^6=64$ Mask: /26

Subnet 2: $120+2=122 \rightarrow 2^7=128$ Mask: /25

Subnet 3: $30+2=32 \rightarrow 2^5=32$ Mask: /27

Subnet 4: $10+2=12 \rightarrow 2^4=16$ Mask: /28

Subnet Allocation:

Subnet	Prefix	Address Range
1	198.51.100.0/26	198.51.100.0 – 198.51.100.63
2	198.51.100.64/25	198.51.100.64 – 198.51.100.191
3	198.51.100.192/27	198.51.100.192 – 198.51.100.223
4	198.51.100.224/28	198.51.100.224 – 198.51.100.239

Question:06

(a)

Group packets by NAT-assigned external ports and monitor sequential IP identification numbers. Each internal host generates its own sequence of IDs, allowing you to distinguish hosts. Full-cone NAT simplifies this as mappings remain consistent for each host.

(b)

This approach fails because random IDs lack sequence patterns, and symmetric NAT maps the same internal IP/port to different external ports based on the destination. A

(c)

Fragmentation makes detection harder since all fragments of a packet share the same ID, and NAT might modify headers. You can reconstruct fragmented packets using fragment offsets and flags. Transport-layer information in the first fragment can help associate fragments with their source.

(d)

UDP lacks sequential ID behaviours, so detection must rely on NAT-assigned port mappings and analyzing traffic patterns (e.g timing or volume). While less precise, observing external port allocations by the NAT can still indicate distinct internal hosts.

Question: 07

(a)

MTU: 1500 bytes

Payload per fragment = 1500 − 20 = 1480 bytes

Original Datagram Size: 13,120 bytes

Payload Size = 13120 − 20 = 13,100 bytes

Number of fragments = $\lceil 13{,}100 / 1480 \rceil$ = 9 fragments

Size of fragments

1-8 : 1500 bytes (1480 + 20 header)

1-9: $13100 - (8 \times 1480) = 1260$ bytes

Total Size = $1260 + 20 = 1280$ bytes

(b)

Fragment	Payload	Length	Identification	Flags	Offset (8-byte)
1	1480	1500	8721	1	0
2	1480	1500	8721	1	185 (1480/8)
3	1480	1500	8721	1	370 (1480×2/8)
4	1480	1500	8721	1	555
5	1480	1500	8721	1	740
6	1480	1500	8721	1	925
7	1480	1500	8721	1	1110
8	1480	1500	8721	1	1295
9	1260	1280	8721	0	1480

(c)

The DF flag prevents fragmentation. Since the datagram exceeds the MTU (1500 bytes), the router cannot forward it.

The router drops the datagram and sends an ICMP "Fragmentation Needed" error back to the sender, including the MTU (1500 bytes).

The sender must reduce the datagram size to fit within the MTU, typically using Path MTU Delivery.

Question:08

Address Class C (subnet mask 255.255.255.0)

Custom Subnet Mask

Boston + R&D → 9+10=19 hosts + 2 = 21 ($2^5=32$)

New York → 7 hosts +2 = 9 ($2^4=16$)

Serial Link (Router A to B) → 2 + 2 = 4 ($2^2=4$)

Boston + R&D → /27 (255.255.255.224)

New York → /28 (255.255.255.240)

Serial Link → /30 (255.255.255.252)

Minimum number of subnets needed 3

Boston + R&D: 1 NY: 1 Serial Link: 1

Number of host addresses in the Largest Subnet Group

Boston + R&D reqs 21 addresses.

we are using /27 so 30 usable host addresses

Arrange sub-networks from Largest to Smallest

1) Boston & R&D /27
2) New York /28
3) Serial Link /30

IP Address Ranges

Router A F0/0 Range: 192.168.1.0 – 192.168.1.31

usable IPs: 192.168.1.1 – 192.168.1.30

New York Range: 192.168.1.32 – 192.168.1.47

Usable IPs: 192.168.1.33 – 192.168.1.46

Routers A to B Ranges 192.168.1.48 – 192.168.1.51

Usable IPs: 192.168.1.49 – 192.168.1.50

Question:09

Address Class B Subnet Mask 255.255.0.0

Custom Subnet Mask

Management + Sales: 30 + 85 = 115 + 2 = 117 ($2^7 = 128$)

/25 (255.255.255.128)

Research: 65 + 2 = 67 ($2^7 = 128$)

/25 (255.255.255.128)

Marketing: 15 + 2 = 17 ($2^5 = 32$)

/27 (255.255.255.224)

Router A to B: 2 + 2 = 4 ($2^2 = 4$)

/30 (255.255.255.252)

Minimum Number of Subnets Needed 4

Number of Host Addresses in the Largest Subnet group

Management + Sales → 115 hosts.

/25 subnet provides 126 usable hosts

Subnet Arrangement

Management + Sales /25

Research /25

Marketing /27

Router A to B /30

IP Address Ranges

Management + Sales: 172.16.0.0 – 172.16.0.127

usable IPs: 172.16.0.1 – 172.16.0.126

Research: 172.16.0.128 – 172.16.0.255

usable IPs: 172.16.0.129 – 172.16.0.254

Marketing: 172.16.1.0 – 172.16.1.31

usable IPs: 172.16.1.1 – 172.16.1.30

Router A to B: 172.16.1.32 – 172.16.1.35

usable IPs: 172.16.1.33 – 172.16.1.34

Question : 10

IP: 172.16.0.0 Subnet Mask 255.255.0.0

Address Class B

Custom Subnet Mask

Ft. Worth : 3200 + 2 = 3202 (2^{12} = 4096)

/20 (255.255.240.0)

Dallas : 2650 + 2 = 2652 (2^{12} = 4096)

/20 (255.255.240.0)

Router A to B, A to C, C to D : 2 + 2 = 4 (2^2 = 4)

/30 (255.255.255.252)

Minimum Number of Subnets Needed 5

Number of host addresses in largest subnet group

Ft Worth → 3200 hosts

/20 subnet provides 4094 usable hosts

Subnet Arrangement

Ft. Worth /20

Dallas /20

Router A to B /30

Router A to C /30

Router C to D /30

IP Address Ranges:-

Ft. Worth 172.16.0.0 – 172.16.15.255

usable IPs: 172.16.0.1 – 172.16.15.254

Dallas 172.16.16.0 – 172.16.31.255

usable IPs: 172.16.16.1 – 172.16.31.254

Router A to B 172.16.32.0 – 172.16.32.3

usable IPs: 172.16.32.1 – 172.16.32.2

Router A to C 172.16.32.4 – 172.16.32.7

usable IPs: 172.16.32.5 – 172.16.32.6

Router C to D 172.16.32.8 – 172.16.32.11

usable IPs: 172.16.32.7 – 172.16.32.10