Name: Ifte Khairul Hakim

Id: 2161319

sec: 22

Course: CSE 421

Assignment 02.

Fall 2024 set B

Answer to the question no.1

i) Given,

host address 32.99.125.255/17

Prefix = /17

Host bit = 32 - 17 = 15

∴ Total usable host : $2^{15} - 2$

= 32766 host

ii) /17 Subnet mask = 255.255.128.0

Network boundary in the 3rd octet 0 - 127

∴ Network address 32.99.0.0/17

∴ Broadcast address 32.99.127.255

iii) Given,

LANA = 2000 Hosts

LANB = 10254 Host

LANC = 3 Host

WAN = 2 Links

Subnet size calculation

Network	Host needed	Subnet	Usable host
LAN A	2000	/21	2046
LAN B	1024	/21	2046
LAN C	3	/29	6
WAN 1	2	/30	2
WA 2	2	/30	2

VLSM address allocation

Subnet	Network address	Prefix
LAN A	32.99.0.0	/21
LAN B	32.99.8.0	/21
LAN C	32.99.16.0	/29
WAN1	32.99.16.8	/30
WAN2	32.99.16.12	/30

Answer to the question no.2

i) To allow external users to initiate a connection to the internal FTP server using the public IP and Port 21, the NAT feature that must be configured is static NAT with port Forwarding.

Public 203.0.113.10.21 → Private 10.0.0.50.21

This permanent mapping allows incoming FTP request from the Internet to reach the internal server. Without port forwarding NAT would block unsolicited inbound connection.

ii) The network is using PAT (post address Translation) because the business has only one public IP address. Multiple internal hosts access the internet at the same time. PAT allows many private IP address to share single public IP by differentiating sessions using port numbers.

Answer to the question no.3

Given,

IHL = 6 → header length = 6 × 4 = 24 bytes

Total length = 6421 bytes

maximum data size per fragment = 1624 bytes

DF = 0

MF = 0 , offset = 0

protocol = 17

Original data size = Total length - Header length

= 6421 - 24

= 6397 bytes

i) Number of fragment created $\frac{6397}{1624}$

$= 3.94$

$= 4$

ii) Data size of last fragment

$= (6397 - (3 \times 1624))$

$= 4872$ bytes

iii) Fragment offset is measured in units of 8 bytes.

∴ fragment offset of the last fragment

$\frac{4872}{8}$

$= 609$

iv) At the destination, the receiving host performs reassembly as follow:

1. ~~identification field~~ All fragments carry the same identification value (5656). So the destination groups fragments with the same.
2. The fragment offset tells where each fragment data belongs within the original payload.
3. The MF flag is 1 for all but the last fragment, and 0 is the last fragment, MF=0 tells the receivers that this the final chunk.
4. The destination buffers incoming fragment, placing their data according to the offset.
5. if not all fragments arrive within a timeout the partially resembled packet is discarded.

v) The MF flag in the IPV4 header indicates whether more fragments follow this one.

* MF=1, This fragment is not the last, there are additional fragment of the same original packet still to come.

* MF=0, This is the last fragment of that datagram. Combined with the fragment offset. It lets the receivers know where the original packet ends and when reassembly is complete.

Answer to the question no.4

i) Directly attached default static route on R2 (AD10)

On R2, the interface S2 is in network 192.168.11.224/30.

A directly attached default route only the exit interface

ip route 0.0.0.0 0.0.0.0 S2 10

ii) Backup default static route in R2 using next-hop IP address

ip route 0.0.0.0 0.0.0.0 192.168.11.266.20

Answer to the question no.5

R_1 R_2, ISP Link state router convenge fastens because they maintain full topology and use SPF algorithm. R_1 R_2 and R_3 will keep track of ~~Neighbor trac~~ their neighbor ~~with Distance vector~~ by ~~pred~~ periodic routing table exchange. and Hello packets and LSDB.

Answer to the question no.6

i) 2001:db8:85a3:8a2e:370:7334

ii) 2607::805:0:0:0:200e

iii) 3-ffe:1900:4545:1003:1200:a0f8:fe21:670f

Answer to the question no. 7

i) ARP request MAC addresses

* Source MAC : PCA
* Destination MAC: FF:FF:FF:FF:FF:FF

ii) Router action

Router R1 drops the ARP request because ARP is a broadcast ~~not~~ and not forwanded.

iii) After receiveing the ARP reply the first action would be PC A updates its ARP table and sends the data packet.

Answer to the question no. 8

Loss of end to end traceability may occur due to.

1. NAT/ PAT usage
2. Shared IP addresses.

3. VPN tunneling

4. Proxy servers

5. Dynamic IP assignments

6. Lack of proper logging

Answer to the question no 9

i) The steps involved in the IP address renewal process with DHCP is

~~1. DHCP REQ~~

1. DHCPREQUEST

2. DHCPACK

ii) The potential reason a device might fail to renew its IP address are

1. DHCP server unreachable

2. Lease expired.

3. Network issues

4. IP conflict.

The action the device take if it cannot renew the IP address is assigns an APIPA address (169.254.xxx)

Answer to the question no 10

The function of the loopback address in network communication is used to test TCP/IP stack and local communicatio

Loop back addresses

* IPV4 : 127.0.0.1
* IPV6 :: 1

Answer to the question no.11

i) State the actions that the switch S2 will take after it receives the packet is checks MAC table. and forward frame to correct port.

ii) They learn MAC addresses by observing source MACs of incoming frames.