Name: NSHIMIYUMUKIZA THIERRY
ID: 23301701

SUMMER-22 SETB

a. i) The broadcast address: 19.253.255.255

ii) prefix mask = 255.254.0.0 or /15 only 15 bits

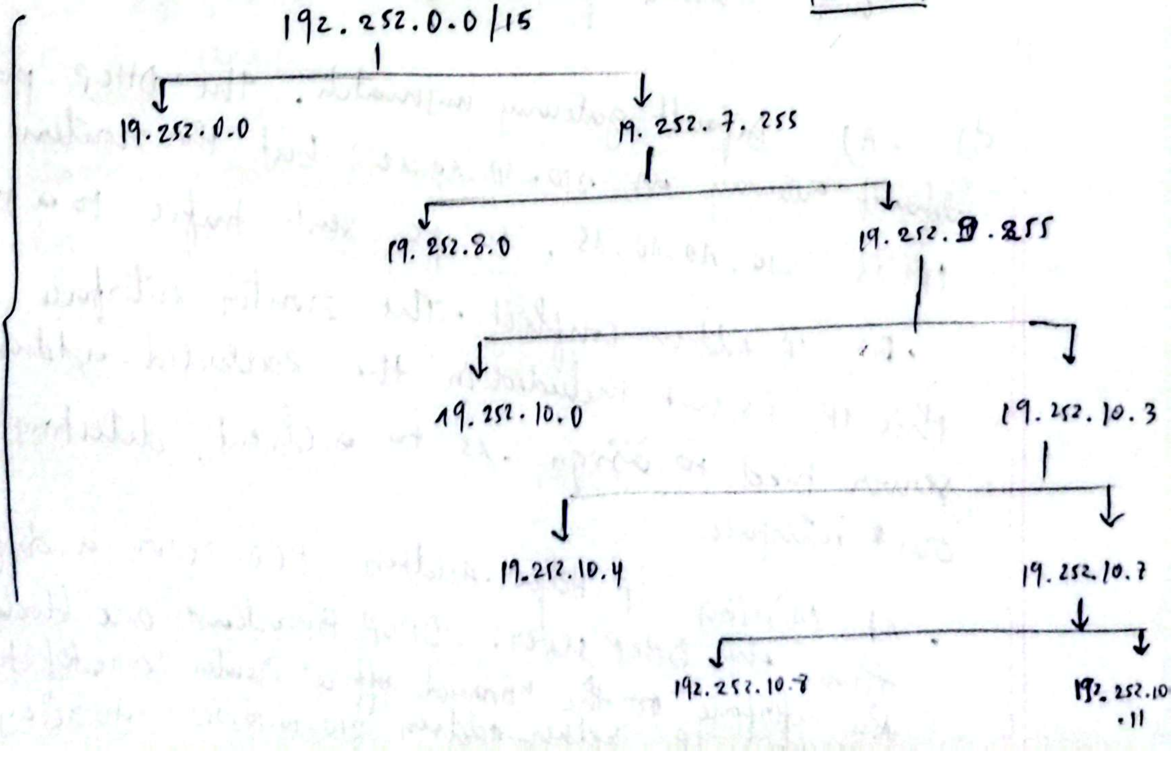
iii) The second usable ip Address is = 19.152.0.2

b) Network address = 19.152.0.0/15

Name	Host	Host +2	block size	Host bit	prefix	waste
S_one	1240	1242	2048	11	21	806
S_two	510	512	512	9	23	0
R_one	2	4	4	2	30	0
R_two	2	4	4	2	30	0 0
R_three	2	4	4	2	30	0

ε = 806

VLSM TREE



② a) Trouble shooting router ;

> The administrator can use the "traceroute" command. this maps the path packets take to a destination, displaying the ip adress and response time of each router along the way.

b) creating server problem

> it is possible to create denial of service (DOS) condition by performing an ICMP Flood or ping of death by sending ping packets of maximum size or at an extreemely high rate.

c) Gaming server access;

> this can be achieved using port forwarding known as static NAT. on the networks gateway router, map the external public IP and a specific external port to the internal private IP 192.168.10.10 and internal port 28180

d) • A) Difault gateway missmatch. the DHCP pool configure the default gateway as 210.10.10.12 but the routers actual interface ip is 210.10.10.15, so pcs sends trafic to a non-existent gateway

• B) IP Address conflict. The router interface is 210.10.10.15 this IP is not Included in the excluded-address range. the DHCP server tried to assign .15 to a client, detecting a conflict with its own interface

• c) Missing ip Helper.Address. PC0 is on a different network (192.10.10.0/24) than the DHCP sever. DHCP Broadcast are blocked by routers. the interface on the "Branch office" router connected to switch1 must be configured with ip helper-address 210.10.10.15 -to relay requests.

3) a) Shortest path and ~~Route~~ cost

- Node b : Cost 3 (path : a → c → b)
- Node c : cost 2 (path : a → c)
- Node d : cost 8 (path : a → c → b → d)
- Node e : cost 10 (path : a → c → b → d → e)
- Node z : Cost 14 (path : a → c → b → d → z)

b) Link state Nighbors

> Nodes keep track of their neighborrs by periodically send and receiving Hello packets. If a router stops receiving hellow packets from a neighbor for a specific interval, It declares the neighbor down and updates the link-state database

c) Distance vector issues

(i) periodic updates are bad for the respnce because they consume significant bandwidth and CPU even when the netwrk is stable.

(ii) > Slower convergence : Changes take a long time to propagate
> Routing loops : prone to loops during convergence times.

4) a) i) significance: 0.0.0.0. 0.0.0.0 represents a default route it maches any destination ip addren that is not explicitely found in the routing table; sending trafic out S0/0/0.

ii) why the second command: it establishes a floating state route the 30 at the end is the Administrative Distance (AD). since Default AD for static rout is 1, the rout (AD 30) will only be installed in the routing table.

b) Route summarisation problem

> The problem is Discontinous subnets leading to innacurate summarization. router A owns networks '.16' and '.64' Router C owns .32 and .48 and .80. these subnets are interleaved within the 192.168.25.x range. you cannot create a single summary route on router B for A without including subnets that belongs to router C. this causes Traffific blackholing, where data meant for C is wrong routed to A.

c) i) Commands;

on R1: ip route 167.18.10.0. 255.255.255.240 S2/0/0

on R2: ip route 167.18.10.0 255.255.255.240 S2/0

ii) floating route: we can increase administrative distance such as

> ip route 167.18.10.0. 255.255.255.240. S1/0 50

5) a) IPV4 / IPVC

> Yes, there is a problem. IPV4 and IPV6 are incompatible protocols they can not communicate directly.

solution: we need to implement dualstack topology. this involves Configuring both IPV4 and IPV6 protocol stacks on all network devices. allowing them to process both type of traffic simultaneously

b) IPVC shortening

Full : FF10 : 00FF : 0000 : 0000 : AC19 : 0000 : 0000 : E600

Shortened : FF10 : FF :: AC19 : 0 : 0 : E000

e) MAC : F0-B2-F0-EA-DF-35

1. Insert FFFE in the middle : F0B2 : F0FF : FEEA : DF35
2. flipping 9th bit of first byte (F0 → F2
3. interface ID : F2B2 : F0FF : FEEA : DF35
4. Link local prefix : FE80::

Therefore Address : FE80 :: F2B2 : F0FF : FEEA : DF35

d) (i) false, IPV6 requires ICMPV6 router Advertisments (RA) to provide the default Gateway information. DHCPV6 does not apply default Gateway option: It supplies Ip addresses and other parameters

ii) purpose of DAD: Duplicate Address detection (DAD) ensures that an IPV6 address is unique on the link before it is assigned to an interface preventing Ip conflicts.

6) a) ARP & PING

i) , ARP in differend netwrk: when the destination is remote, the ~~most~~ host sends an ARP Request for the Default gateway's MAC address not the destination host's MAC. the packet is then framed to the router.

ii) MAC addresses;

, ARP Frames: Source: MAC—HostA, Destination: FF:FF:FF:FF:FF:FF

, ping Frame : Source: MAC_HOSTA, Destinatn: MAC_Defaulgateway

b)

i) handling: the switch will broadcast (flood) the frame on all ports exlept ingress port

ii) S3 MAC Table

MAC Addres	port	TTL
Hos·A MAC	F0/0	60

c) i) Type: unicast because the first byte is E0 and in bynary it is (1110 0000) - the least significant bit is 0 indicating a unicast.

ii) portable: it means the MAC address is hard coded onto network interfale card (NIC) - if you physically move NIC to a differend netwrk, the mode address remains the same while an IP address.