Date :.....

CSE-421

Assignment : 02

Afia Jannat Saima

Id: 23101286

Section : 23

(Spring 24 : SET B)

Date :.....

Q(1) Ans:

(i) Given, Network = 1.2.128.0/17

A/17 network has 15 has bits

Number of subnets = 2^n

Maximum possible subnets = 2^{15} = 32,768 subnets.

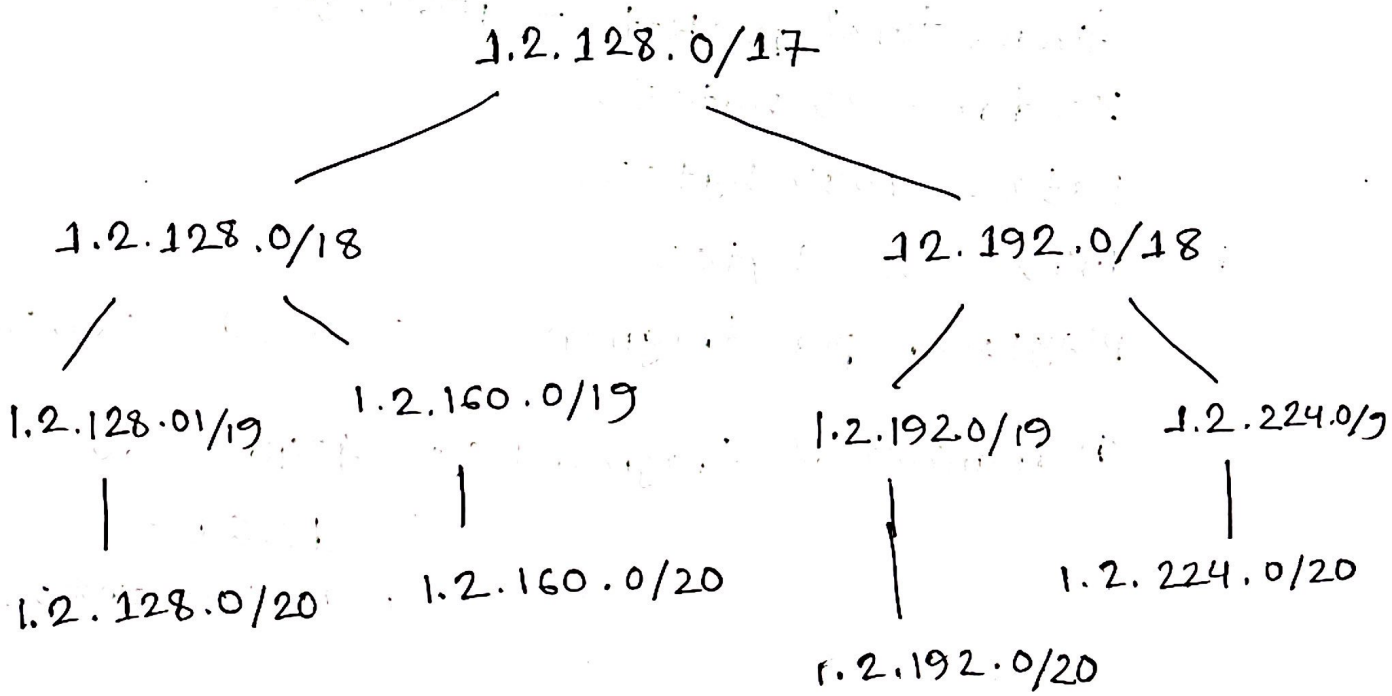
(ii) Network range: 1.2.128.0 – 1.2.255.255

each subnets increase based on borrowed bits

hierarchical split: /18 → 1.2.128.0/18, 1.2.192.0/1

/19 → four subnets. continue recursively.

Tree is drawn by binary division from MSB to LSB.



Date :

Q(2) Ans:

(i) R3 LANS share common prefix.

Binary comparison = common bits retained

Summarized network = smallest supernet covering all LANS.

Static summary route on R1:

R1(config)* ip route <summarized-network> <mask> <next-hop>

(ii) Floating static route (AD=50):

R1 (config)* ip route <LAN2-network> <mask> <exit-interface-to-R2> 50.

Q(3) Ans:

Given, total packet = 4560 bytes.

Header = 20 bytes.

Data = 4540 bytes.

MTU = 380 bytes.

playload per fragment = 380 - 20 = 360 byte.

(i) Number of fragments: 4540 ÷ 360

= 12.61.

≈ 13 fragments.

Date :

(ii) Fragment offset of 4th fragment : $(3 \times 360) \div 8$

$= 1080 \div 8$

$= 135$

(iii) MF bit of 5th fragment = 1.

Q(4) (Ans):

DHCP uses broadcast. Routers do not forward boadcast. for solving the problems we have to configure DHCP relay agent on router.

interface <LAN - interface>.

ip helper-address <DHCP-server-IP>

Q(5) Ans:

False. NAT/PAT allows multiple internal devices to share one public IP.

Q(6) Ans:

Yes, R2 sends routing updates out all interfaces expect the one it learn from the route.

for prevent loops uses split harizon rule.

Date :.....

Q(7) Ans:

(i) MAC = 98:0B:98:00:00

(ii) IPv6 address type - FE80:: → Link-local address.

Q(8) Ans:

PC4 ⟶ PC3

Known MAC ⟶ Unicast forwarding

PC4 ⟶ PC2

Unknown MAC ⟶ flooding

Updated MAC table:

S3 learns PC4 MAC

S2 remains unchanged

Date :.....

Q(9) (Aws):

A website can be prevented from responding to HTTP request by using an ICMP flood. In this attack, an attacker sends a very large number of ICMP PING packets to target server continuously. The server attempts to reply to each request which consumes its processing power, memory and network bandwidth. As a result the server becomes overloaded and cannot handle traffic such as HTTP requests from real users. this causes the website to become slow or completely unavailable.

Q(10) Aws:

when PC1 sends an ARP request to discover the MAC address of PC5 the request is sent as a broadcast frame because PC1 doesnot know the destination MAC address. S1 receives the broadcast and forwards it through all ports expeets the incoming port. the request then reaches S2, which again floods the frame to all connected ports expected the source

Date :.....

port. Similarly, S3 forwards the ARP request to all its ports allowing PC5 to receive it. After receving the ARP request PC5 sends an ARP reply as a unicast frame back to PC1. PC1 receive the reply, it stores PC5's IP to MAC address mapping in its ARP cache and then starts sending data frames directly to PC5 using the learned MAC address.

Q(11) Ans:

IPv6 packets are encapsulated invid IPv4 Packets because many networks in the internet still don't support IPv6. when an IPv6 packet needs to travel through IPv4 only network, it can't be forwarded directly. To solve this problem, the IPv6 packet is encapsulated within an IPv4 packet so that it can pass through the IPv4 infrastructure without modification. This process aollows communication between IPv6 network over IPv4 which called tunneling.

Date :.....

Q(12) Ans:

(i) Unicast

(ii) A MAC address is considered a flat address because it doesnot contain any hierarchical or location based information. It is assigned by manufacturer and remains fixed regardless of the network where the device is connected. Unlike an IPv4 address, a MAC address does not provide any information about the network or subnet and cannot be used for routing decisions.

Q(13) Ans:

In a distance vector routing protocol, routers handle topology changes by updating their routing tables and sending triggered updates to neighboring routers. the neighbors then propagate the updated information further in the network. To reduce problems such as routing loops and the count to infinity issue, techniques like split horizon, route poisioning and poison reverse are used.