Name: MD. Akhlakur Rahman Zowarder

ID: 22299464

Section: 23

Spring25 (B)

1

I) IP address = 3.12.66.26/19

Network bits = 19

∴ Network address = 3.12.64.0/19

II)

Segment	End Devices	+Router interface	Needed Hosts	Best subnet
R2 LAN	1000	+1	1001	122
SW LAN	509	+1	510	123
R4 LAN	128	+1	129	124
R1-R2 link	—	2	2	130
R3-R4 link	—	2	2	130

Subnet Allocation

1. R2 LAN (1000 hosts)

   3.12.64.0/22

   Usable: 3.12.64.1 – 3.12.67.254

   Broadcast: 3.12.67.255

2. SW LAN (509 hosts)

   3.12.68.0/23

   Usable: 3.12.68.1 – 3.12.69.254

   Broadcast: 3.12.69.255

3. R4 LAN (128 hosts)

   3.12.70.0/24

   Usable: 3.12.70.1 – 3.12.70.254

   Broadcast: 3.12.70.255

4. R_1–R_2 WAN Link

   3.12.71.0/30

   Usable: 3.12.71.1 – 3.12.71.2

   Broadcast: 3.12.71.3

5. R3 – R4 WAN Link

3.12.71.4/30

Usable: 3.12.71.5 → 3.12.71.6

Broadcast: 3.12.71.7

iii) R2 LAN got /22 → usable hosts = 1022

Required = 1000 end devices + 1 router interface = 1001

Wasted = 1022 – 1001 = 21 IPs wasted

2.

i) In a Cisco routing table, directly connected networks are identified by:

Code C = connected (directly connected network)

Code L = Local (the router's own interface IP/32)

ii) ~~Assuming the R1 IP on the R1-R2 link~~

ip route 0.0.0.0 0.00.0 192.10.11.2

iii) ip route 0.0.0.0 0.0.0.0 s1/0/1 5

iv) Brackets show:

[Administrative Distance / Metric]

S0: [40/0]

40 = Administrative Distance

0 = Metric

v) A directly attached static route specifies the exit interface, so:

* No extra lookup is needed
* Faster forwarding
* Less CPU overhead
* Works even if Next-hop lookup might fail.

Whereas a recursive route requires:

* Lookup next-hop IP
* The lookup how to reach that next hop.

3

Given: Total = 4584B, ~~Header = 42B~~.

Header = 42B → Data = 4542B

9th fragment size = 362B → Data = 362-42 = 320B (MF=1)

i) MTU (x) = 362 bytes

ii) Each full fragment Data = 320B = 40×8

offset (5th) = (5-1) × 40 = 160

∴ Fragment offset = 160

iii)

iii) Total number of fragments

4542/320 = 14 remainder 62 → 15 fragments

∴ Total fragments = 15

4

i) R3 learns PC C network via R2 → R1 → R4

∴ 2 iterations

ii) R1 detects the R1 - R4 link ~~lost~~ loss using:

* interface down event (Physical/link-layer down)

* Hello timer failure (stops receiving Hellos from R4 → neighbor dead timer expires)

5

i) Expanded (longest form) : ~~2001:0db8:12af:0001:~~

2001:0db8:12af:0001:0000:0000:0000:0003

Type: Global Unicast

Purpose: Used ~~from~~ for publicly routable IPV6 communication on the Internet.

11) Expanded (longest form):

0000:0000:0000:0000:0000:0000:0000:0000

Type: Unspecified address

Purpose: Used as a source address when a host doesn't yet know its IPV6 address

6

Some routers/firewalls block ICMP to improve security and reduce abuse (ICMP can be used for scanning or DoS)

Example: An attacker can send a large number of ICMP Echo Requests (Ping flood) to overload a server so the firewall blocks or rate-limits ICMP.

7

MTU Discovery is used to find the largest packet size that can travel end-to-end without fragmentation.

We need it because different links have different MTUs, so it prevents packet drops by ensuring packets fit the path MTU (using ICMP "Fragmentation needed / Packet too Big").

8

Broadcast ~~DHCPRE~~ DHCP request after accepting one offer because the client may receive multiple DHCP offers - broadcasting tells all DHCP servers which offer it accepted, so the others withdraws / free their offered IPs.

During renewal DHCP request is usually unicast directly to the original ~~server~~ DHCP server, because the client already has a valid IP and knows the server.

9

i) Rajib's server behind NAT/firewall, so incoming connections from the internet are blocked (no inbound mapping)

ii) Configure NAT port forwarding (static NAT/PAT) on the home router to forward the game port (eg. UDP/TCP) to the server's private IP.

10

i) Anycast addressing.
It's allowed because multiple servers share the same IPv6 address

ii) Benfits:
* Better performance: Users reach the closest DNS server → lower latency.

* High reliability: If one server / site fails, traffic automatically routed to another anycast server.

11

1) Destination MAC = MAC of R1's interface connected to S1 (part of 9 size)

How it's determined (ARP):

* Host X checks ARP table → empty
* Host X broadcasts ARP Requests.
* R1 replies with its MAC
* Host X then sends the frame with:

  Dst MAC = R1 MAC
  Dst IP = 10.0.2.2 (Host Y)

11) Switches learn MAC addresses by reading the source MAC of incoming frames and storing.

* when Host X sends first frame, S1 learns 11-11-11-11-11-11 → F1

* when traffic comes from R1 to S1, S1 learns R1's MAC on F2.

* Similarly, S2 learns

22-22-22-22-22-22 → F4 and R1's MAC on R.F3