Paper Source
Subject
Date : Time:

Ans: to the Qus: No: 01

1. Given that,

Network = 1.2.128.0/17

A/17 network has 15 hos bits

Number of subnets = 2^n

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

11. Network range : 1.2.128.0 – 1.2.255.255

Each subnet increases based on borrowed bits.

Example hierarchical split:

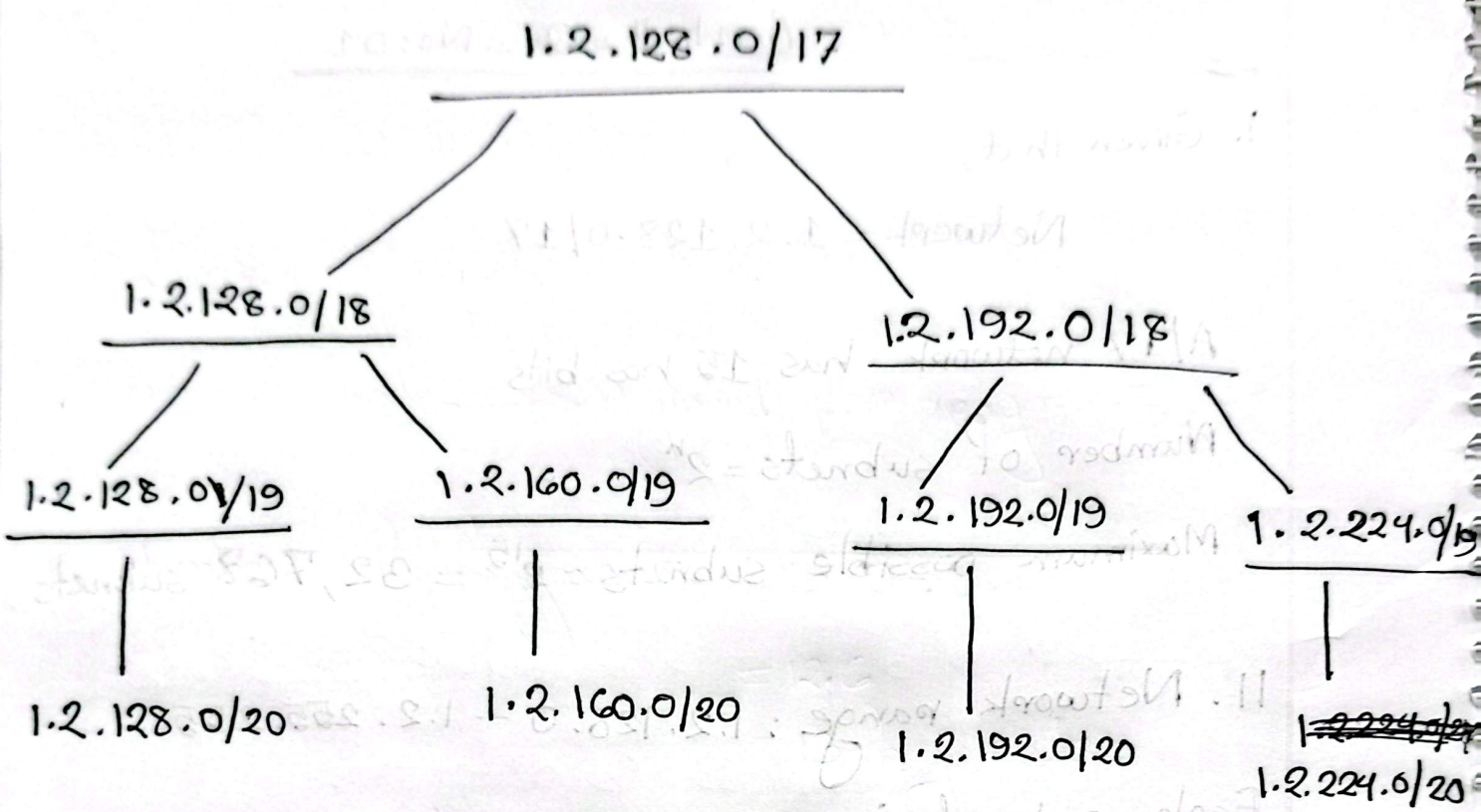
/18 → 1.2.128.0/18 , 1.2.192.0/18

/19 → four subnets

Continue recursively

Tree is drawn by binary division of network bits from MSB to LSB.

Paper Source
Subject
Date : Time:



Paper Source
Subject.....
Date :.....Time:.....

Ans: to the Qus: No: 02

1. 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-R3> 50.

Paper Source
Subject
Date : Time:

Ans: to the Qus: No: 03

Original packet = 4560 bytes

Header = 20 bytes → Data = 4540 bytes.

MTU = 380 bytes → Payload per fragment = 360 bytes.

i. Number of fragments = 4540 ÷ 360
= 12.6
= 13 fragments.

ii. Fragment offset of 4th fragment = (3 × 360) ÷ 8
= 135.

iii. MF bit of 5th fragment = 1.

Paper Source
Subject
Date : Time:

Ans: to the Qus: No: 04

DHCP uses broadcast. Routers do not forward broadcasts. To solve this problems we have to configure DHCP relay Agent on router:-

interface <LAN-interface>

ip helper-address <DHCP-server-IP>

Ans: to the Qus: No: 05

False. Using PAT, multiple devices can share one public IP. Differentiation done using port numbers

Ans: to the Qus: No: 06

Yes,

AR2 sends routing updates out all interfaces except the one it learned the route from. Uses split horizon rule. Prevents routing loops.

Paper Source
Subject
Date : Time:

Ans: to the Qus: No: 07

I. MAC = 98:0B:98:00:00

II. IPv6 address is link-local type address. Which is starts with FE80::/10.

Ans: to the Qus: No: 08

PC4 → PC3

* Known MAC → Unicast forwarding

PC4 → PC2

* Unknown MAC → Flooding.

Updated MAC Tables:—

S3 learns PC4 MAC

S2 remains unchanged.

Paper Source
Subject
Date : Time:

Ans: to the Qus: No: 09

ICMP Smurf attack. In an ICMP Smurf attack, the attacker sends a large number of ICMP Echo Request packets to a network broadcast address while spoofing the victim website's IP address as the source. All hosts in that network reply with ICMP Echo Replies to the victim simultaneously, overwhelming it with traffic. As a result, the website becomes overloaded and cannot respond to legitimate HTTP requests.

Ans: to the Qus: No: 10

PC1 sends an ARP request, which is a broadcast frame. Switch S1 floods the ARP request out of all ports except the incoming port. Switch S2 receives the broadcast and floods it to all its ports, including the link toward S3. Switch S3 also floods the ARP request

Paper Source
Subject
Date : Time

to all connected ports, allowing PC5 to receive it. After receiving the ARP reply, PC1 performs updates its ARP cache by storing the IP-MAC address mapping of PC5. Encapsulates and sends the actual data frame to PC5 using the learned MAC address.

Ans: to the Qus: NO: 11

IPv6 packets are encapsulated inside IPv4 packets to allow communication between IPv6 networks over IPv4 only infrastructure, since IPv4 routers cannot understand IPv6 packets. This encapsulation and decapsulation mechanism is called tunneling.

Paper Source
Subject.....
Date :.....Time:.....

Ans: to the Que: No: 12

i. Unicast.

ii. A MAC address is a flat address because, it does not contain ~~to~~ any location or network information. It is assigned by the manufacturer. It does not change when a device moves to another network. Switches must learn MAC ~~addressing~~ addresses dynamically, not calculate paths using address structure. IPv4 addresses are hierarchical. Because they consist of network portion and host portion. Routers use this hierarchy to make routing decisions, perform route summarization and scale efficiently.

Paper Source
Subject.....
Date :.....Time:.....

Ans to the Qus1 No:13

Distance Vector protocol handles any changes in the topology when routers send periodic updates. Uses triggered updates. May cause count-to-infinity. Mitigations like split horizon, poison reverse and hold-down timers.