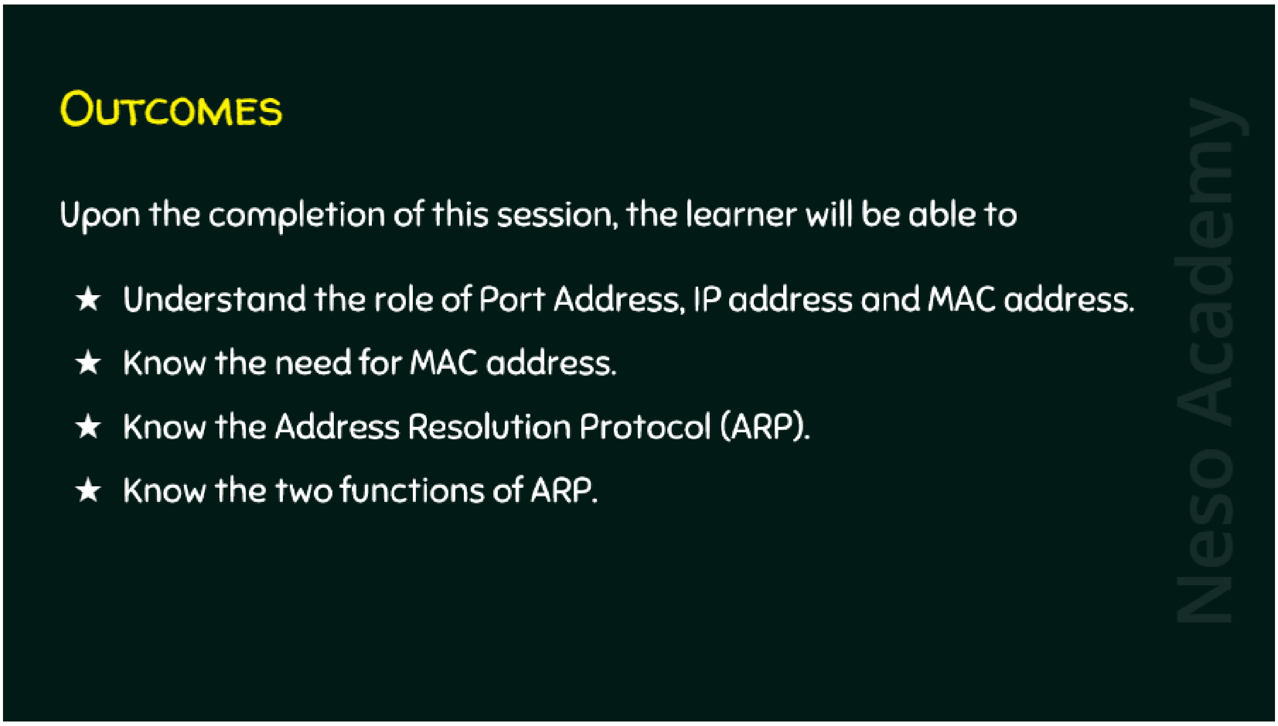
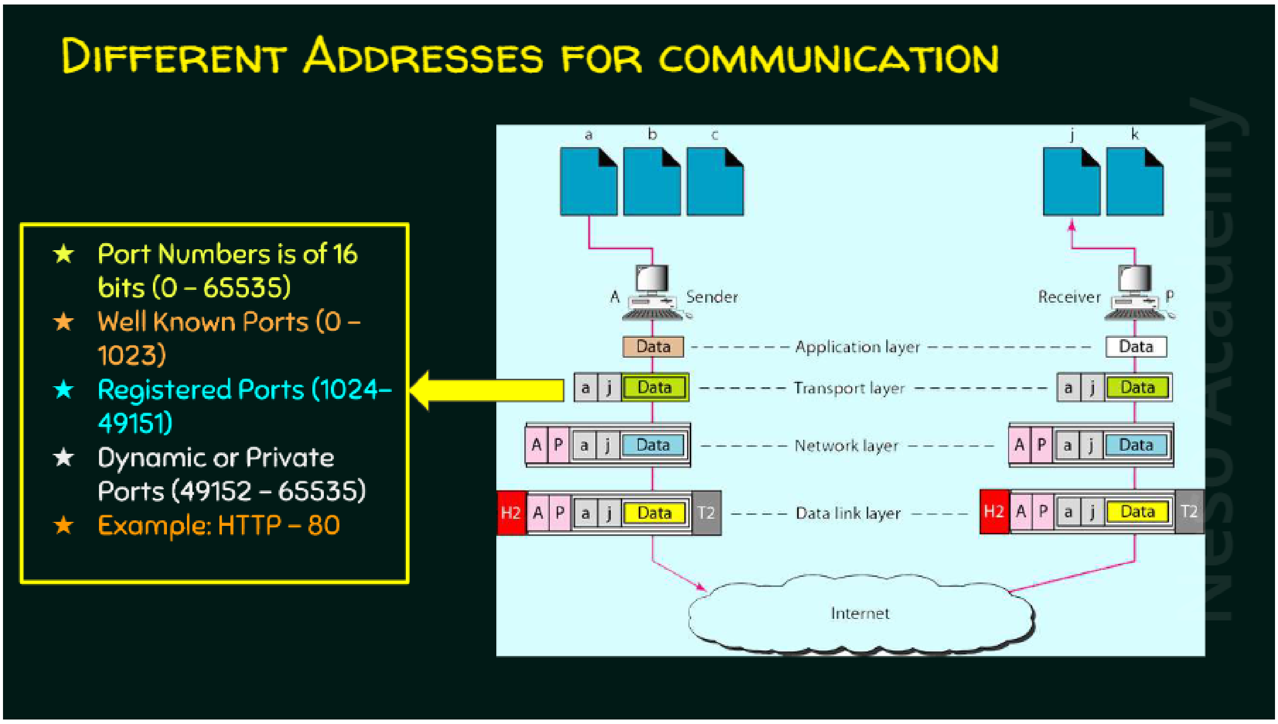
Network Layer Protocols | Neso Academy

nesoacademy.org/cs/06-computer-networks/ppts/04-networklayerprotocols

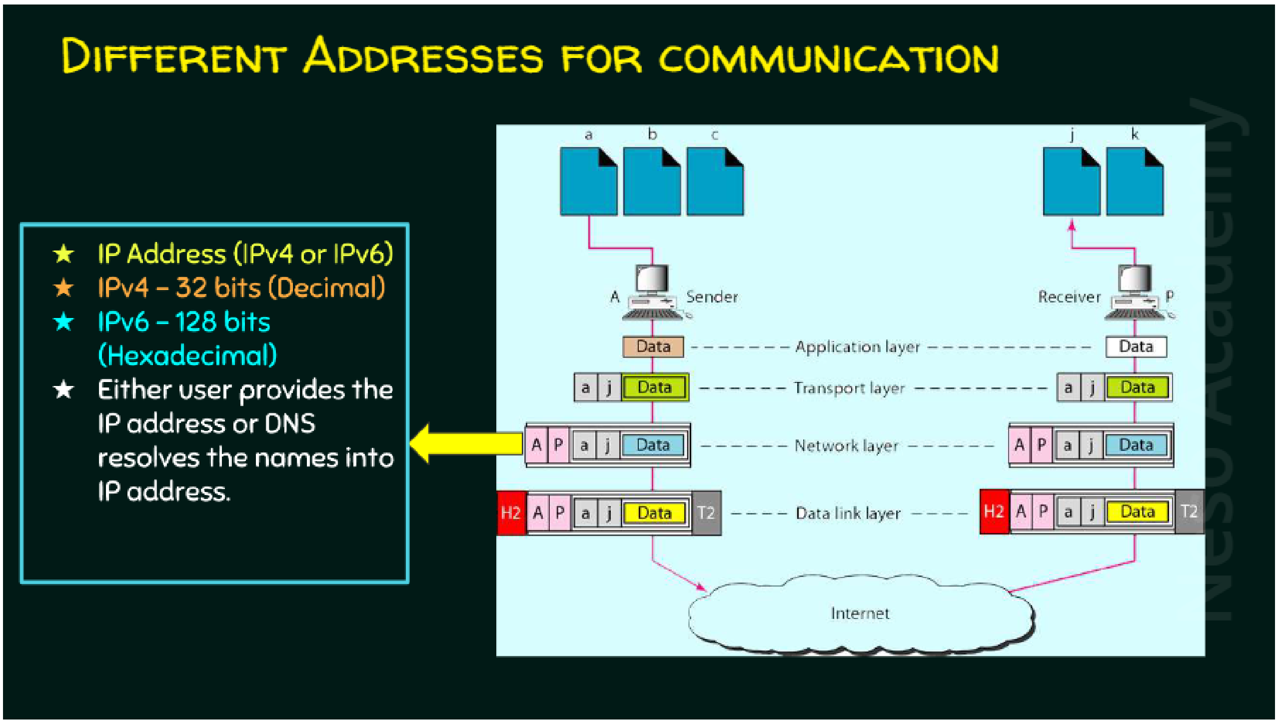
Network LayerProtocolsNeso AcademyCHAPTER - 4



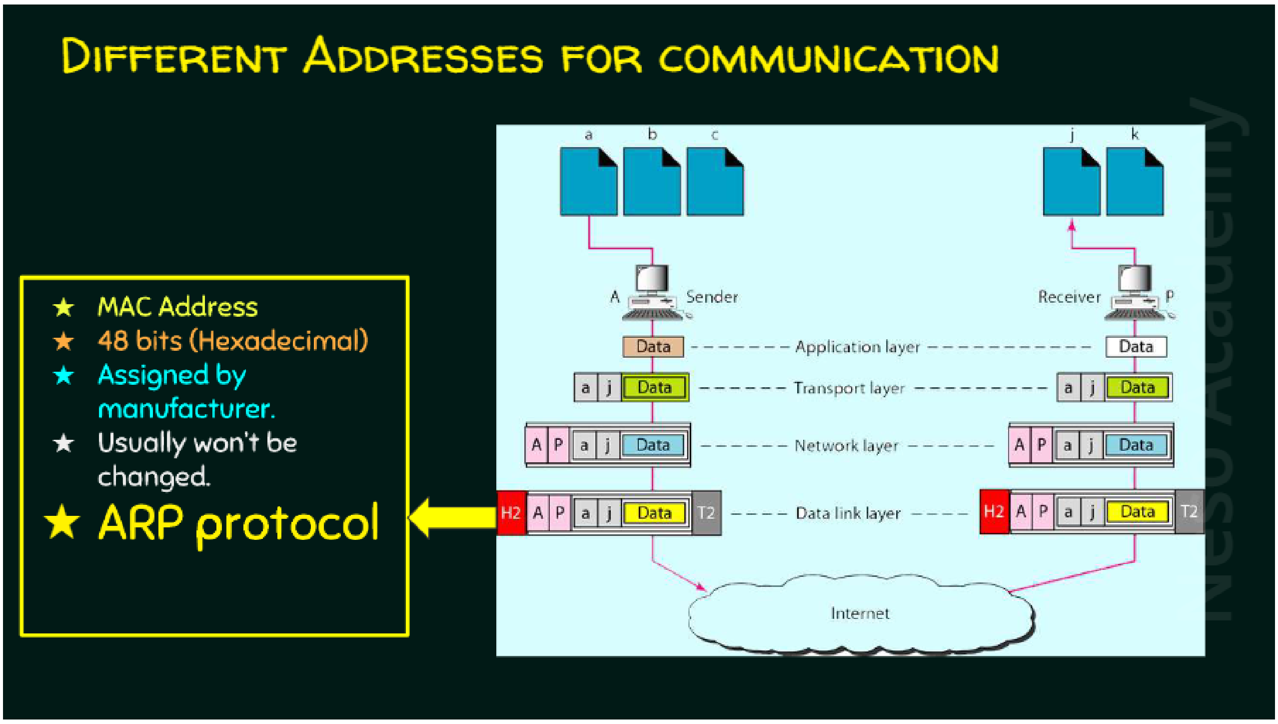
Outcomes★★★★Neso Academy



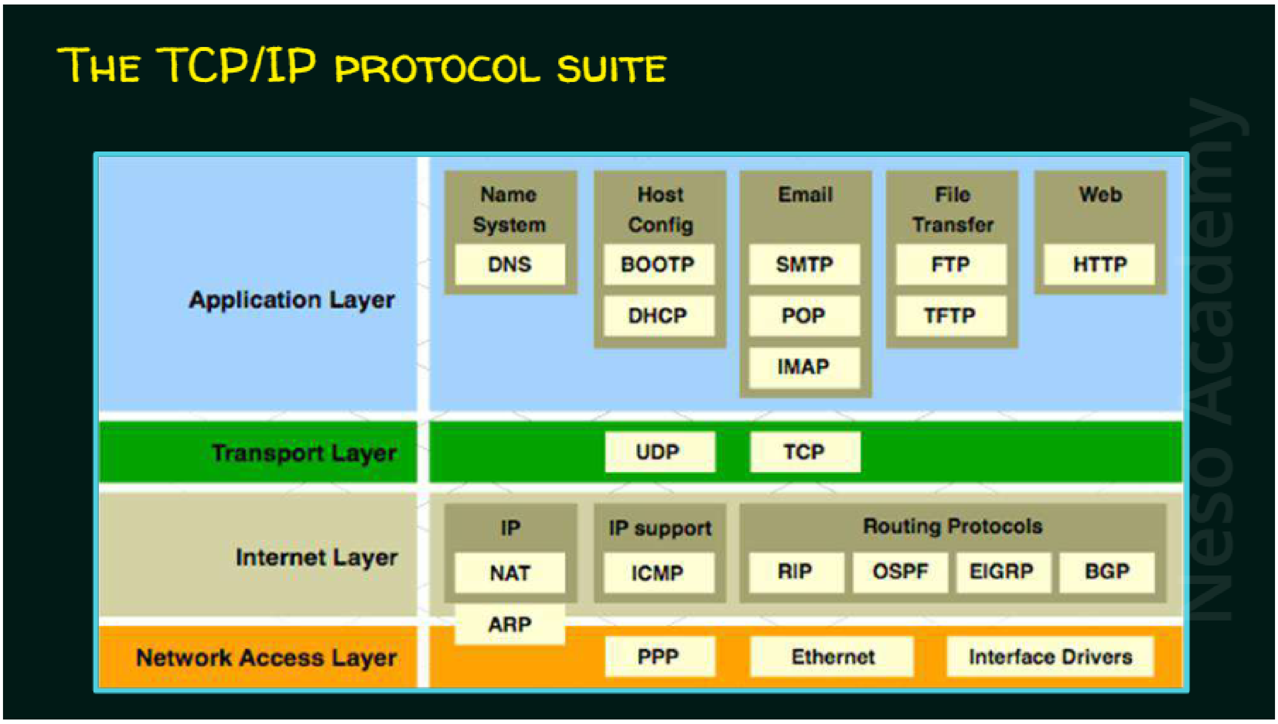
Different Addresses for communication★★★★★Neso Academy



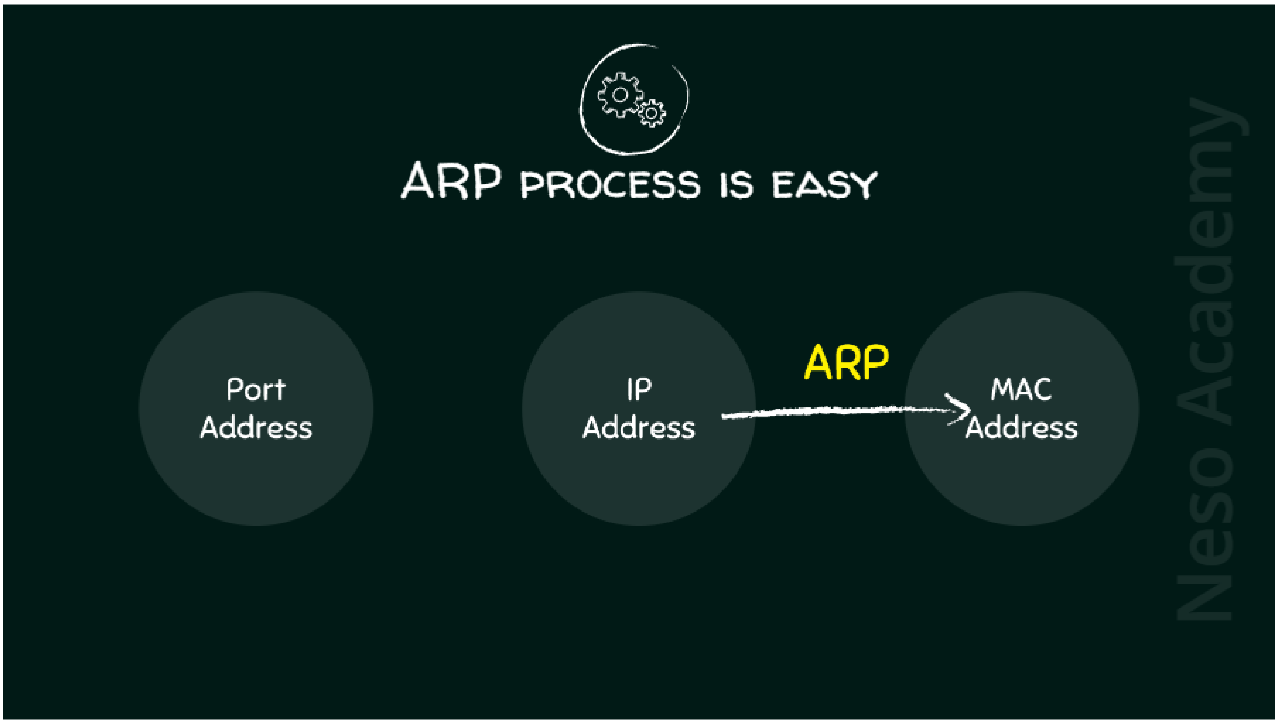
Different Addresses for communication★★★★Neso Academy



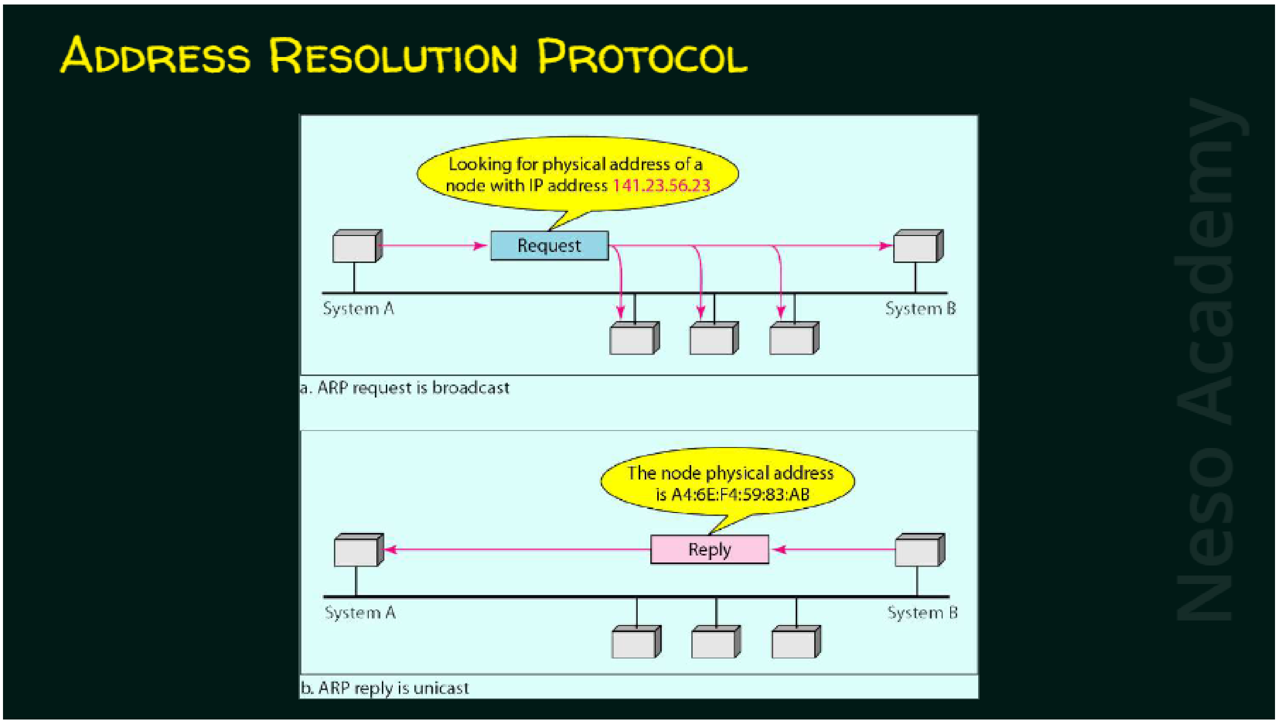
★★★★★Different Addresses for communicationNeso Academy



The TCP/IP protocol suiteNeso Academy



ARP process is easyNeso Academy



Address Resolution ProtocolNeso Academy

Address Resolution Protocol

The ARP protocol provides two basic functions:

1. Resolving IPv4 addresses to MAC addresses.
2. Maintaining a table of mappings.

Address Resolution ProtocolNeso Academy

Homework

The address resolution protocol (ARP) is used for

[GATE CS 2005]

(A) Finding the IP address from the DNS.

(B) Finding the IP address of the default gateway.

(C) Finding the IP address that corresponds to a MAC address.

(D) Finding the MAC address that corresponds to an IP address.

HomeworkNeso Academy

Outcomes

Upon the completion of this session, the learner will be able to

★ Understand the working of ARP.

Outcomes★Neso Academy

Address Resolution Protocol

★ ARP: Map IP addresses into physical addresses.

★ Table of IP to physical address bindings.

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.29.173 --- 0x14
  Internet Address      Physical Address      Type
  192.168.29.1          78-dd-12-b5-ad-bc     dynamic
  192.168.29.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
```

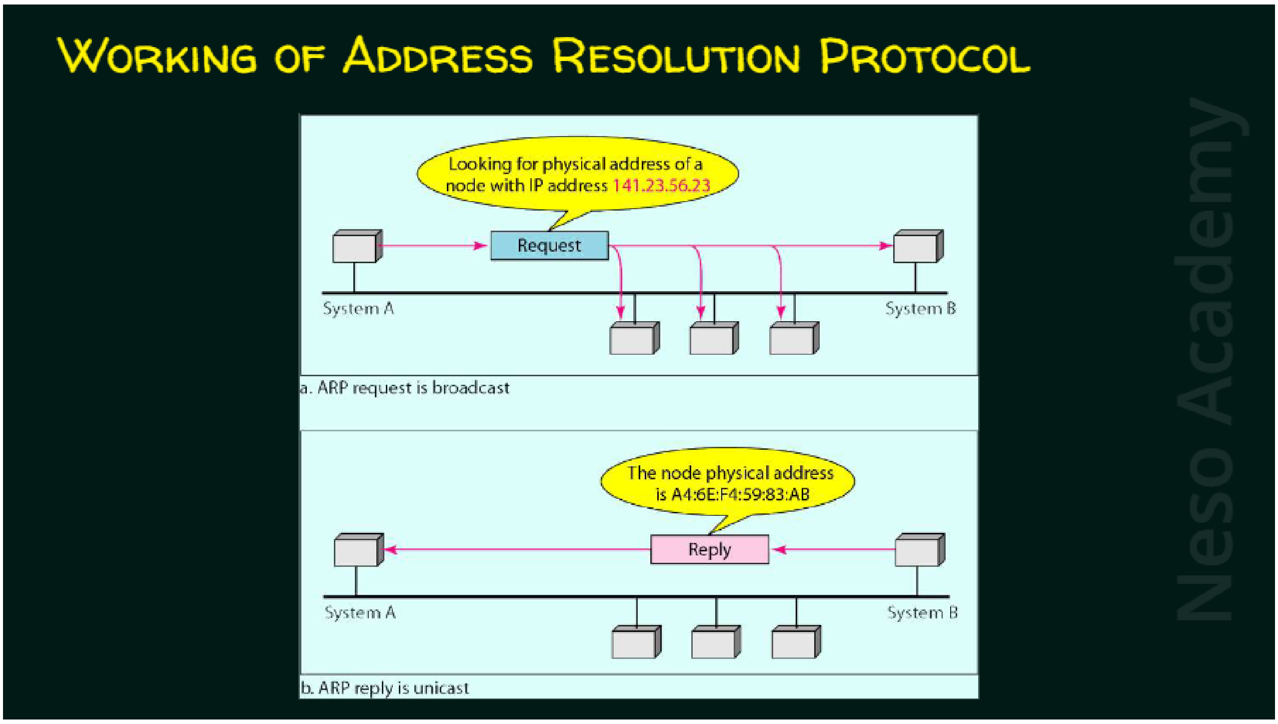
★ Broadcast request if IP address not in table.

★ The broadcast address: MAC address.

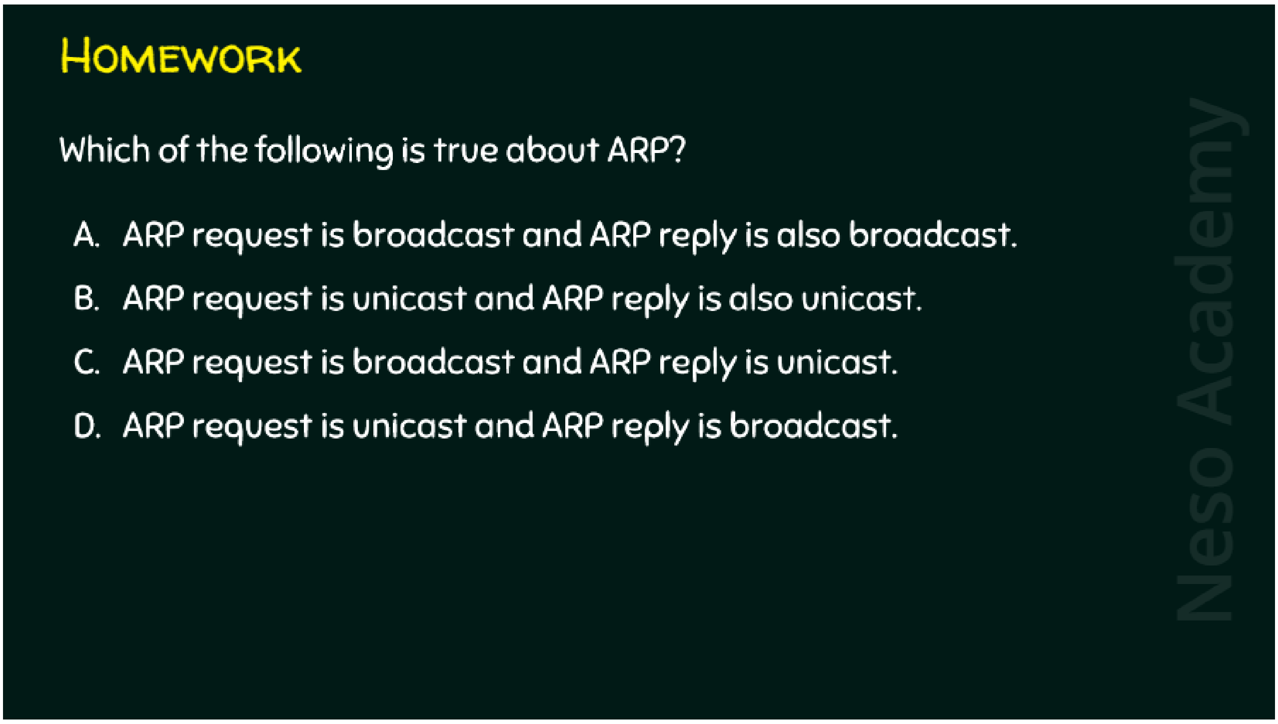
★ Target machine responds (unicast) with its physical address.

★ Table entries are discarded if not refreshed.

Address Resolution Protocol★★★★★★Neso Academy



Working of Address Resolution ProtocolNeso Academy



HomeworkNeso Academy

QUESTION

Suppose that in an IP-over-Ethernet network, a machine X wishes to find the MAC address of another machine Y in its subnet. Which one of the following techniques can be used for this?

[GATE CS 2019]

(A) X sends an ARP request packet with broadcast IP address in its local subnet

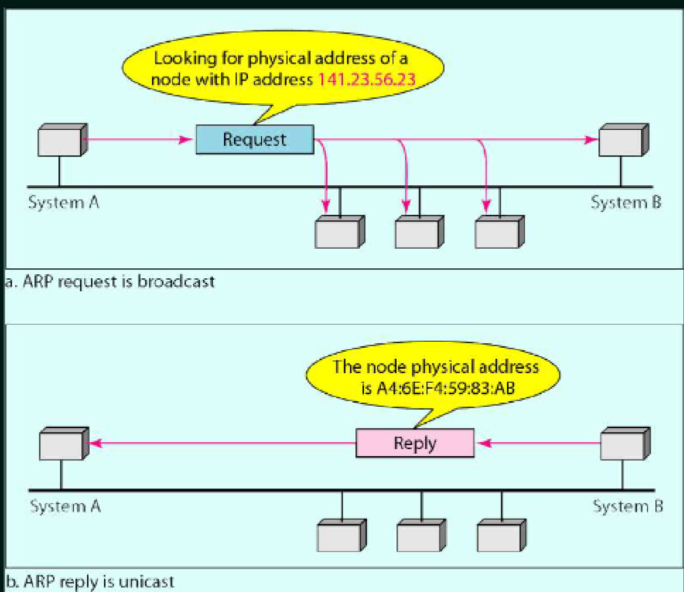
(B) X sends an ARP request packet to the local gateway's MAC address which then finds the MAC address of Y and sends to X

(C) X sends an ARP request packet with broadcast MAC address in its local subnet

(D) X sends an ARP request packet to the local gateway's IP address which then finds the MAC address of Y and sends to X

QuestionNeso Academy

ADDRESS RESOLUTION PROTOCOL



Address Resolution ProtocolNeso Academy

Question

Suppose that in an IP-over-Ethernet network, a machine X wishes to find the MAC address of another machine Y in its subnet. Which one of the following techniques can be used for this?

[GATE CS 2019]

(A) X sends an ARP request packet with broadcast IP address in its local subnet

(B) X sends an ARP request packet to the local gateway's MAC address which then finds the MAC address of Y and sends to X

(C) X sends an ARP request packet with broadcast MAC address in its local subnet ✔

(D) X sends an ARP request packet to the local gateway's IP address which then finds the MAC address of Y and sends to X

Question✓Neso Academy

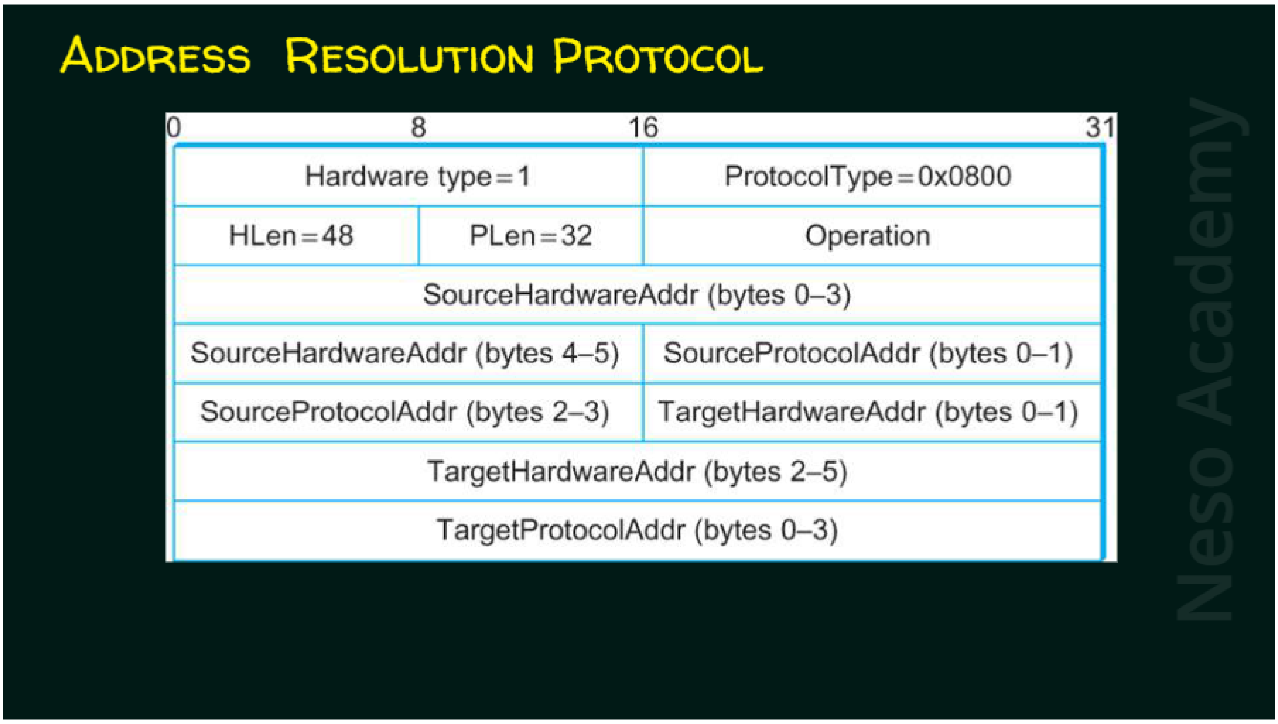
Outcomes

Upon the completion of this session, the learner will be able to

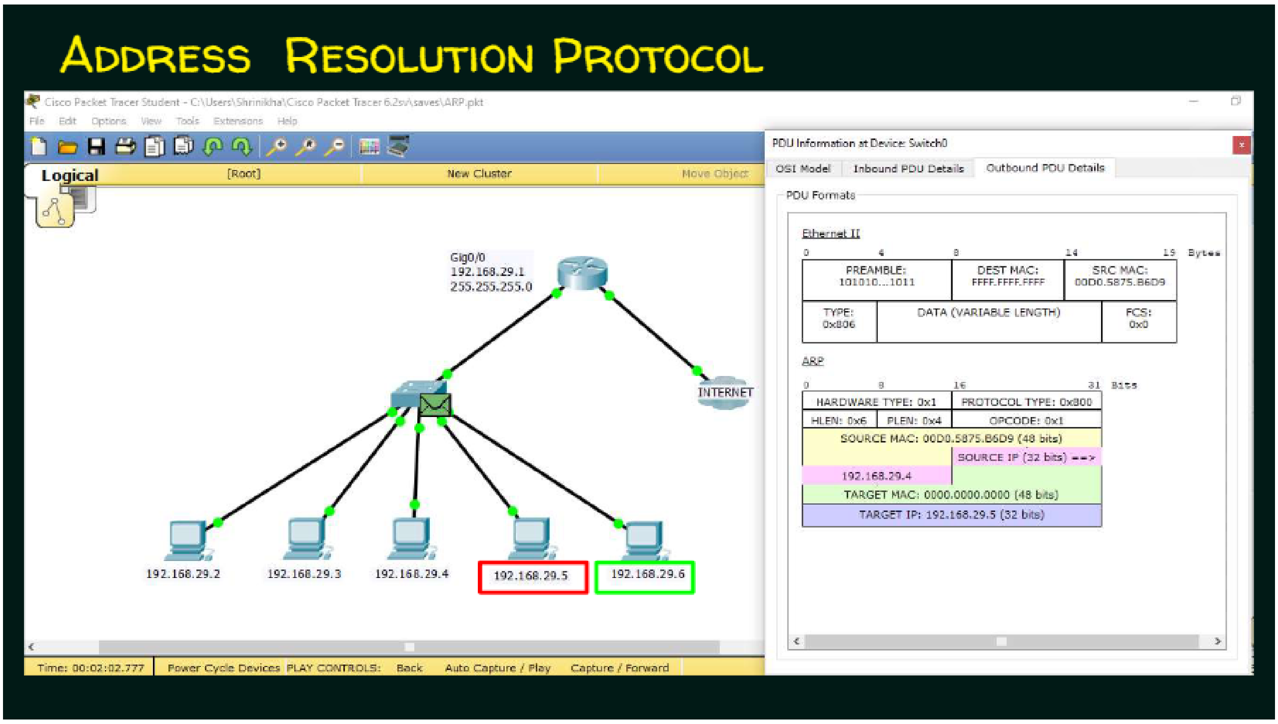
★ Know the ARP Header Format and its various fields.

★ See the ARP Header and other headers in Cisco Packet Tracer.

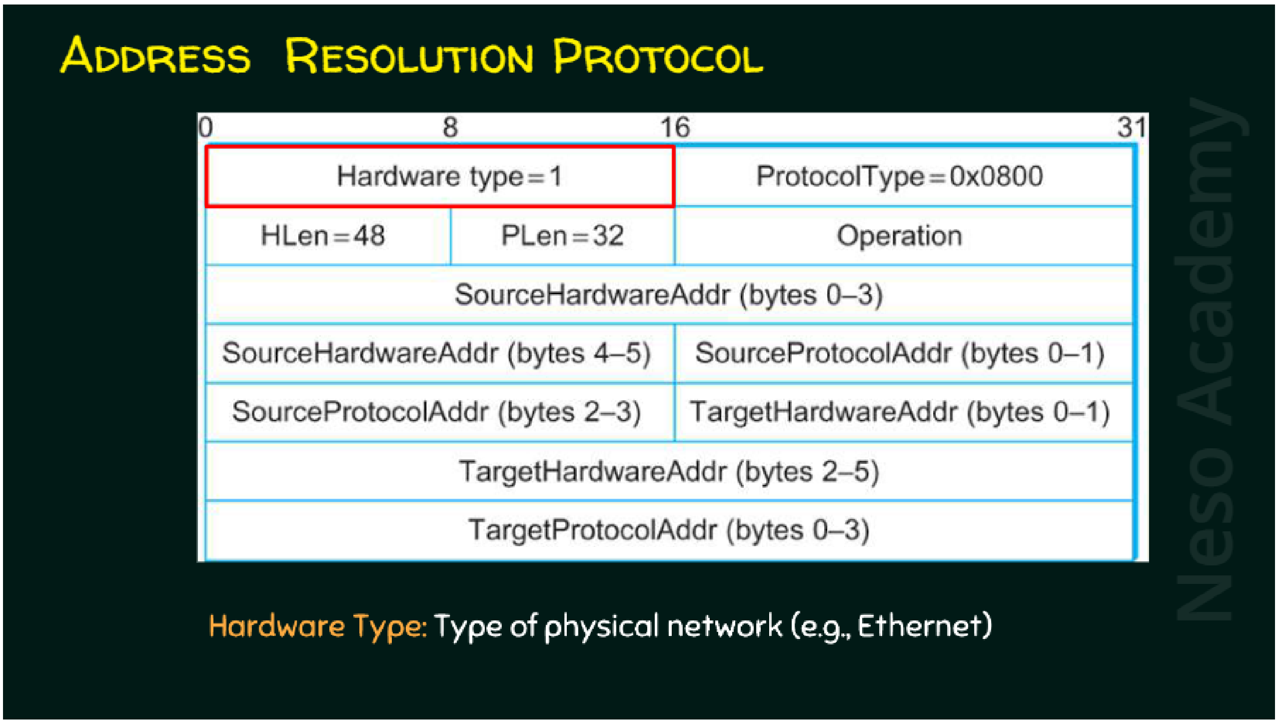
Outcomes★★Neso Academy



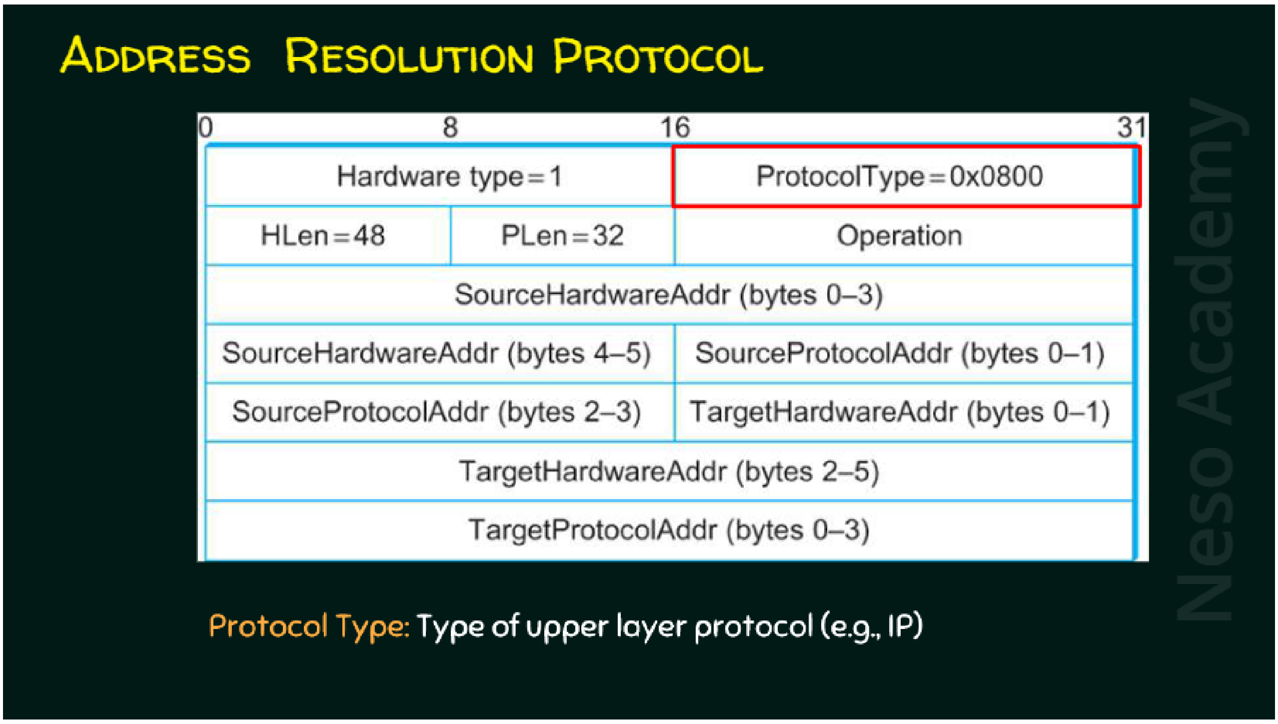
Address Resolution ProtocolNeso Academy



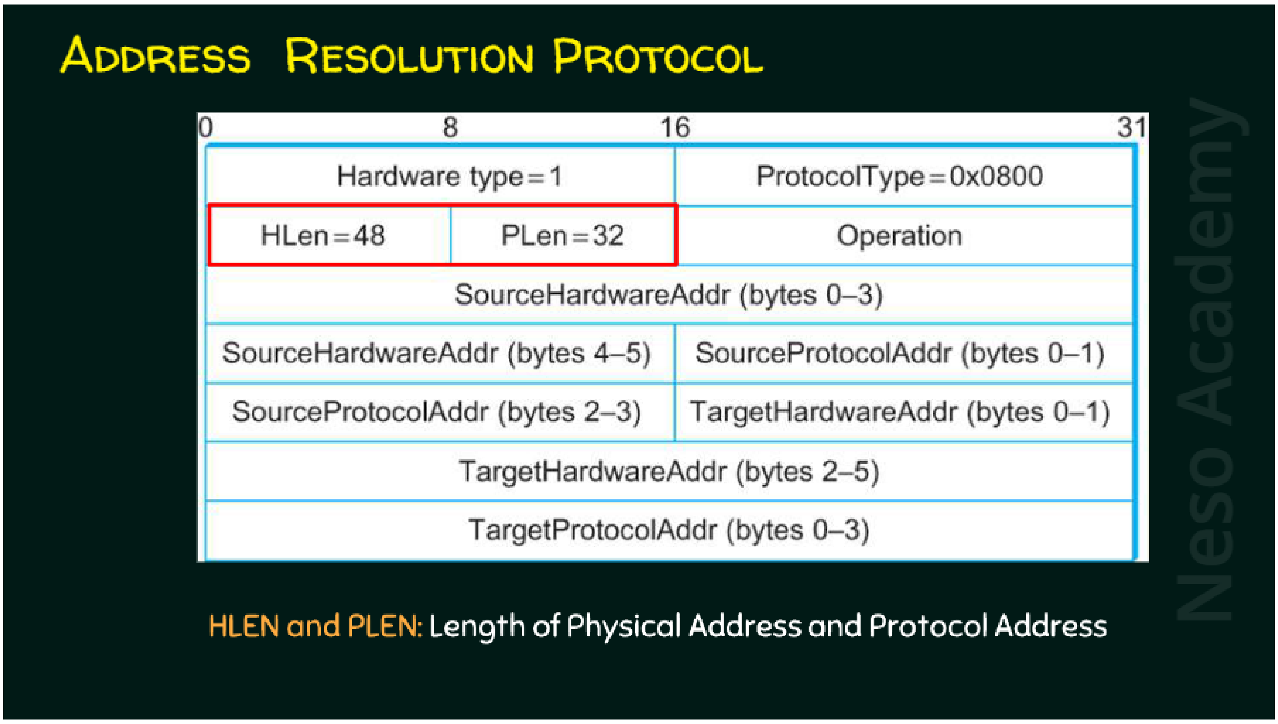
Address Resolution ProtocolNeso Academy



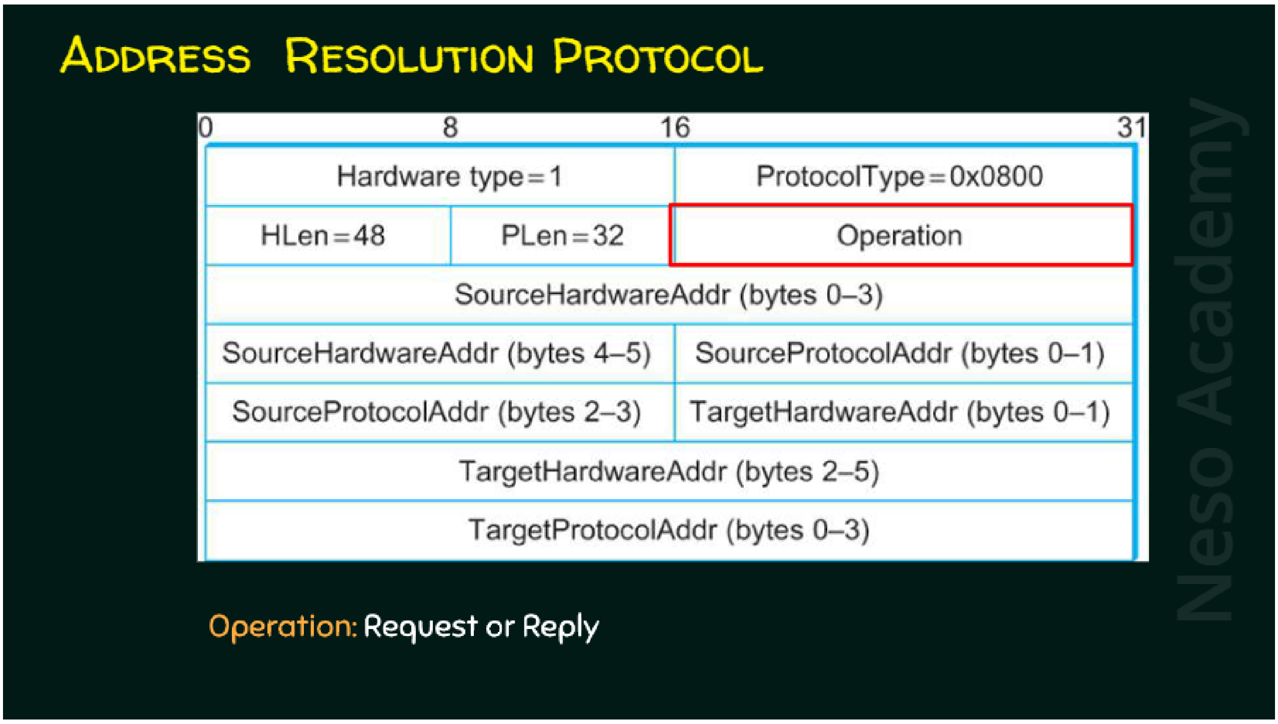
Address Resolution ProtocolNeso Academy



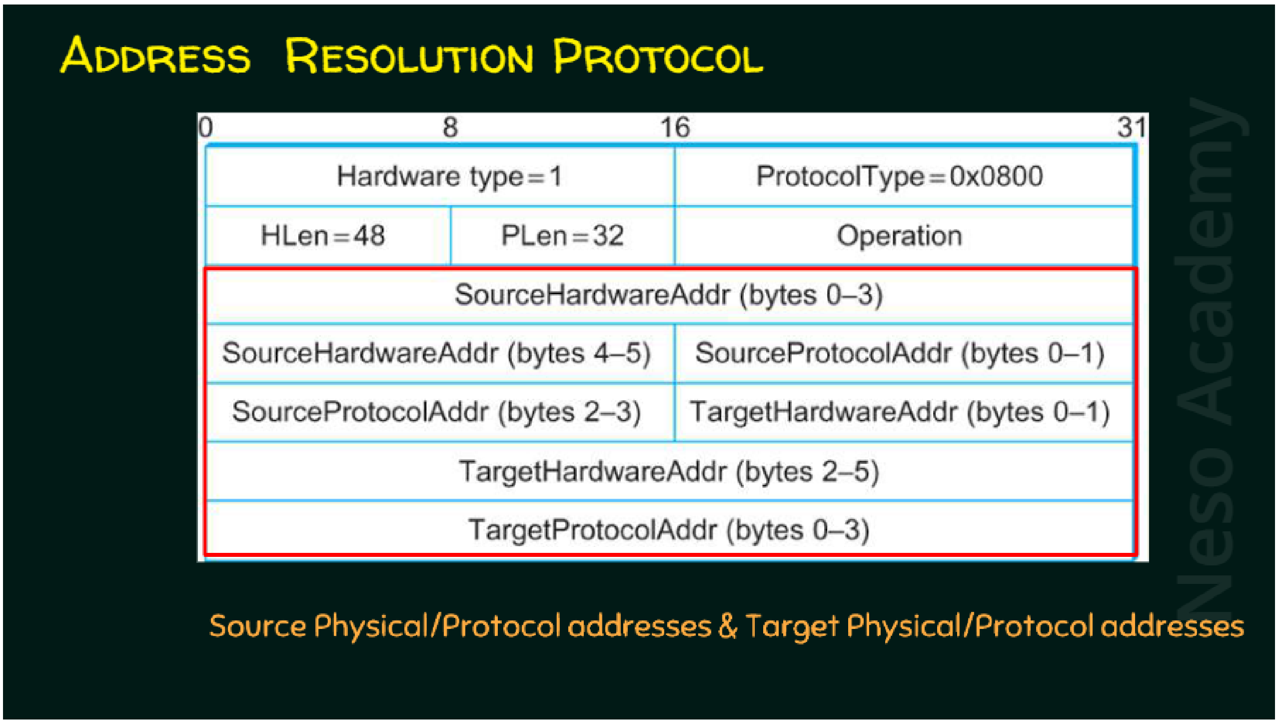
Address Resolution ProtocolNeso Academy



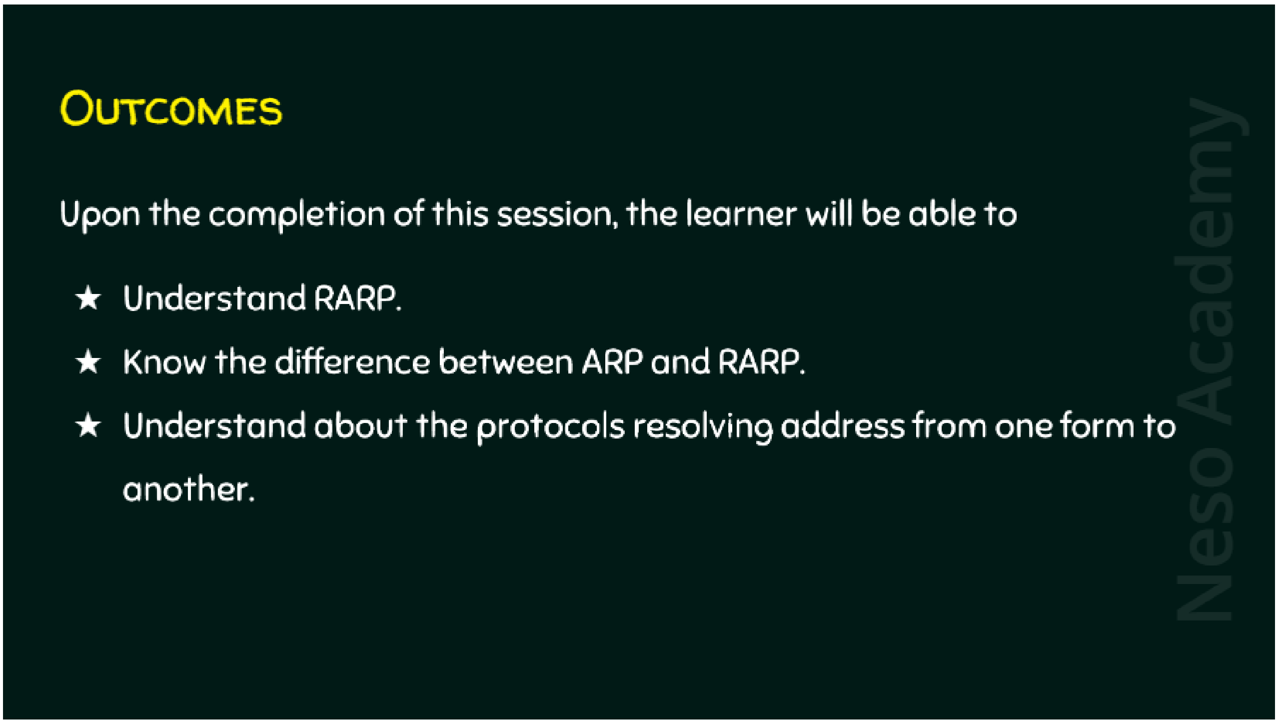
Address Resolution ProtocolNeso Academy



Address Resolution ProtocolNeso Academy



Address Resolution ProtocolNeso Academy



Outcomes★★★Neso Academy

ARP AND RARP

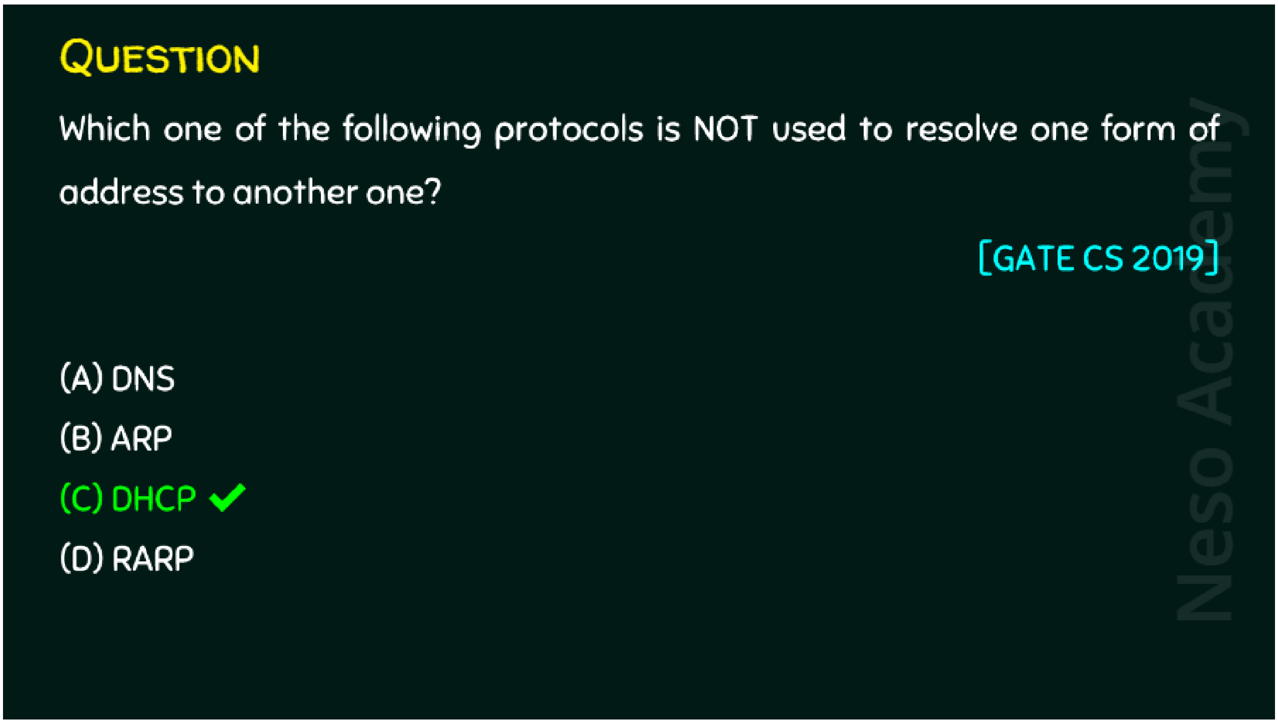
- ★ ARP: Maps IP address to Physical address.
- ★ Reverse ARP (RARP) is an obsolete computer networking protocol used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its link layer or hardware address, such as a MAC address.
- ★ This protocol can use the known MAC address to retrieve its IP address. Functionality wise, RARP is the complete opposite of the ARP. The ARP uses the known IP address to determine the MAC address of the hardware.

ARP and RARP★★★Neso Academy

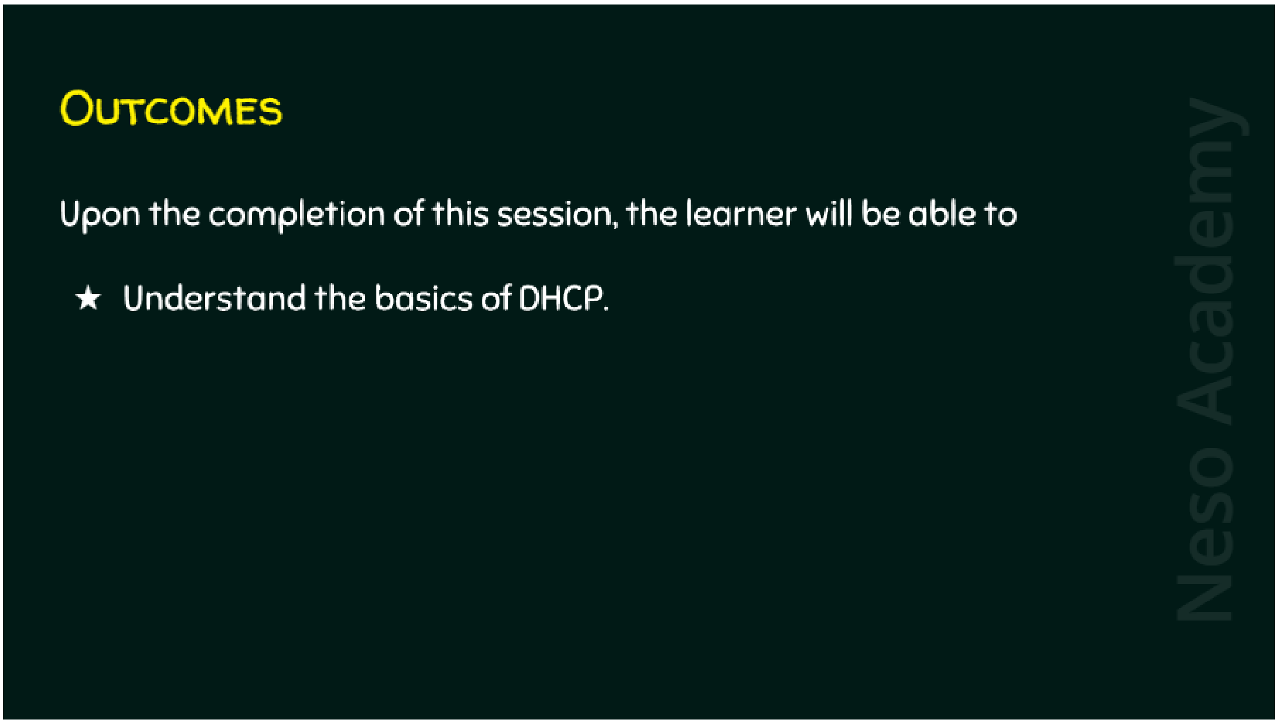
ARP AND RARP

- ★ It is possible for a device to not know its own IP address. This may happen if, for example, the device could not save the IP address because there was insufficient memory available. In such cases, the Reverse ARP is used.
- ★ It has been rendered obsolete by the Bootstrap Protocol (BOOTP) and the modern Dynamic Host Configuration Protocol (DHCP), which both support a much greater feature set than RARP.
- ★ The RARP cannot handle subnetting because no subnet masks are sent. If multiple subnets are deployed, an RARP server must be available in each subnet.

ARP and RARP★★★Neso Academy

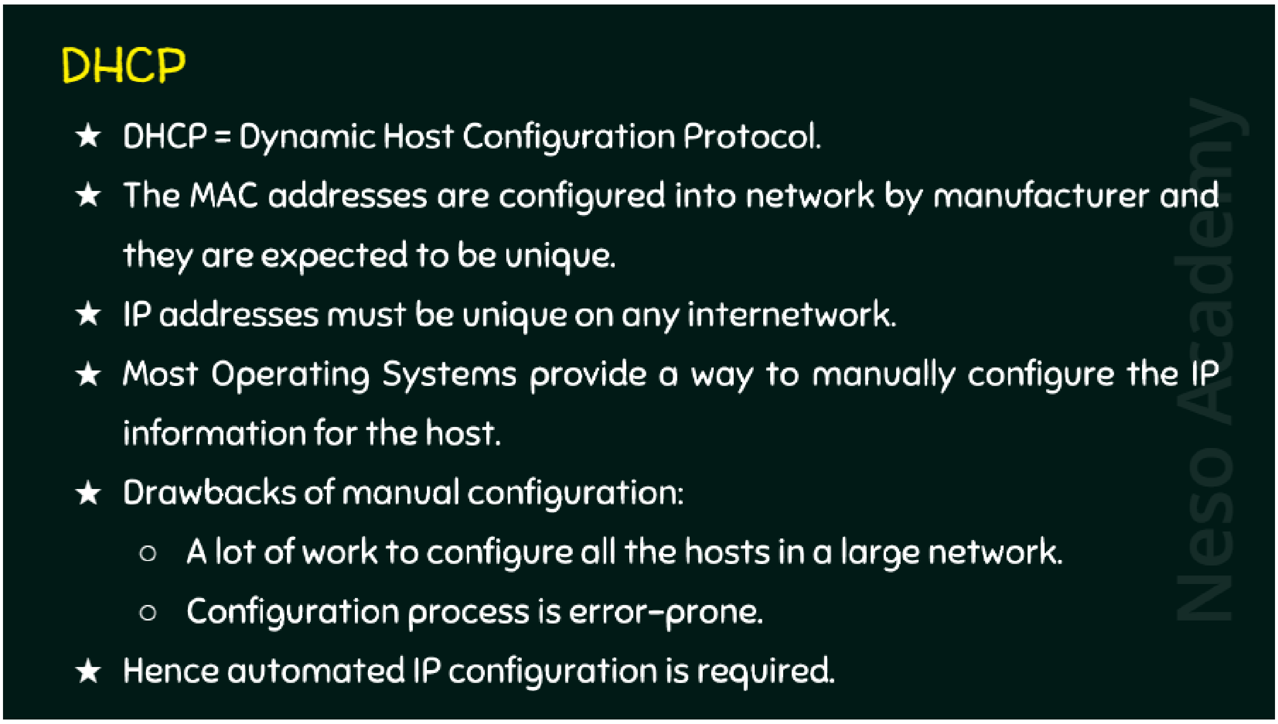


Question✓Neso Academy

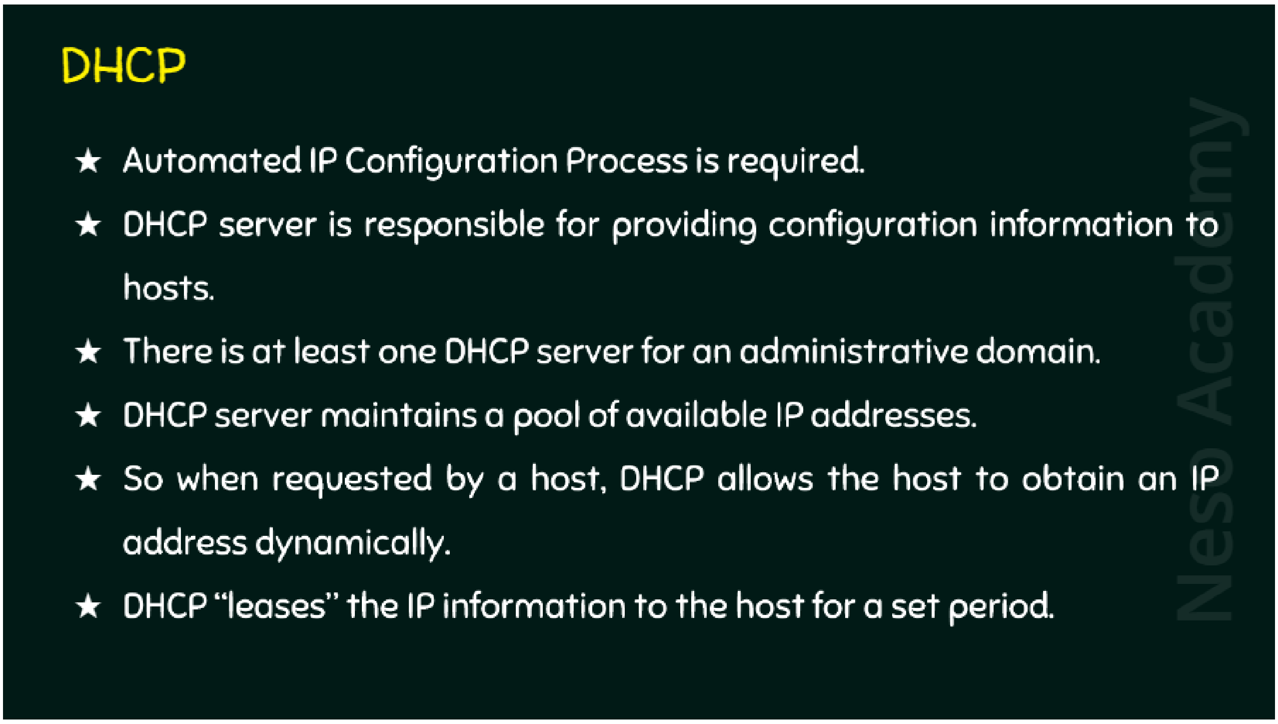


Outcomes★Neso Academy

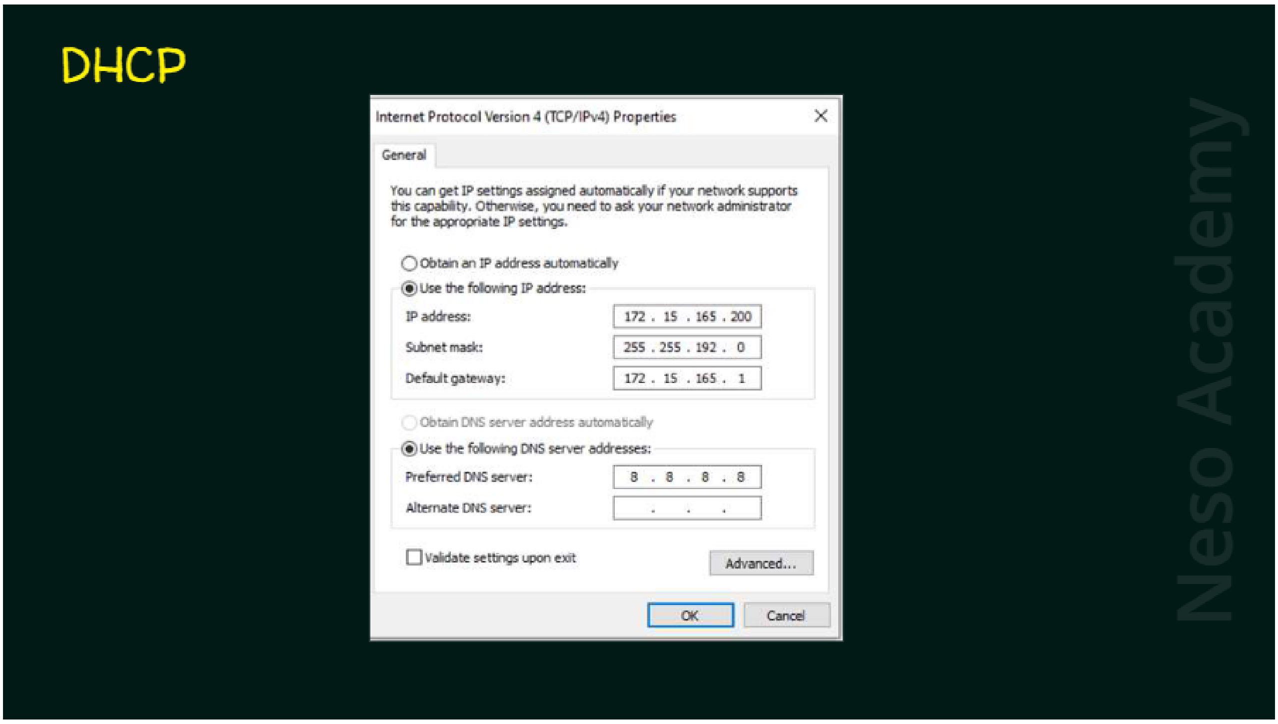
You are a Network administrator!Neso Academy



DHCP★★★★★○○★Neso Academy

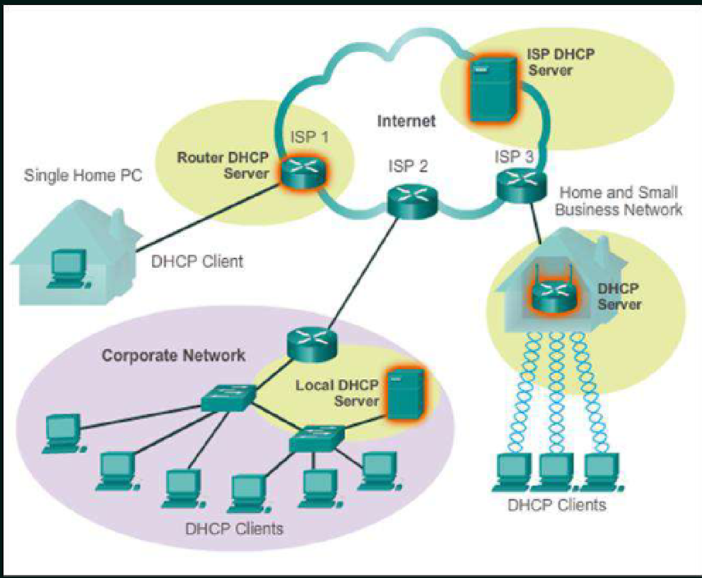


DHCP★★★★★★Neso Academy



DHCPNeso Academy

DHCP



DHCPNeso Academy

Outcomes

Upon the completion of this session, the learner will be able to

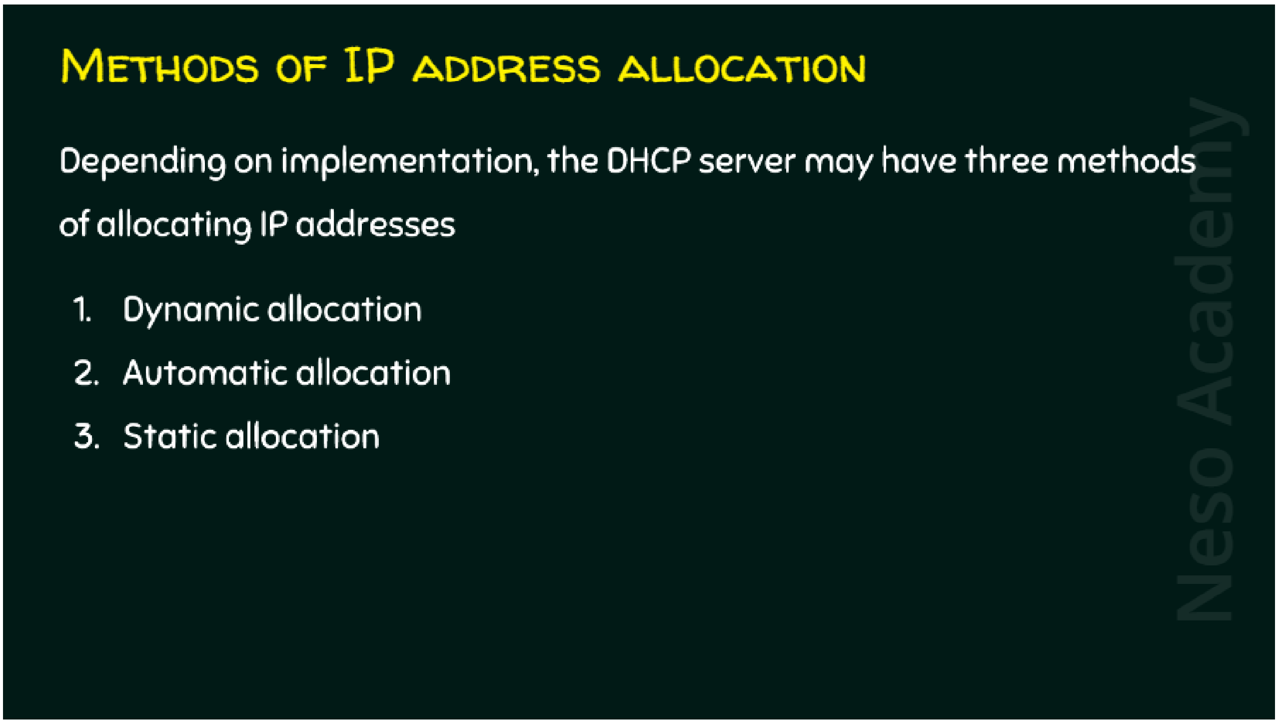
★ Know the various methods of IP address allocation.

★ Understand the working of DHCP server in same network.

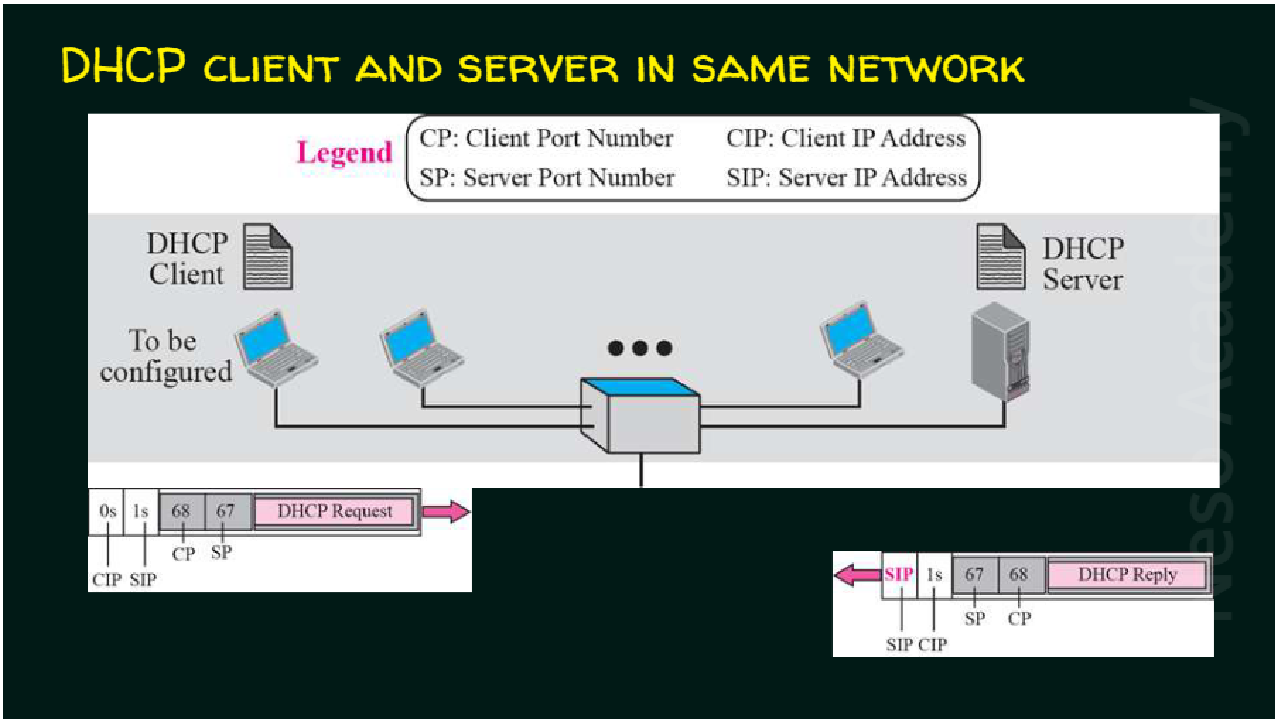
★ Understand the working of DHCP server in different network.

★ Know the DHCP packet format.

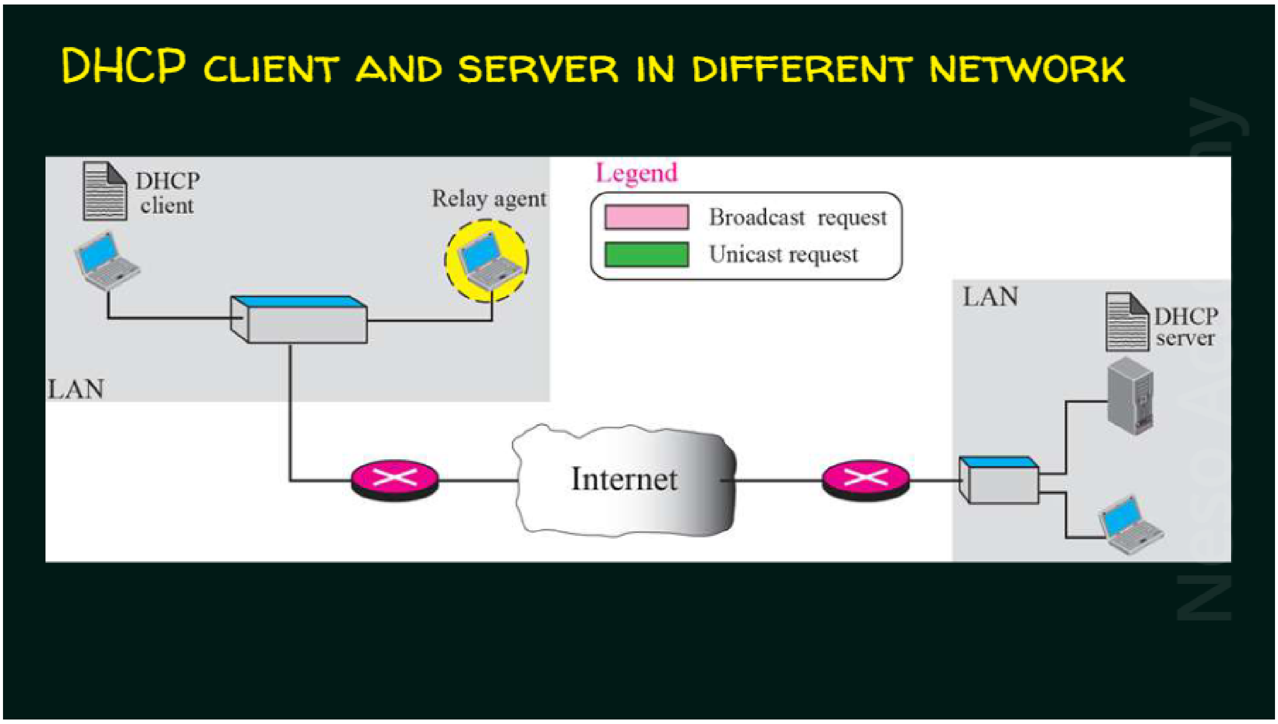
Outcomes★★★★Neso Academy



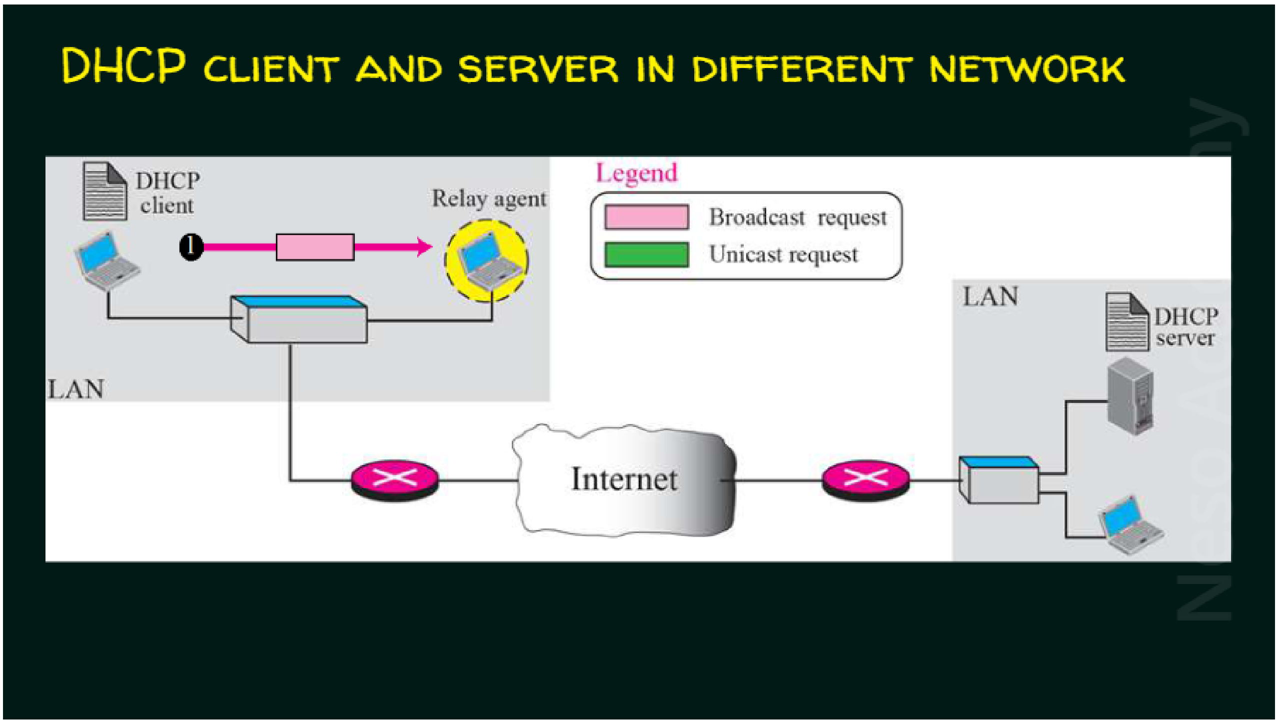
Methods of IP address allocationNeso Academy



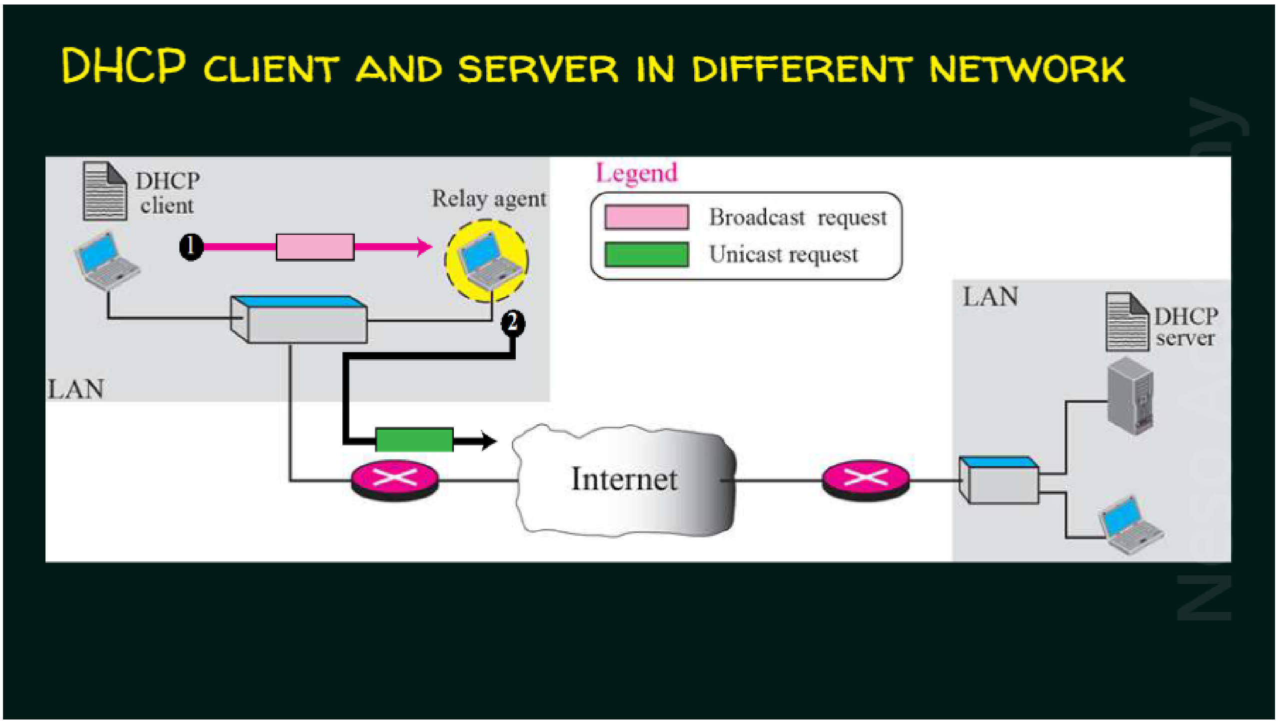
DHCP client and server in same networkNeso Academy



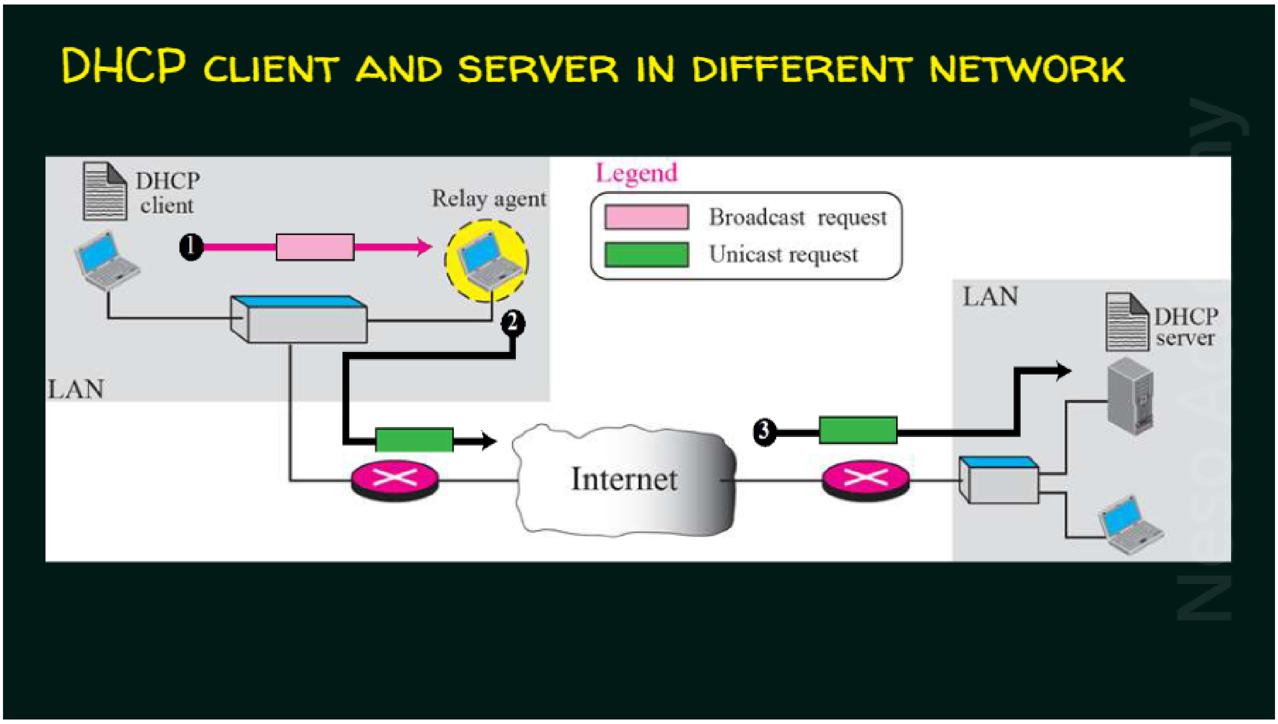
DHCP client and server in different networkNeso Academy



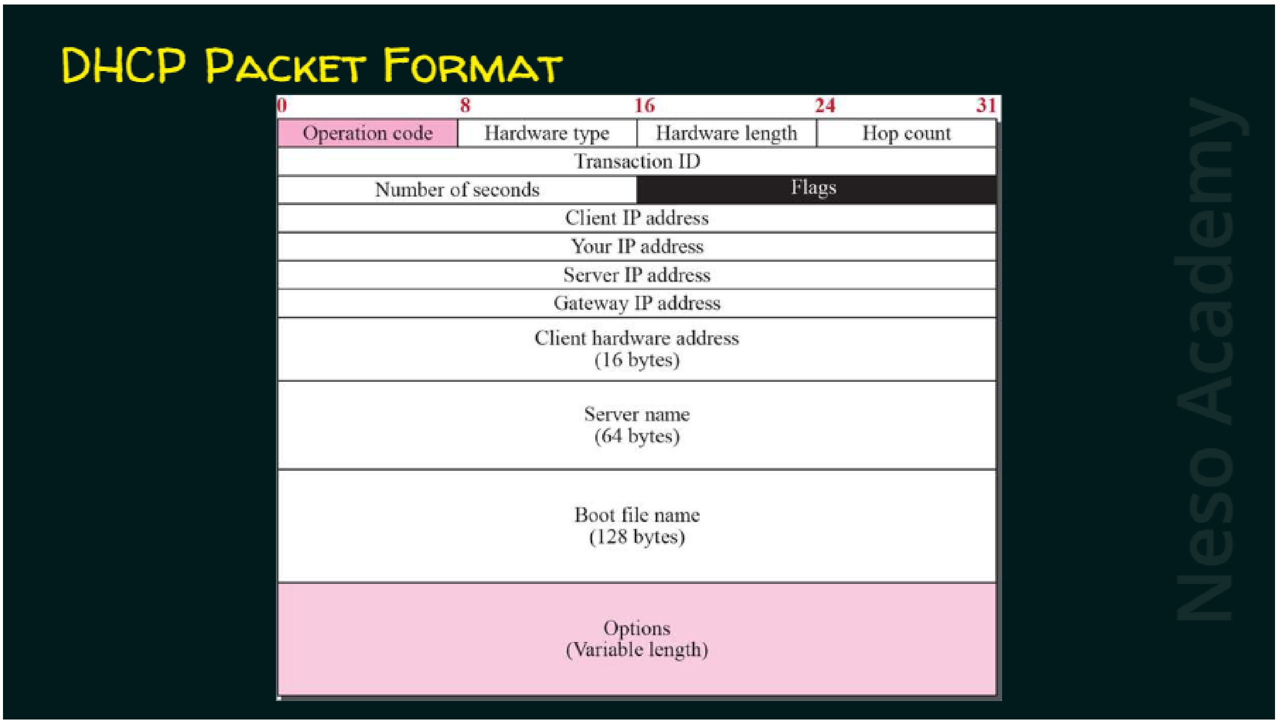
DHCP client and server in different networkNeso Academy



DHCP client and server in different networkNeso Academy



DHCP client and server in different networkNeso Academy

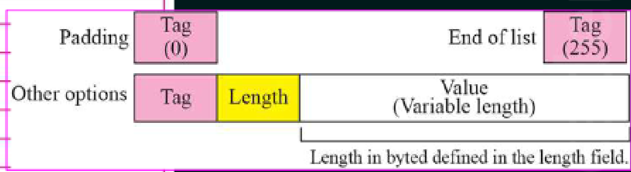


DHCP Packet FormatNeso Academy

DHCP Packet Format

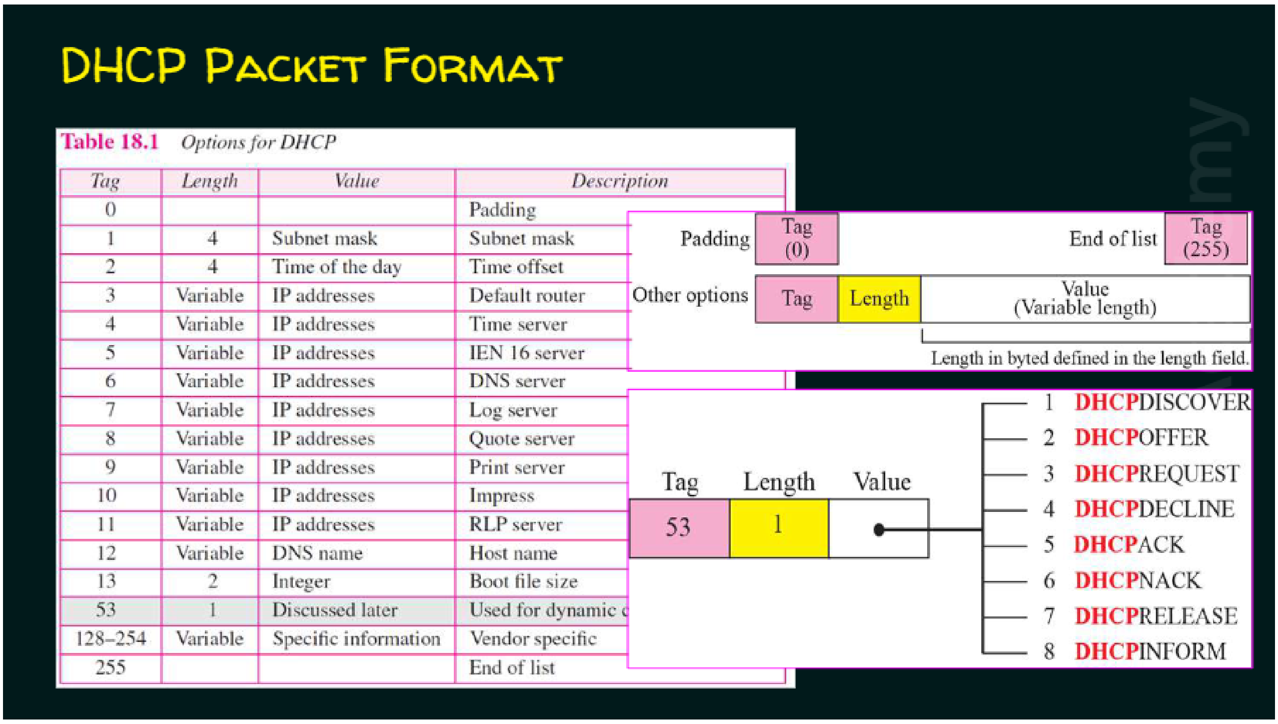
Table 18.1 *Options for DHCP*

Tag	*Length*	*Value*	*Description*
0			Padding
1	4	Subnet mask	Subnet mask
2	4	Time of the day	Time offset
3	Variable	IP addresses	Default router
4	Variable	IP addresses	Time server
5	Variable	IP addresses	IEN 16 server
6	Variable	IP addresses	DNS server
7	Variable	IP addresses	Log server
8	Variable	IP addresses	Quote server
9	Variable	IP addresses	Print server
10	Variable	IP addresses	Impress
11	Variable	IP addresses	RLP server
12	Variable	DNS name	Host name
13	2	Integer	Boot file size
53	1	Discussed later	Used for dynamic configuration
128–254	Variable	Specific information	Vendor specific
255			End of list



Neso Academy

DHCP Packet FormatNeso Academy



DHCP Packet Format

Table 18.1 *Options for DHCP*

Tag	*Length*	*Value*	*Description*
0			Padding
1	4	Subnet mask	Subnet mask
2	4	Time of the day	Time offset
3	Variable	IP addresses	Default router
4	Variable	IP addresses	Time server
5	Variable	IP addresses	IEN 16 server
6	Variable	IP addresses	DNS server
7	Variable	IP addresses	Log server
8	Variable	IP addresses	Quote server
9	Variable	IP addresses	Print server
10	Variable	IP addresses	Impress
11	Variable	IP addresses	RLP server
12	Variable	DNS name	Host name
13	2	Integer	Boot file size
53	1	Discussed later	Used for dynamic c
128–254	Variable	Specific information	Vendor specific
255			End of list

DHCP Packet FormatNeso Academy

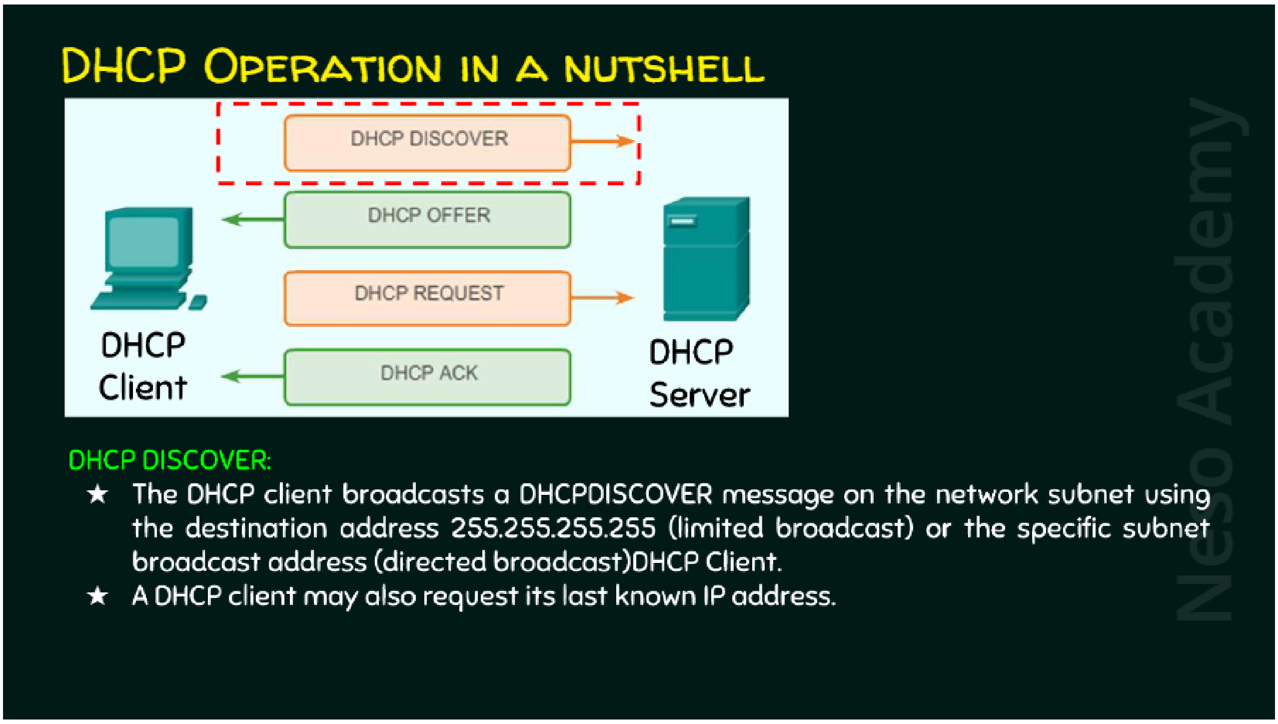
Outcomes

Upon the completion of this session, the learner will be able to

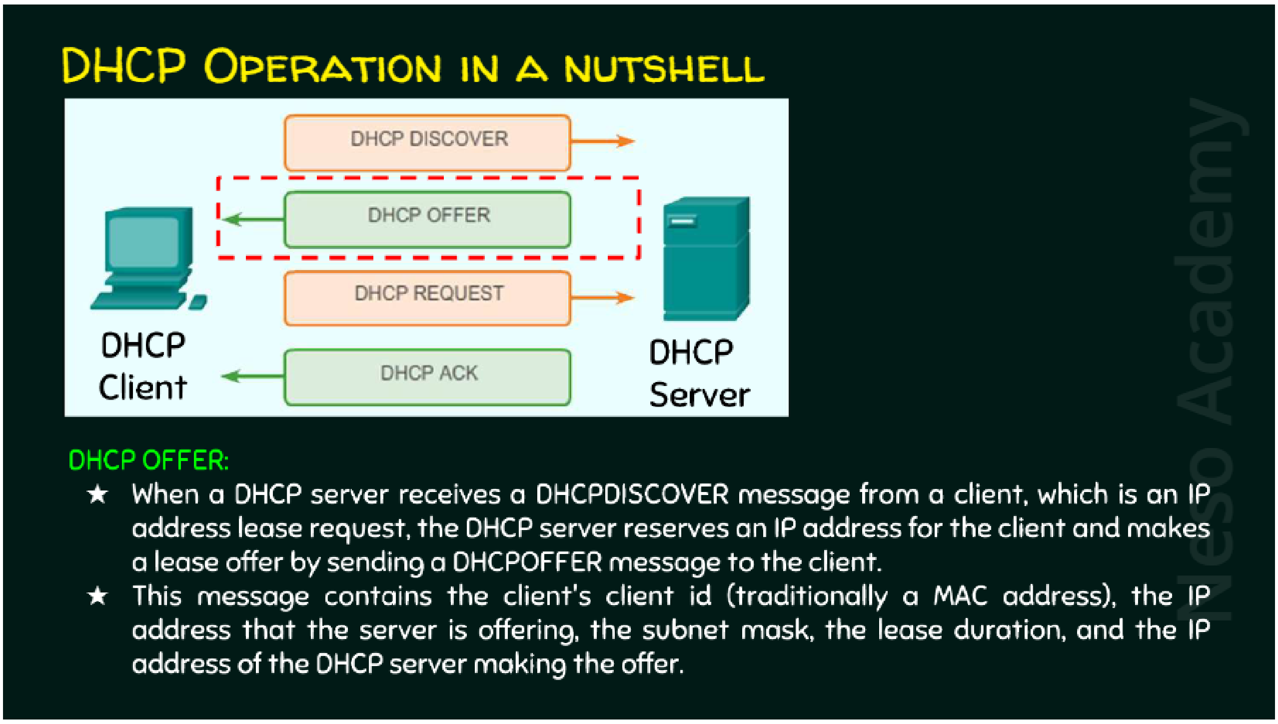
★ Know the DHCP packet format.

★ Know the operation of DHCP.

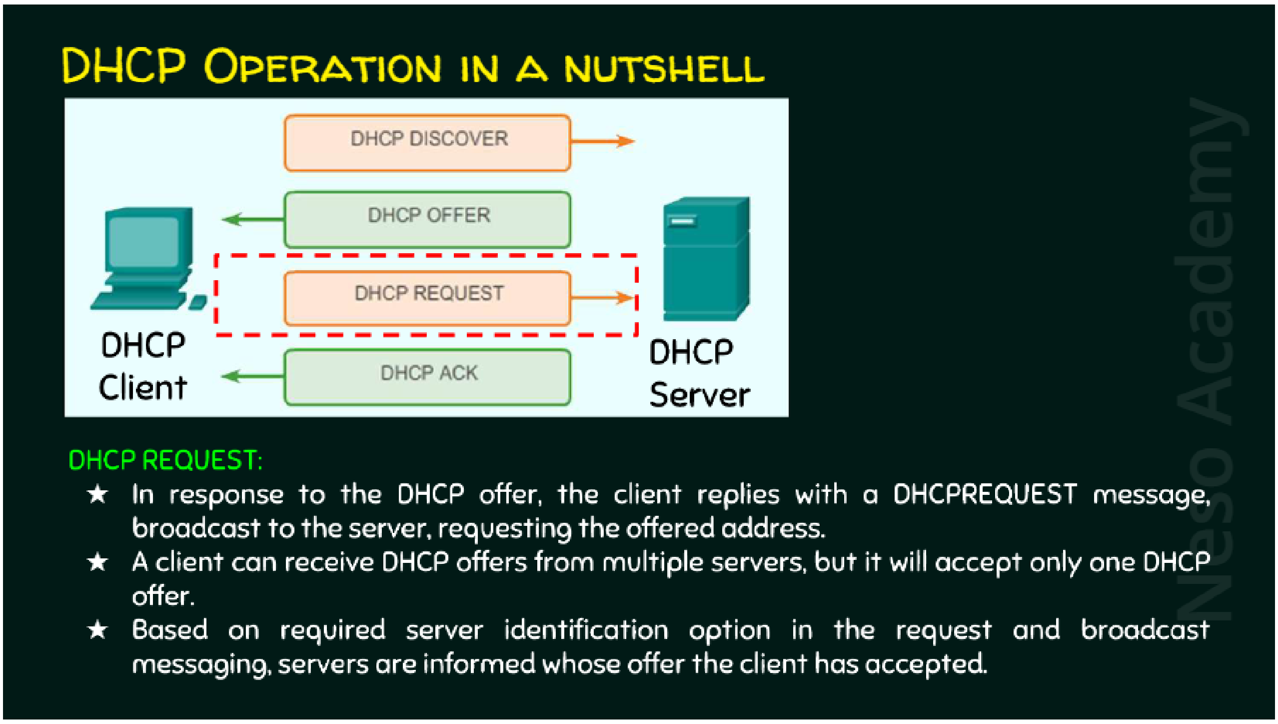
Outcomes★★Neso Academy



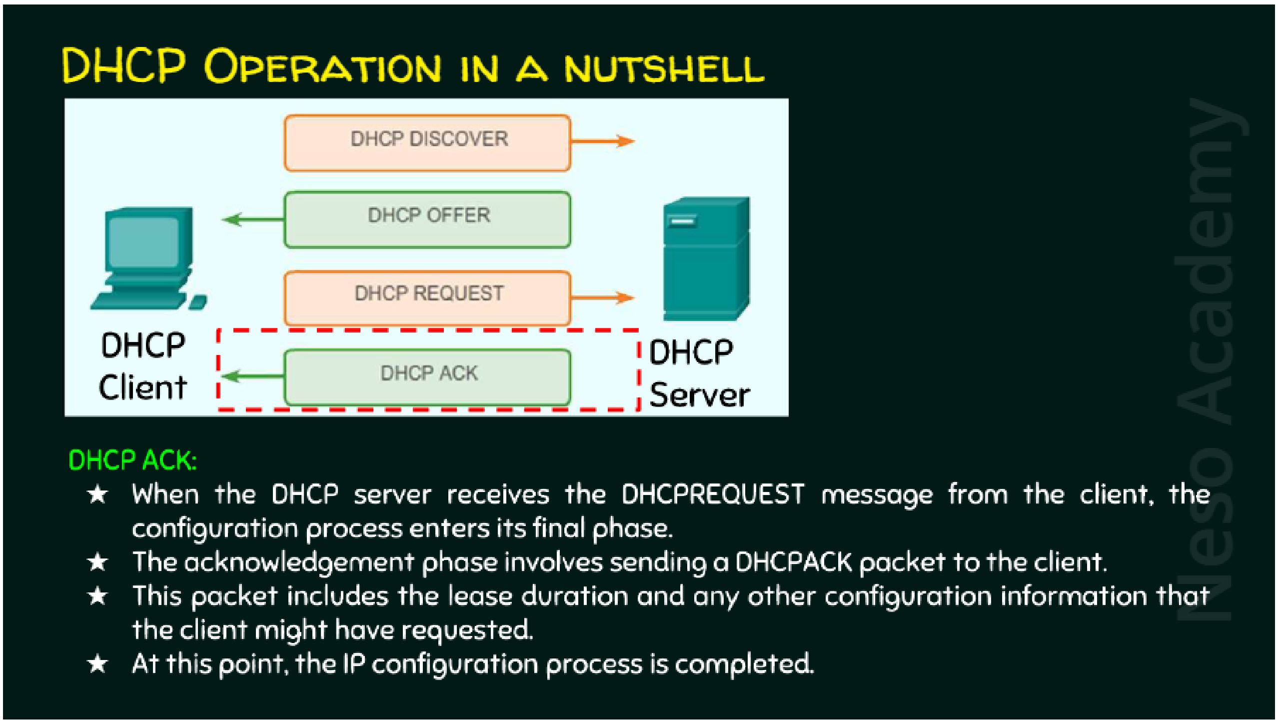
DHCP Operation in a nutshell★★Neso Academy



DHCP Operation in a nutshell★★Neso Academy



DHCP Operation in a nutshell★★★Neso Academy



DHCP Operation in a nutshell★★★★Neso Academy

Outcomes

Upon the completion of this session, the learner will be able to

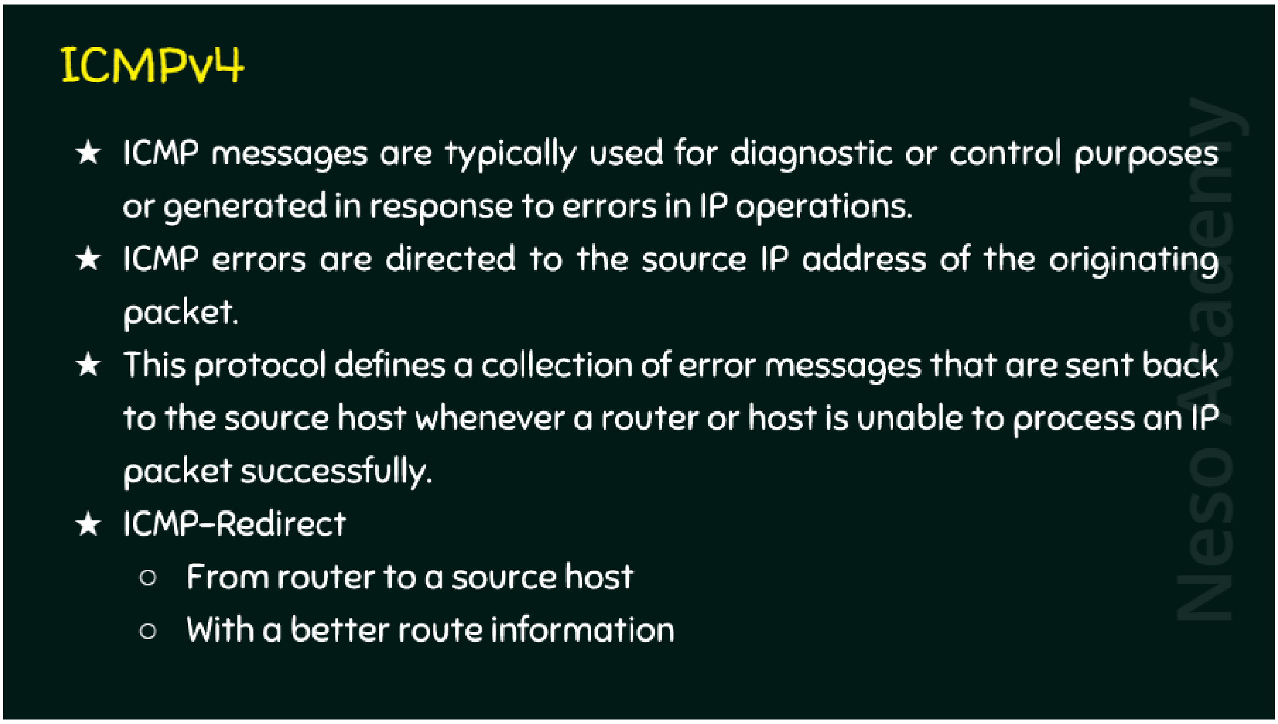
- ★ Know about ICMPv4.
- ★ Understand ICMP Redirect.
- ★ Know the ICMPv4 packet format.

Outcomes★★★Neso Academy

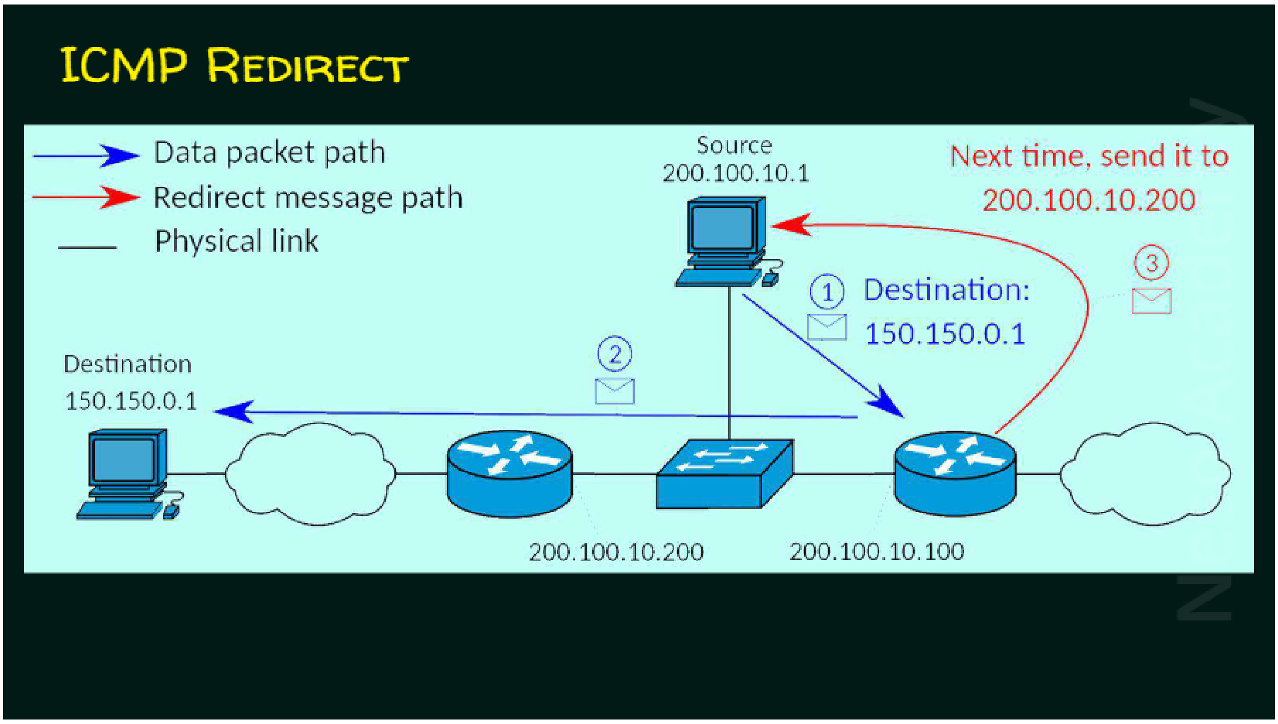
ICMPv4

- ★ ICMP = Internet Control Message Protocol.
- ★ ICMP is a supporting protocol in the Internet protocol suite.
- ★ It is used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address.
- ★ Examples:
  - ○ Destination host unreachable due to link /node failure
  - ○ Reassembly process failed
  - ○ TTL had reached 0 (so datagrams don't cycle forever)
  - ○ IP header checksum failed

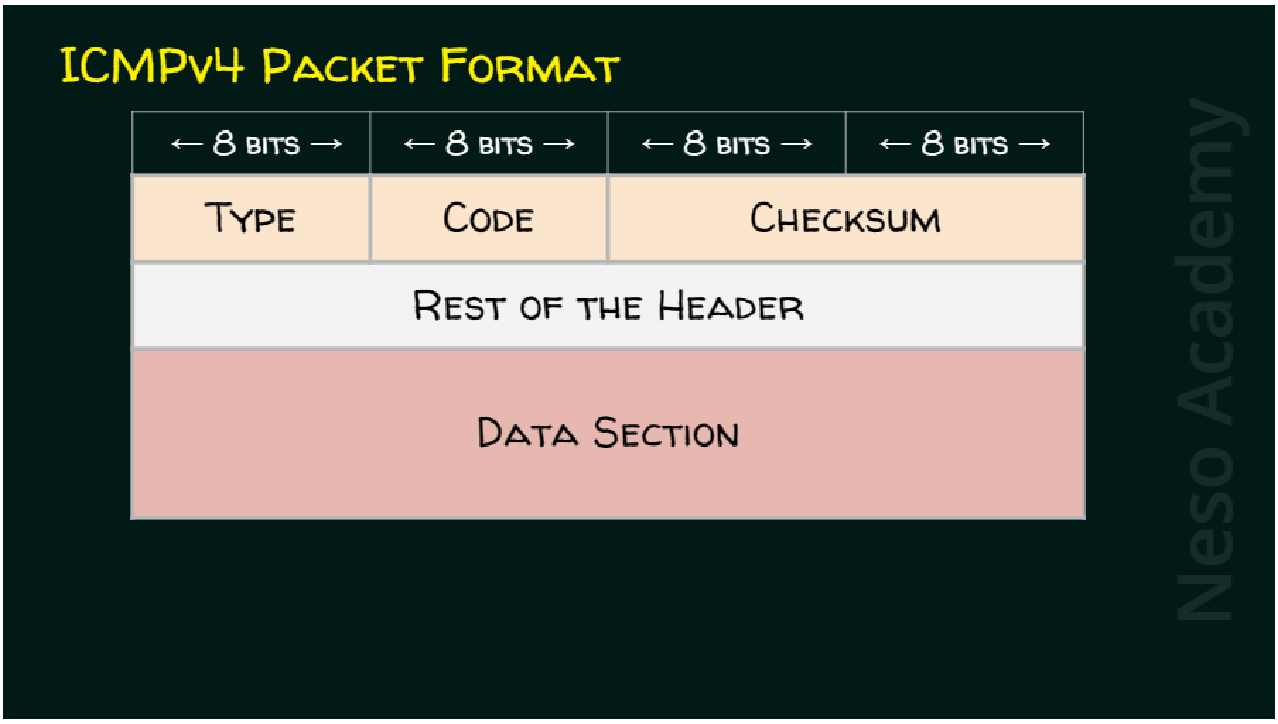
★★★★○○○○ICMPv4Neso Academy



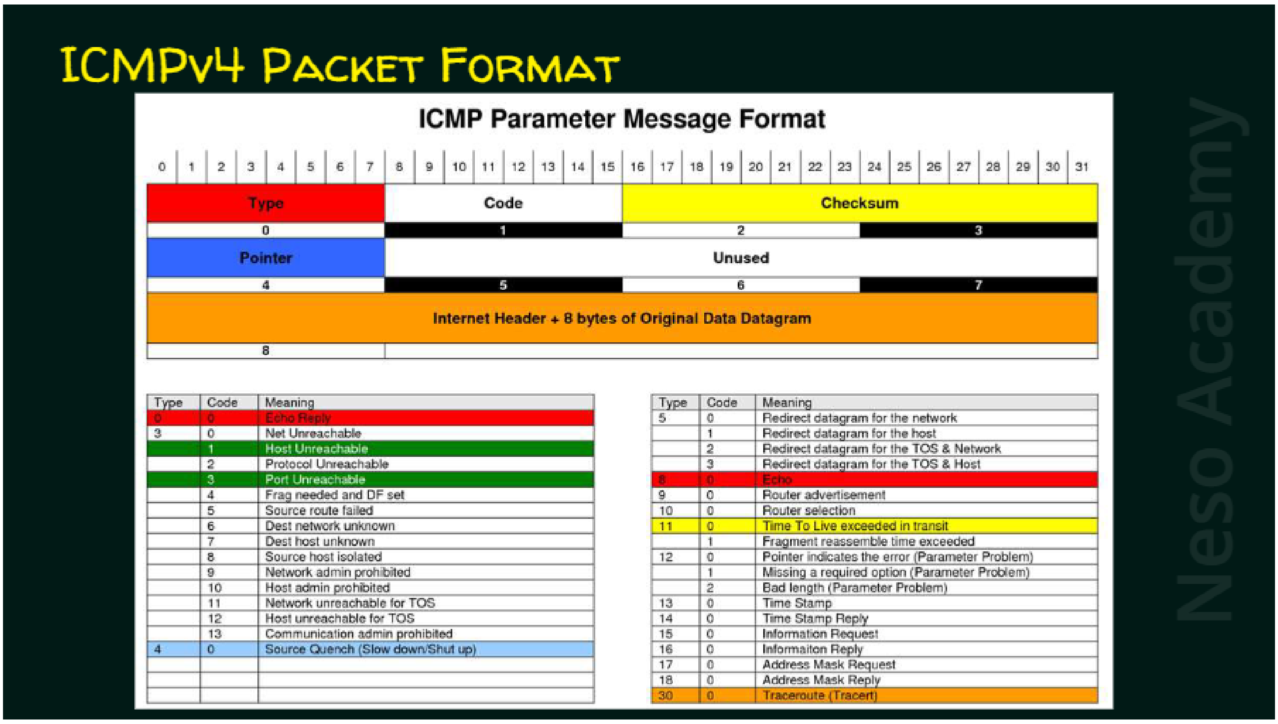
★★★★○○ICMPv4Neso Academy



ICMP RedirectNeso Academy



ICMPv4 Packet Format←8 bits →←8 bits →←8 bits →←8 bits →TypeCodeChecksumRest of the HeaderData SectionNeso Academy



Type	Code	Meaning
0	0	Echo Reply
3	0	Net Unreachable
	1	Host Unreachable
	2	Protocol Unreachable
	3	Port Unreachable
	4	Frag needed and DF set
	5	Source route failed
	6	Dest network unknown
	7	Dest host unknown
	8	Source host isolated
	9	Network admin prohibited
	10	Host admin prohibited
	11	Network unreachable for TOS
	12	Host unreachable for TOS
	13	Communication admin prohibited
4	0	Source Quench (Slow down/Shut up)

Type	Code	Meaning
5	0	Redirect datagram for the network
	1	Redirect datagram for the host
	2	Redirect datagram for the TOS & Network
	3	Redirect datagram for the TOS & Host
8	0	Echo
9	0	Router advertisement
10	0	Router selection
11	0	Time To Live exceeded in transit
	1	Fragment reassemble time exceeded
12	0	Pointer indicates the error (Parameter Problem)
	1	Missing a required option (Parameter Problem)
	2	Bad length (Parameter Problem)
13	0	Time Stamp
14	0	Time Stamp Reply
15	0	Information Request
16	0	Informaiton Reply
17	0	Address Mask Request
18	0	Address Mask Reply
30	0	Traceroute (Tracert)

ICMPv4 Packet FormatNeso Academy

Outcomes

Upon the completion of this session, the learner will be able to

★ Understand the checksum calculation for ICMPv4.

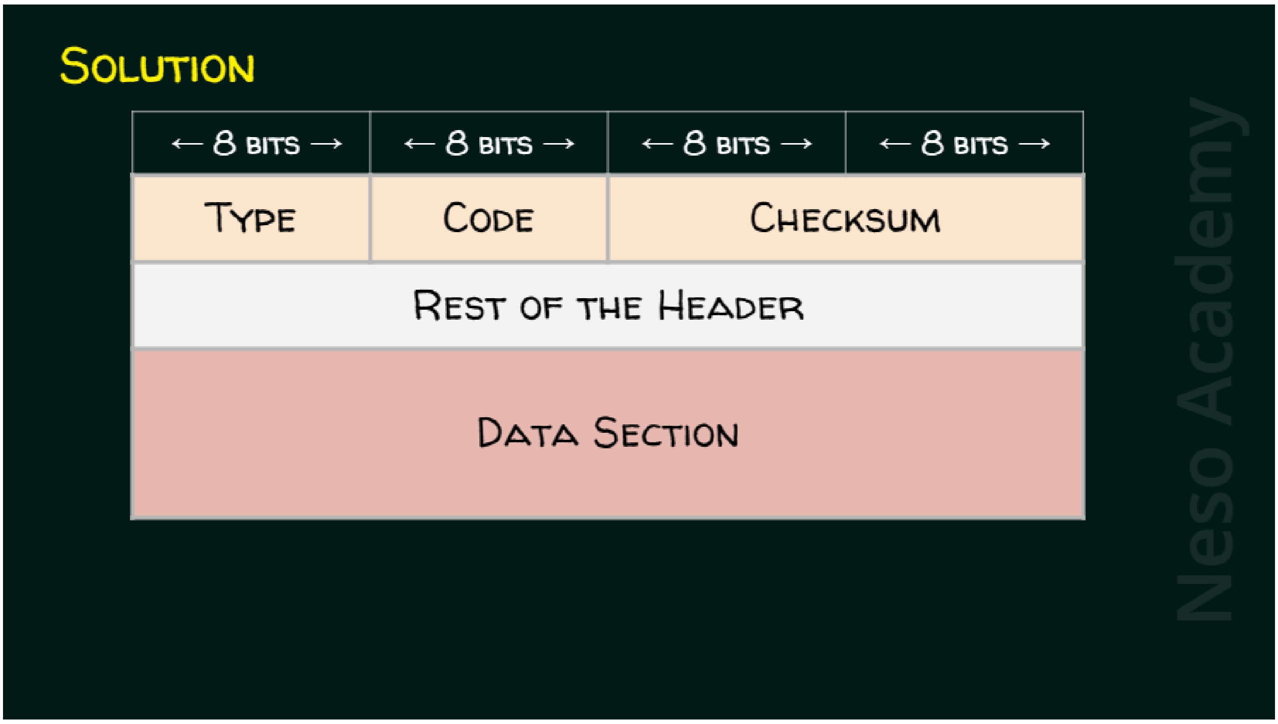
Outcomes★Neso Academy

Question

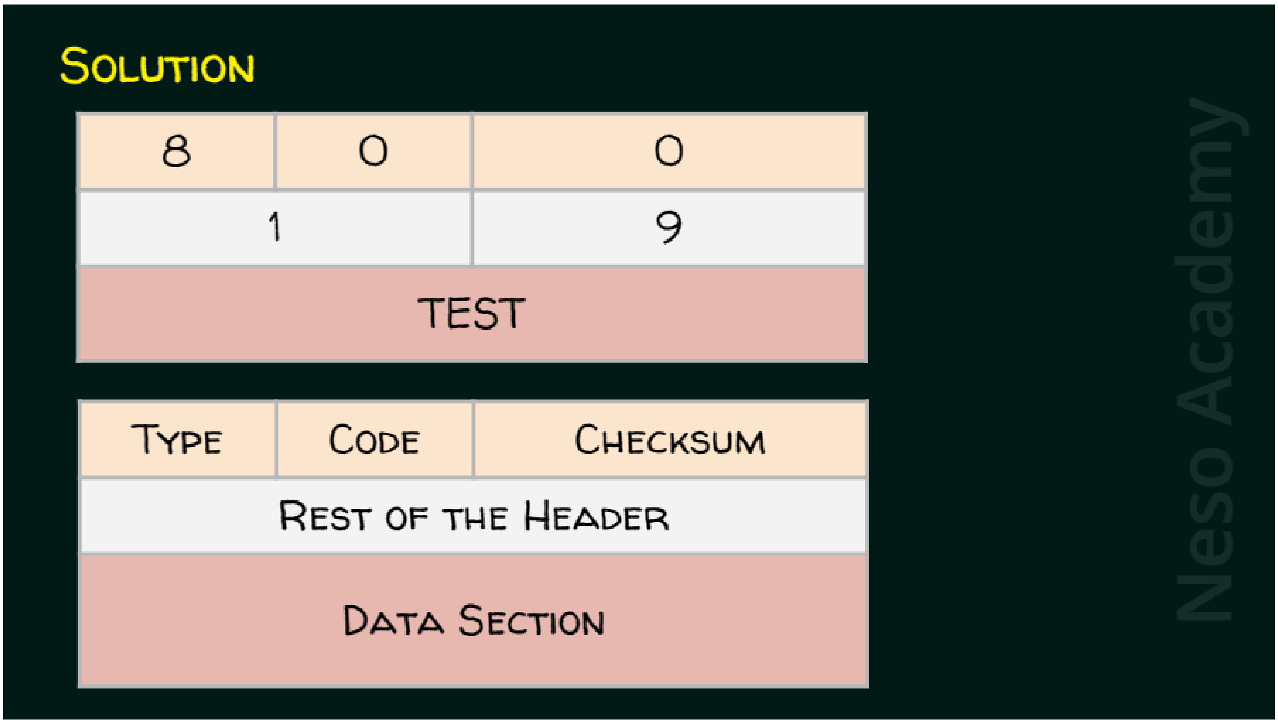
Calculate the checksum for the following ICMPv4 packet.

8	0	0
1		9
TEST		

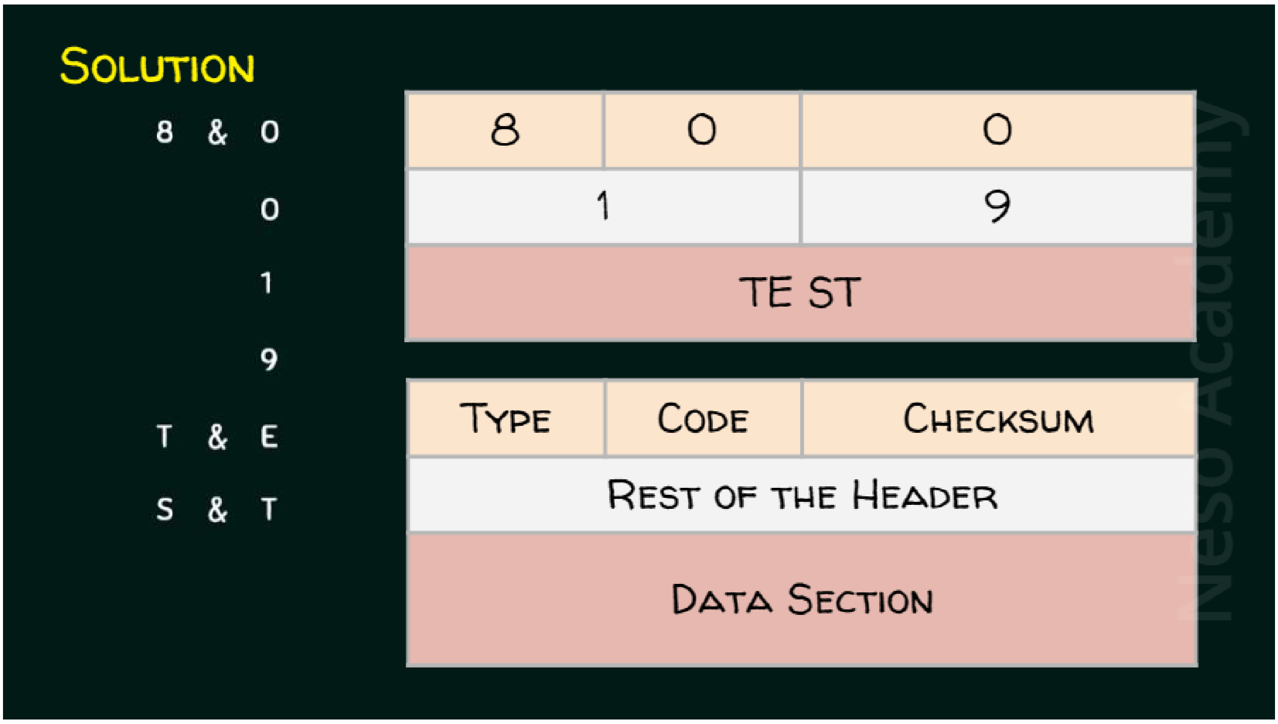
Question80019TESTNeso Academy



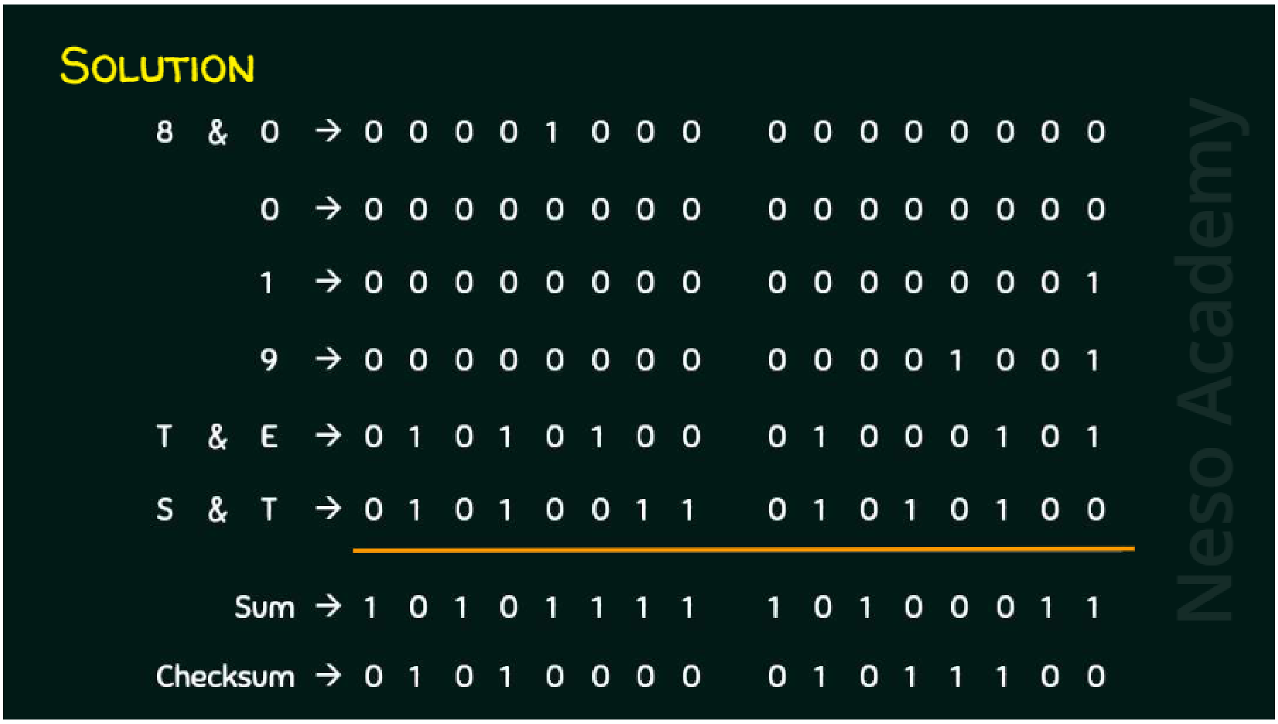
Solution←8 bits →←8 bits →←8 bits →←8 bits →TypeCodeChecksumRest of the HeaderData SectionNeso Academy



Solution80019TESTTypeCodeChecksumRest of the HeaderData SectionNeso Academy



Solution80019TE STTypeCodeChecksumRest of the HeaderData SectionNeso Academy



SolutionNeso Academy

Solution

Calculate the checksum for the following ICMPv4 packet.

8	0	0101000001011100
1		9
TEST		

Solution80010100000101110019TESTNeso Academy

Outcomes

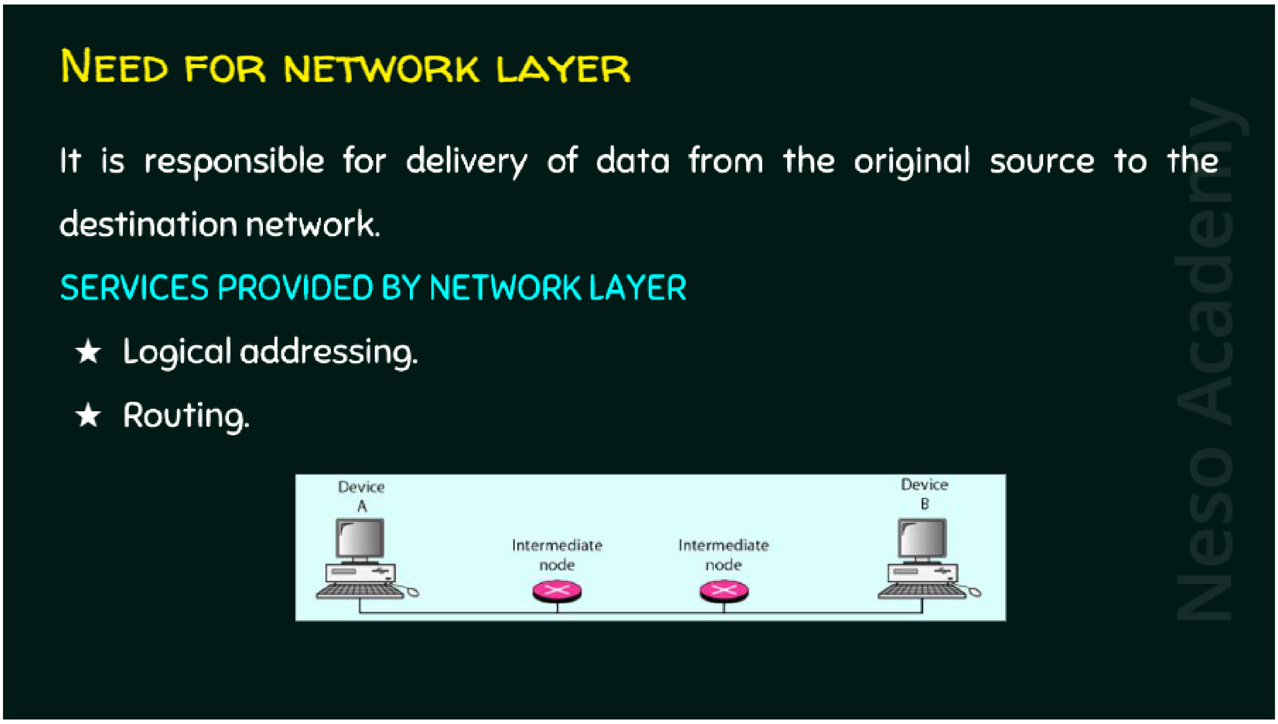
Upon the completion of this session, the learner will be able to

★ Know the need for network layer.

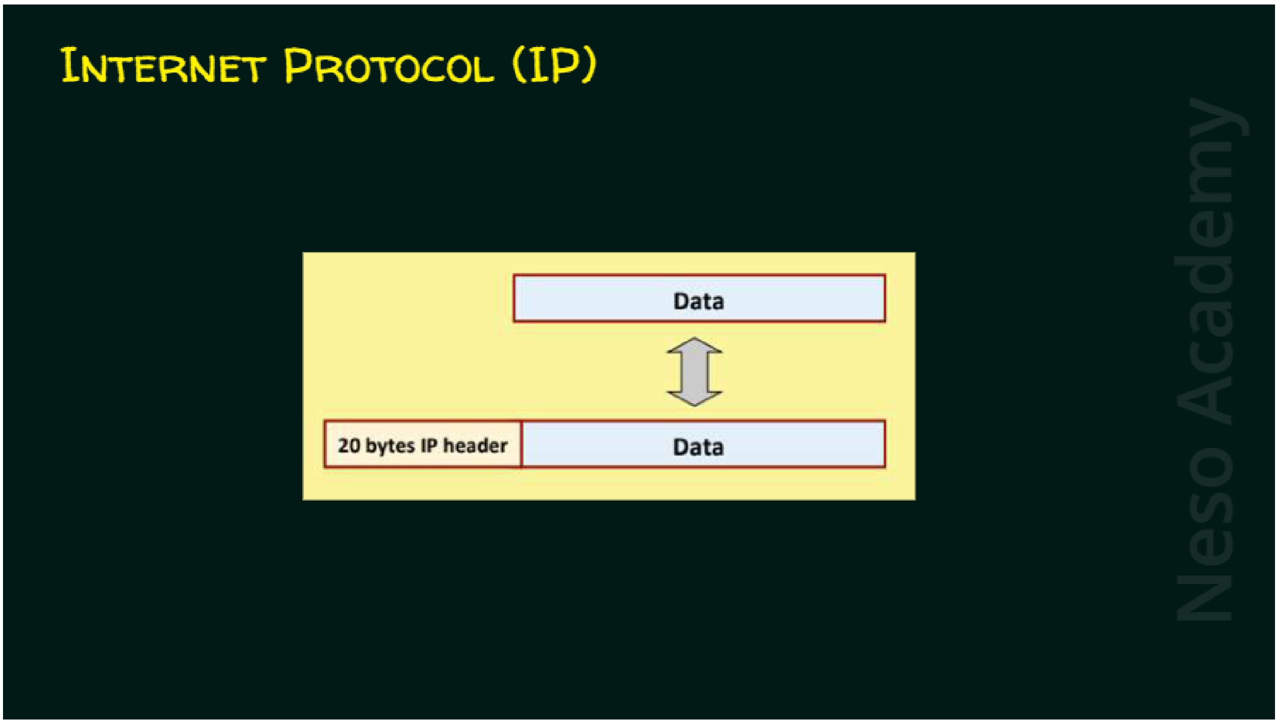
★ Understand the most widely used IPv4 Protocol.

★ Know IPv4 header format and various fields..

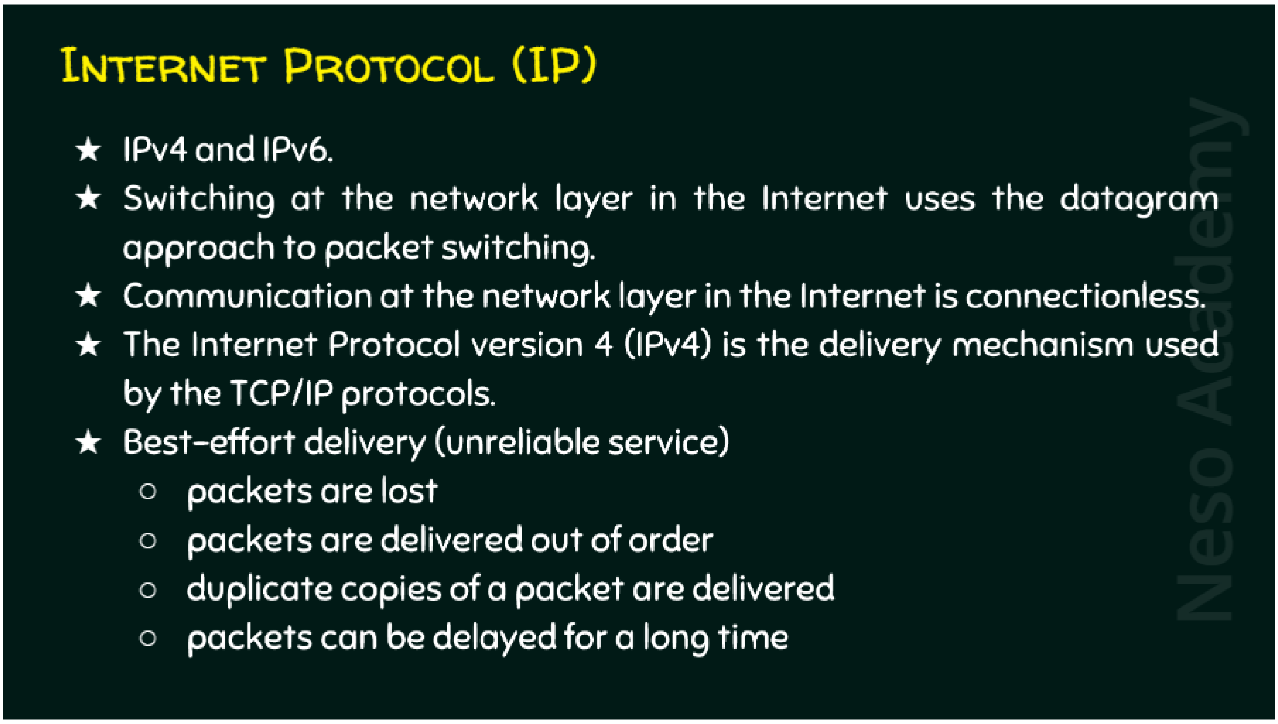
Outcomes★★★Neso Academy



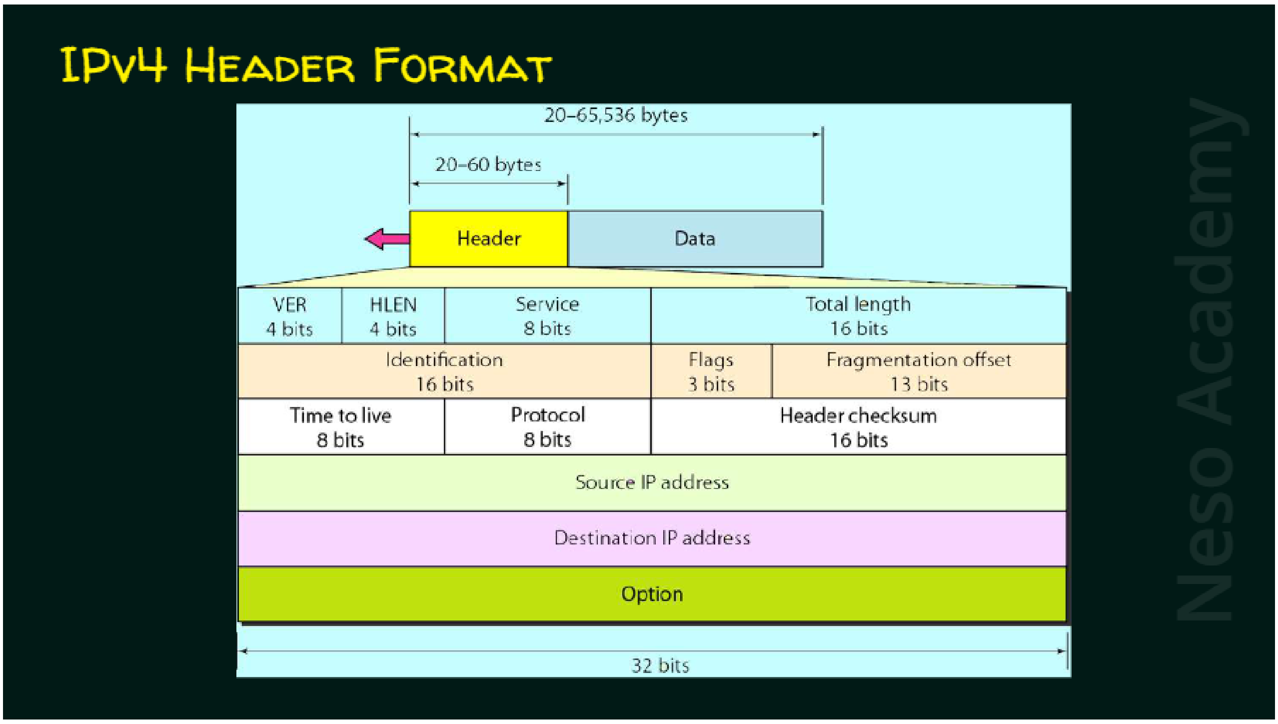
★★Need for network layerNeso Academy



Internet Protocol (IP)Neso Academy



★★★★★○○○○Internet Protocol (IP)Neso Academy



IPv4 Header FormatNeso Academy

IPv4 Header Format

<table>
<tr><td>VER
4 bits</td><td>HLEN
4 bits</td><td colspan="2">Service
8 bits</td><td colspan="3">Total length
16 bits</td></tr>
<tr><td colspan="4">Identification
16 bits</td><td>Flags
3 bits</td><td colspan="2">Fragmentation offset
13 bits</td></tr>
<tr><td colspan="2">Time to live
8 bits</td><td colspan="2">Protocol
8 bits</td><td colspan="3">Header checksum
16 bits</td></tr>
<tr><td colspan="7">Source IP address</td></tr>
<tr><td colspan="7">Destination IP address</td></tr>
<tr><td colspan="7">Option</td></tr>
<tr><td colspan="7">DATA (Variable Size)</td></tr>
</table>

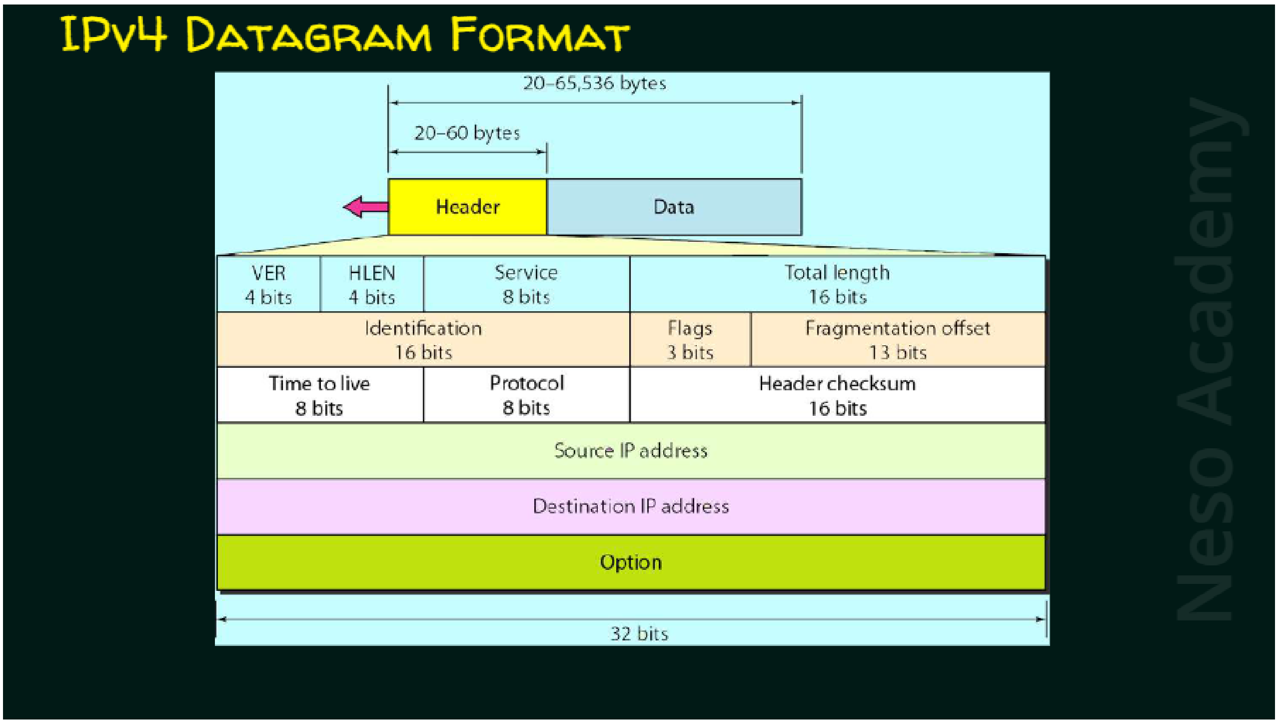
IPv4 Header FormatDATA (Variable Size)Neso Academy

Outcomes

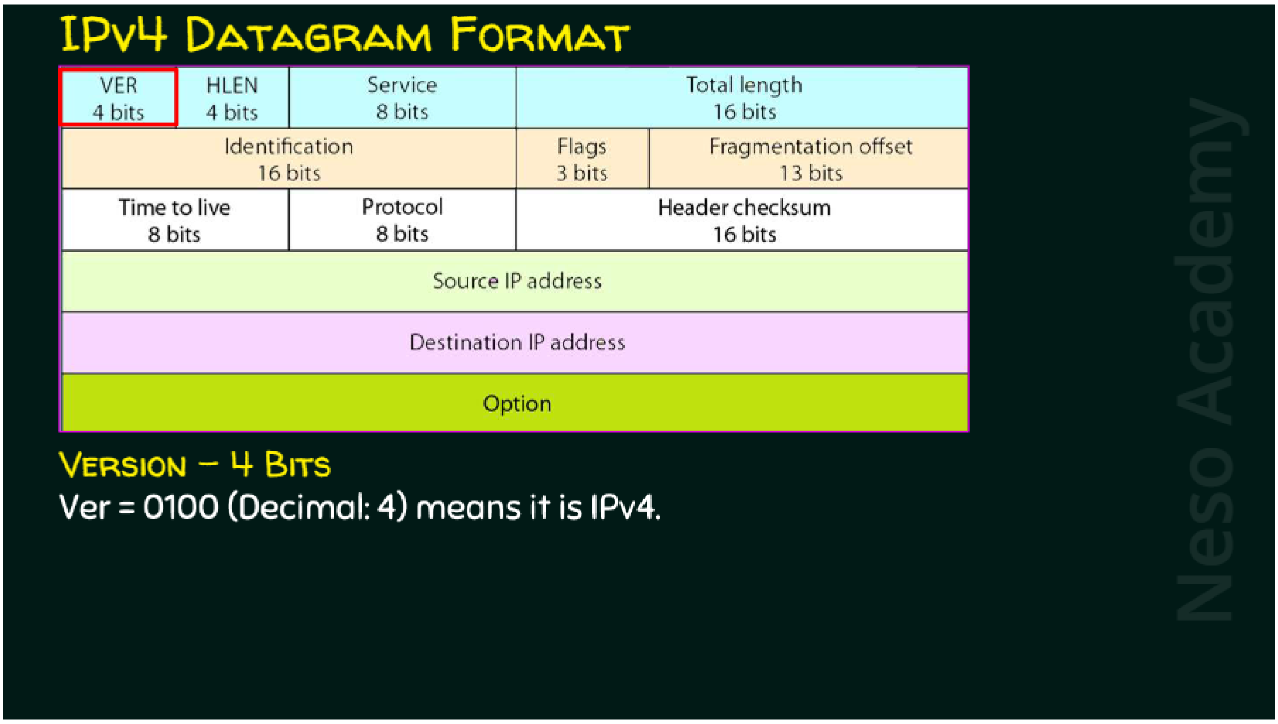
Upon the completion of this session, the learner will be able to

★ Understand the various fields of the IPv4 header format.

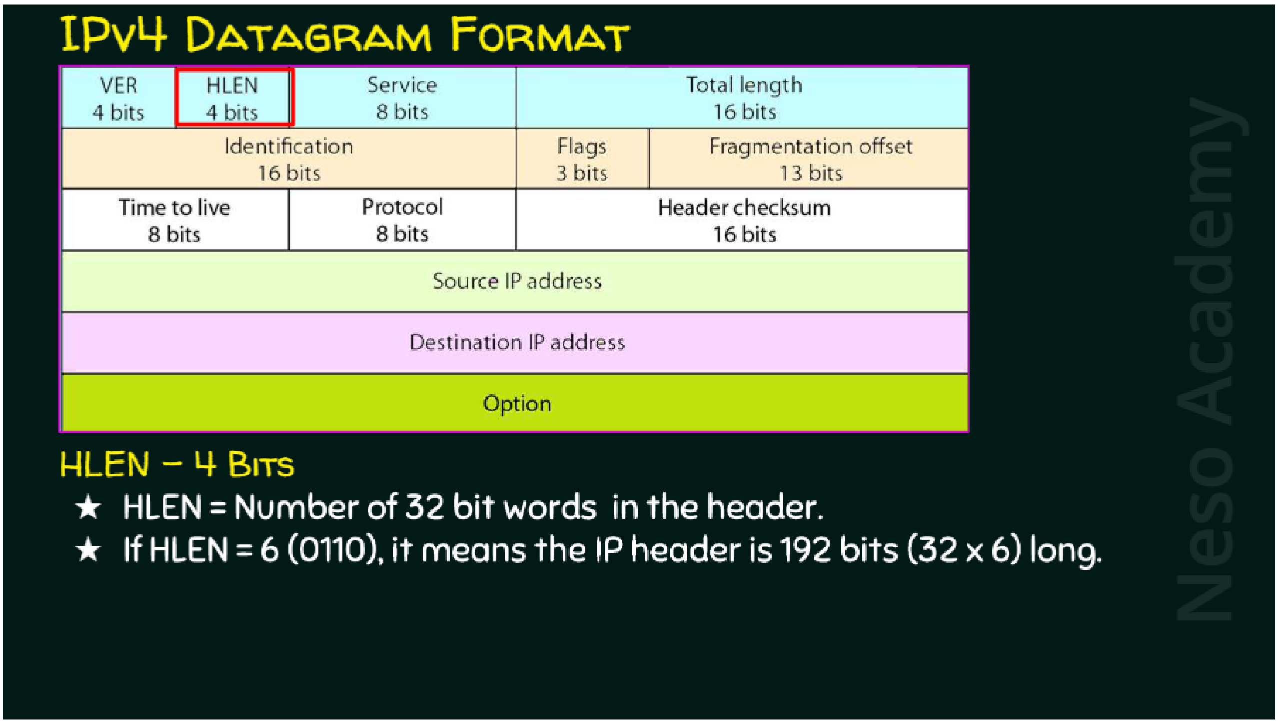
★OutcomesNeso Academy



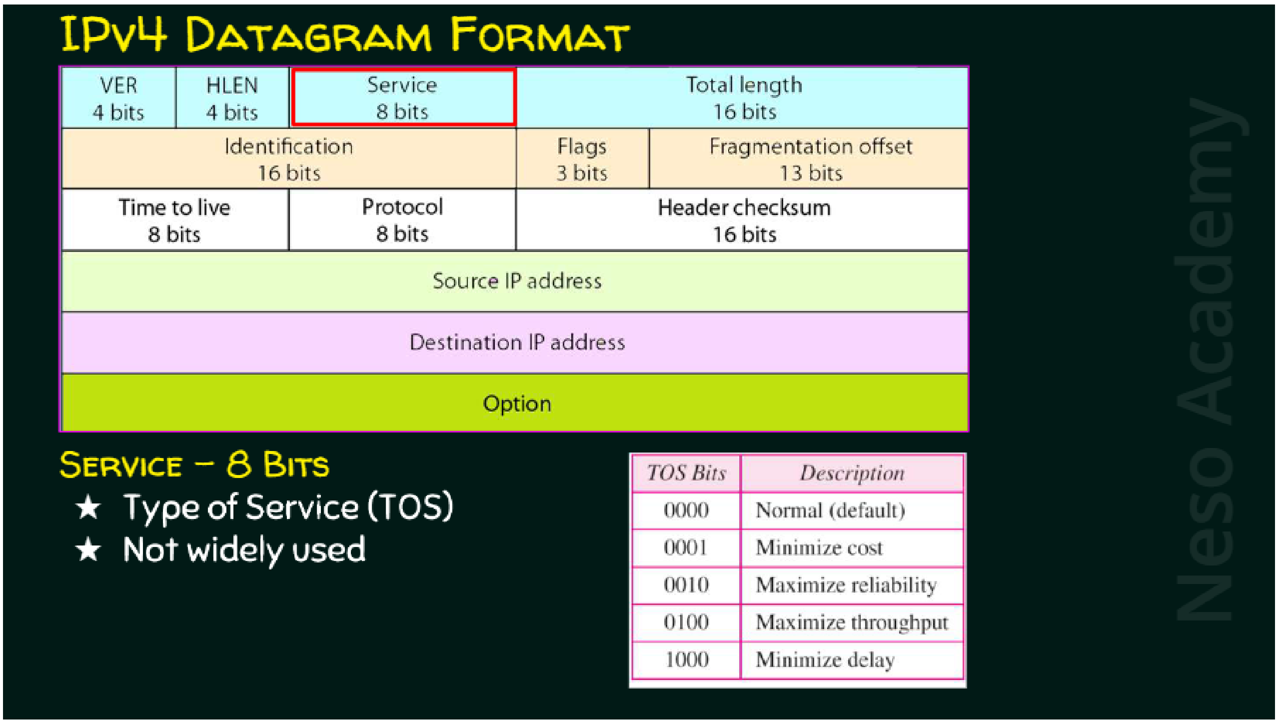
IPv4 Datagram FormatNeso Academy



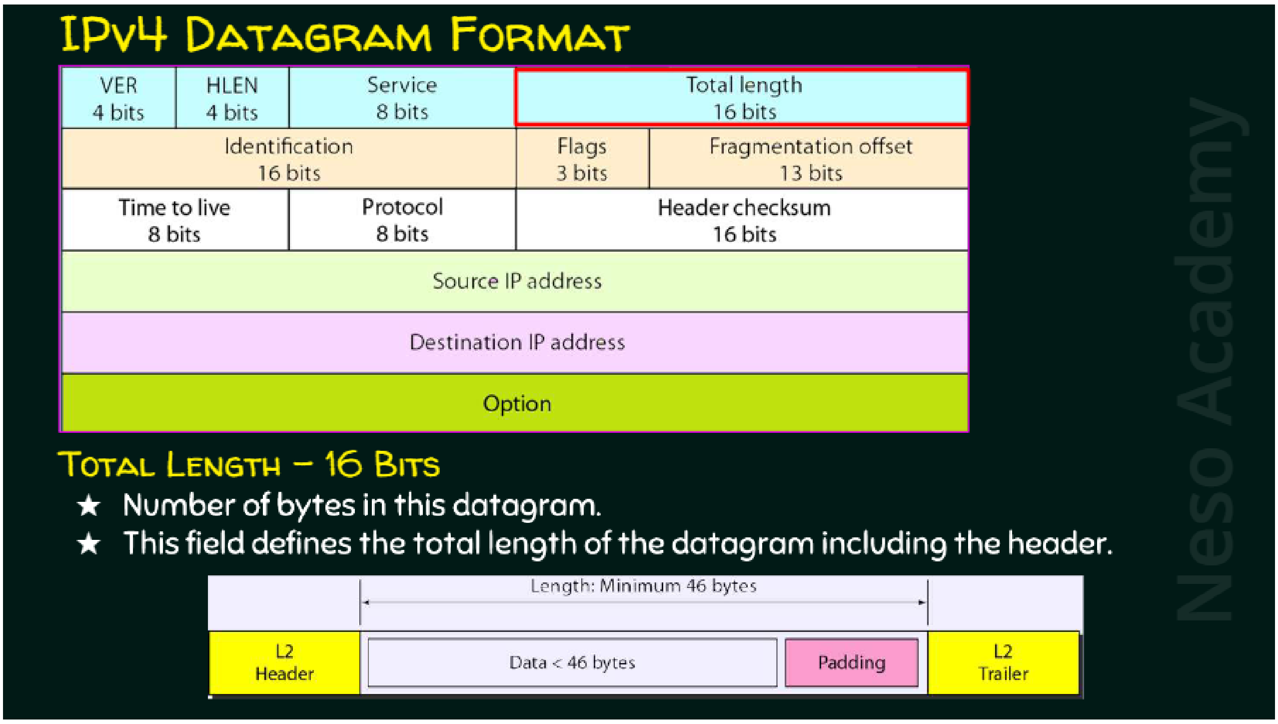
IPv4 Datagram FormatVersion -4 BitsNeso Academy



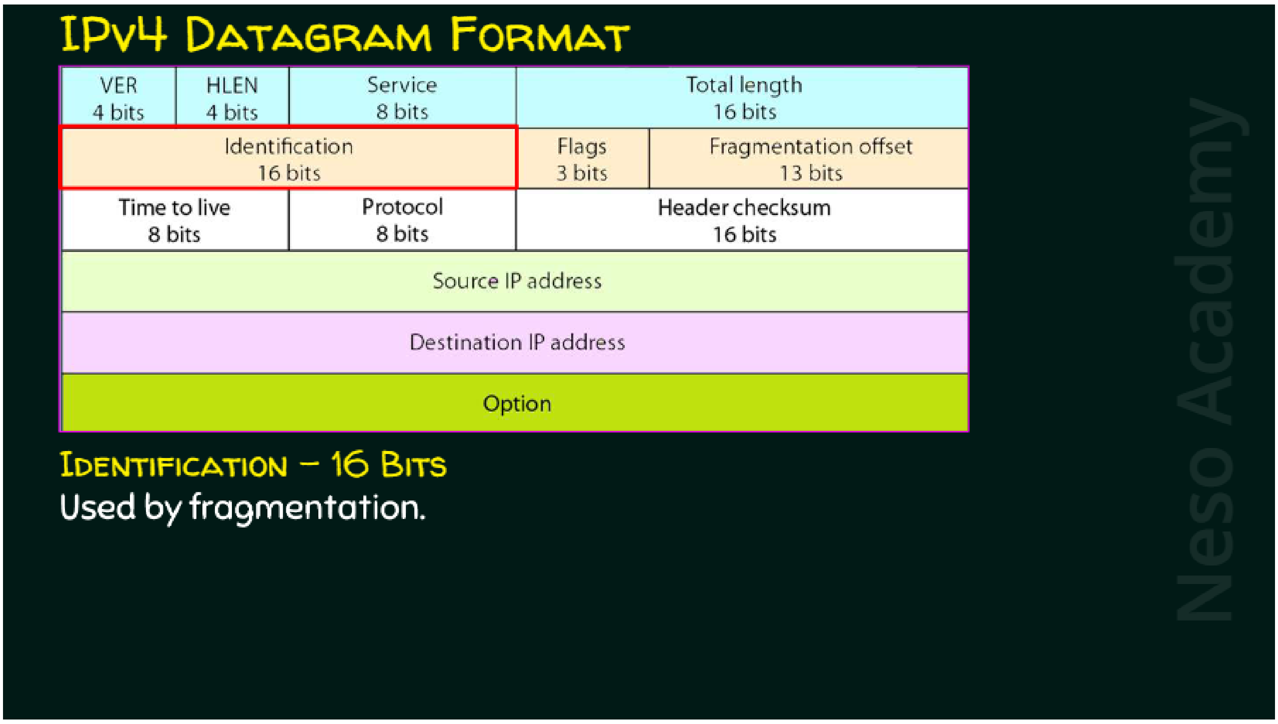
IPv4 Datagram FormatHLEN -4 Bits★★Neso Academy



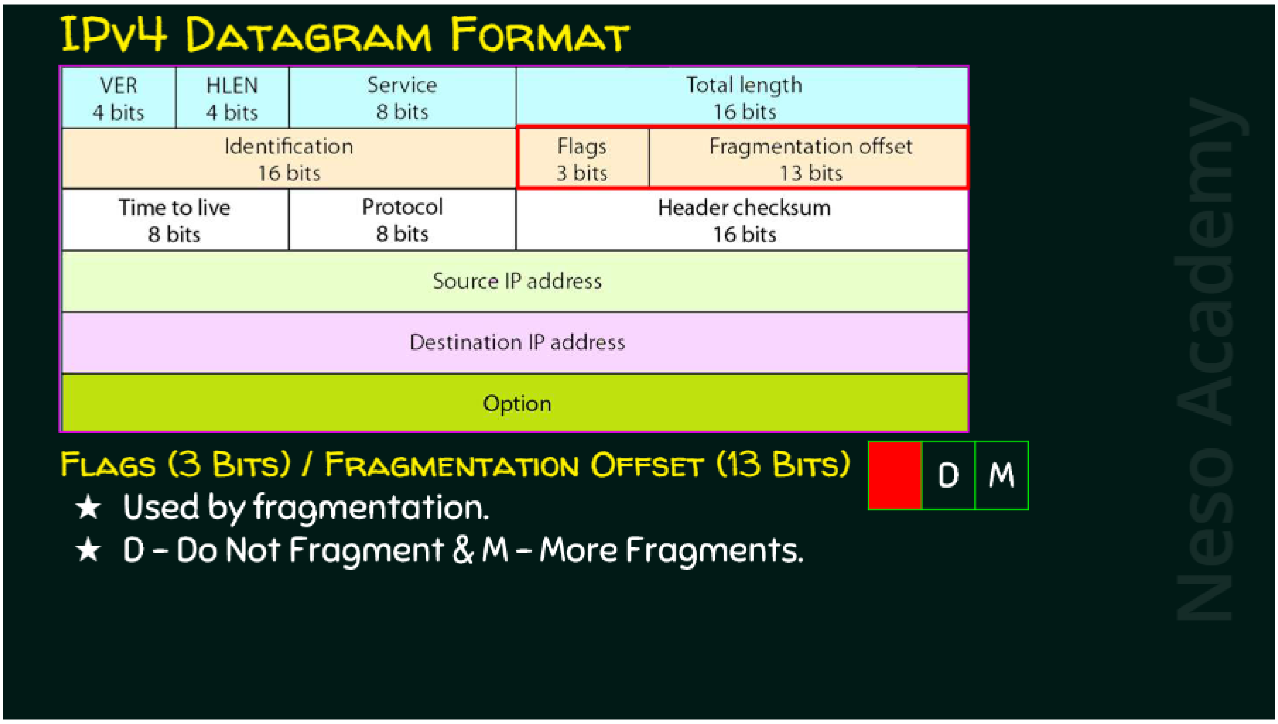
IPv4 Datagram FormatService -8 Bits★★Neso Academy



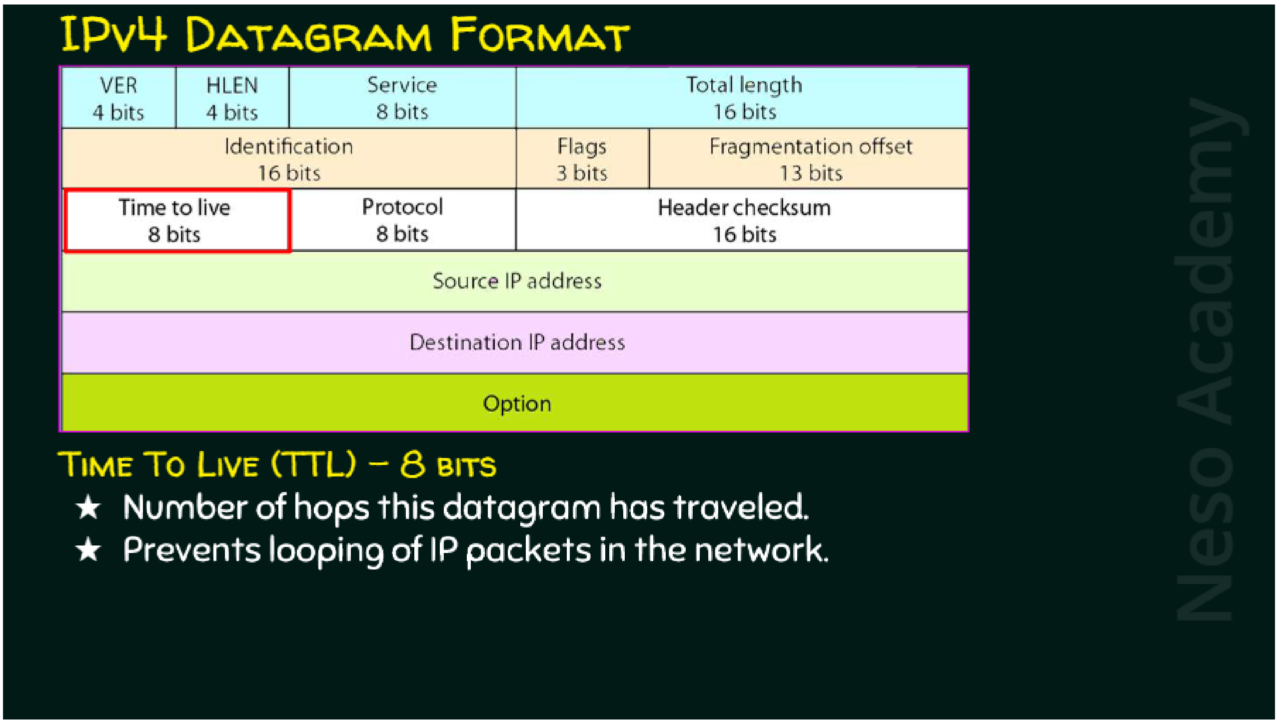
IPv4 Datagram FormatTotal Length -16 Bits★★Neso Academy



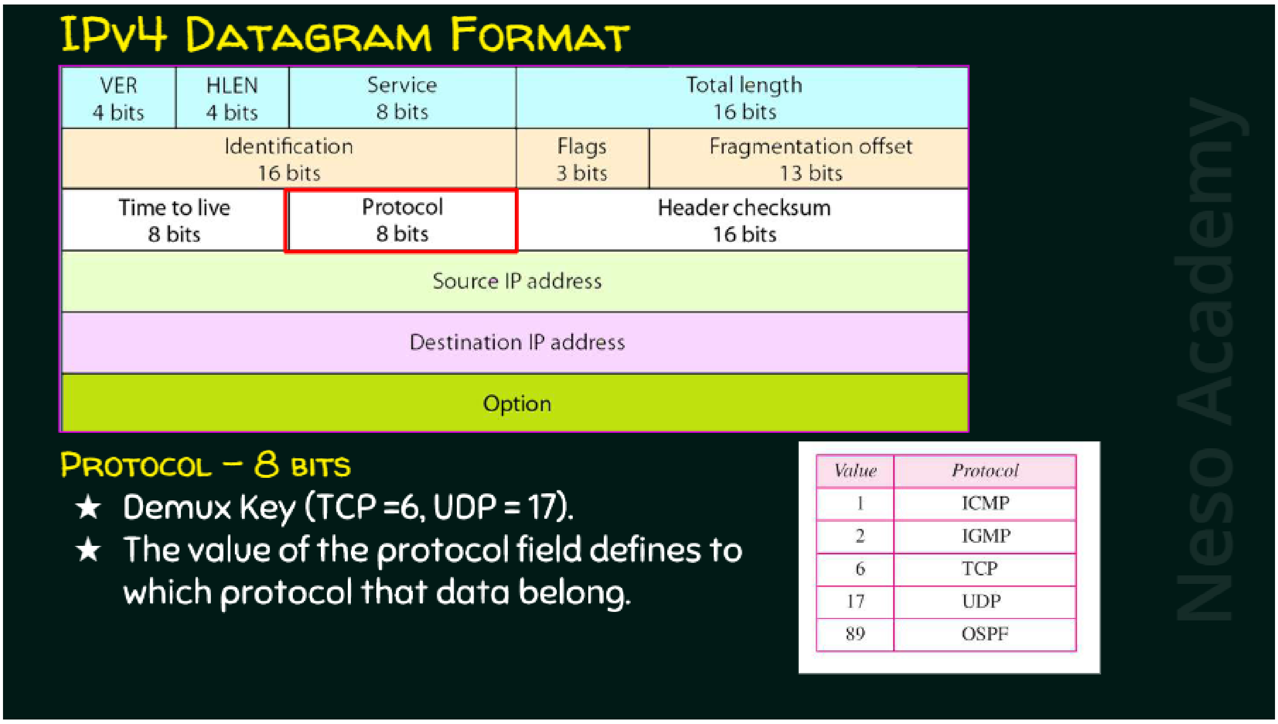
IPv4 Datagram FormatIdentification -16 BitsNeso Academy



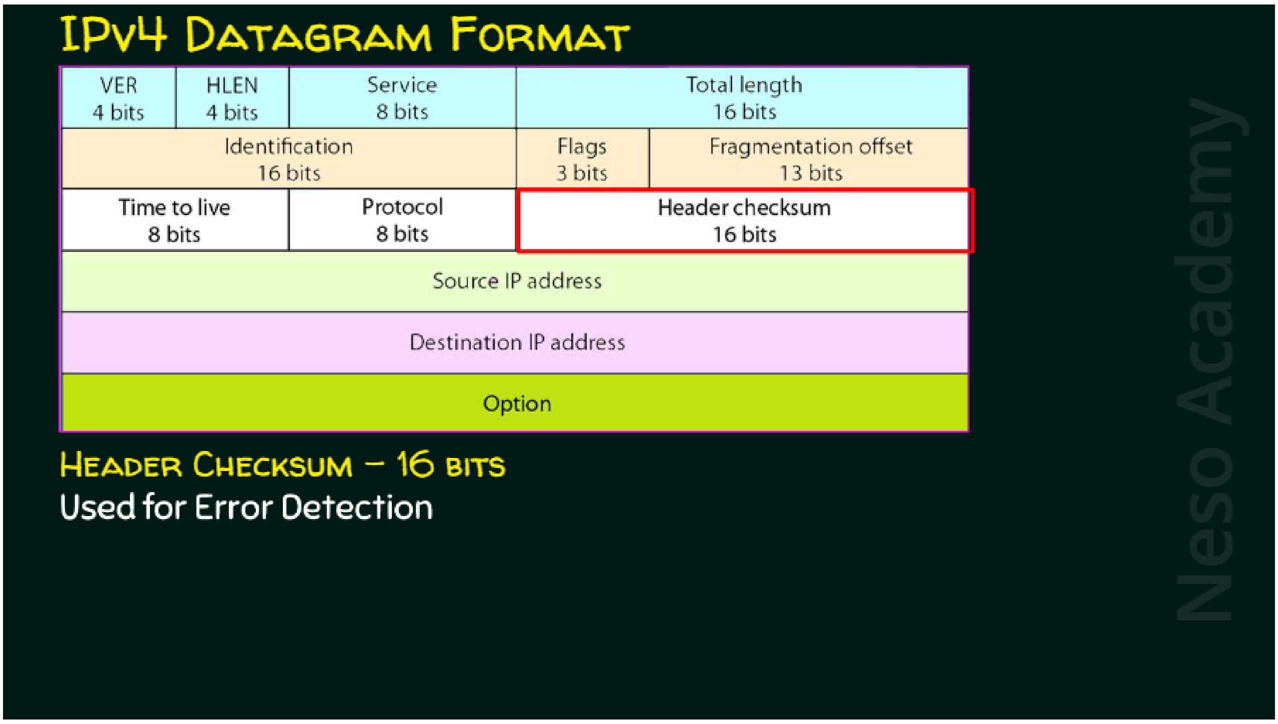
IPv4 Datagram FormatFlags (3 Bits) / Fragmentation Offset (13 Bits)★★Neso Academy



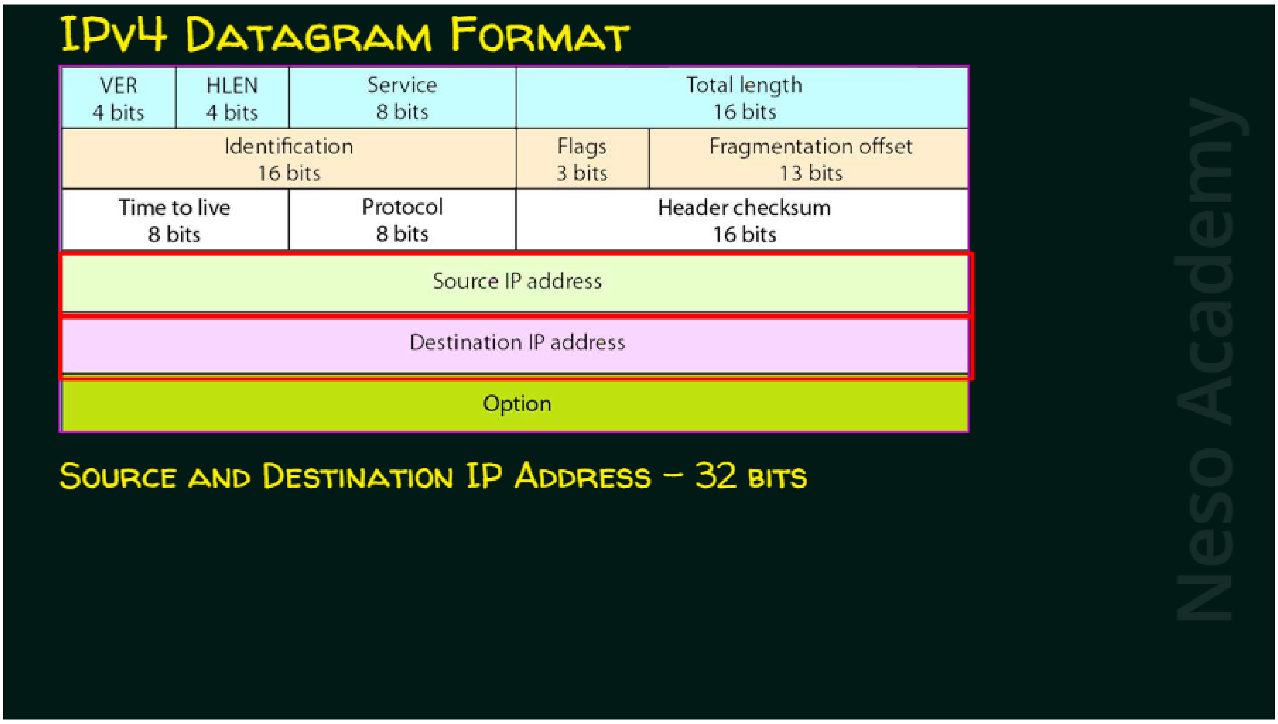
IPv4 Datagram FormatTime To Live (TTL) -8 bits★★Neso Academy



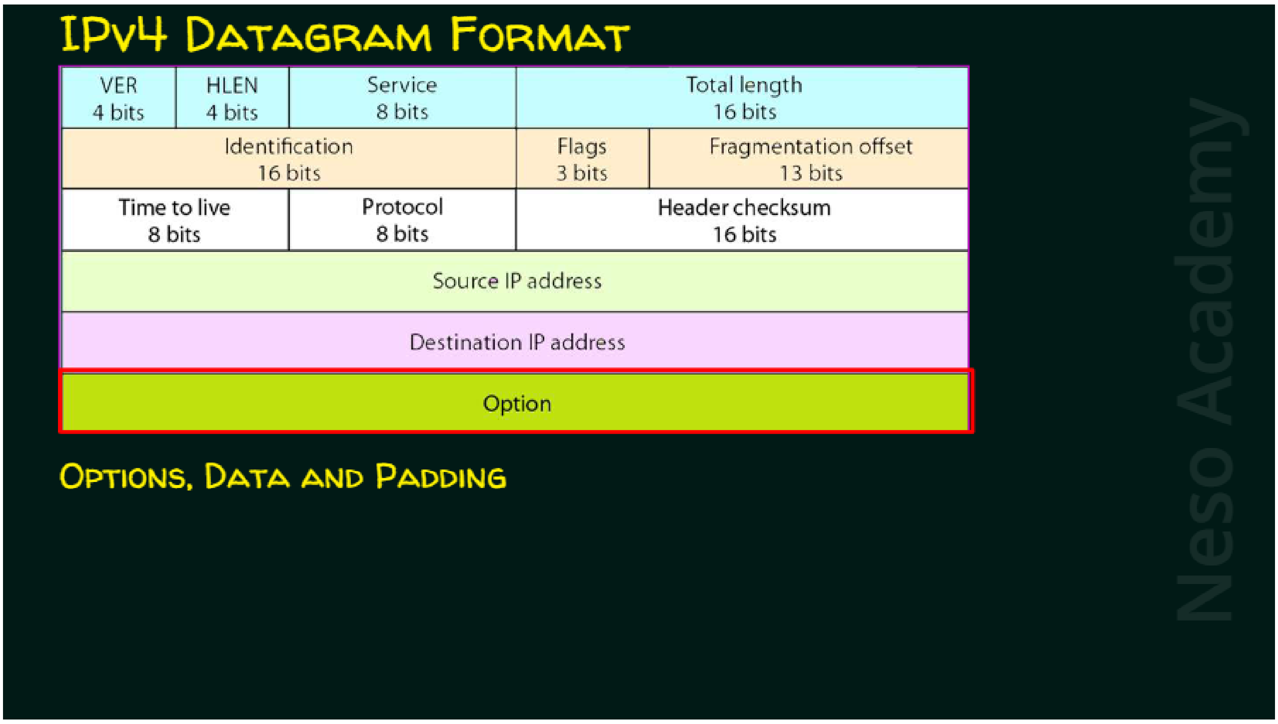
IPv4 Datagram FormatProtocol -8 bits★★Neso Academy



IPv4 Datagram FormatHeader Checksum -16 bitsNeso Academy



IPv4 Datagram FormatSource and Destination IP Address -32 bitsNeso Academy



IPv4 Datagram FormatOptions, Data and PaddingNeso Academy

Question

An IPv4 packet has arrived with the first 8 bits as shown: 01000010. The receiver discards the packet. Why?

QuestionNeso Academy

Solution

Given: The first 8 bits of IP Packet is 01000010

0100 → VERSION

0010 → HLEN

SolutionNeso Academy

Solution

Given: The first 8 bits of IP Packet is 01000010

There is an error in this IP packet.

The first 4 bits i.e. leftmost bits (0100) show the version, which is correct.

The next 4 bits (0010) show an invalid header length ($2 \times 4 = 8$).

The minimum number of bytes in the header must be 20.

The packet has been corrupted in transmission.

SolutionNeso Academy

Question

In an IPv4 packet, the value of HLEN is 1000 in binary. How many bytes of options are being carried by this packet?

QuestionNeso Academy

Solution

Given: HLEN is 1000

Convert the HLEN from binary to decimal: 8

HLEN = 8 means the total number of bytes in the header is 8 × 4 = 32 bytes.

The minimum number of bytes in the header must be 20.

Therefore, the first 20 bytes are the base header.

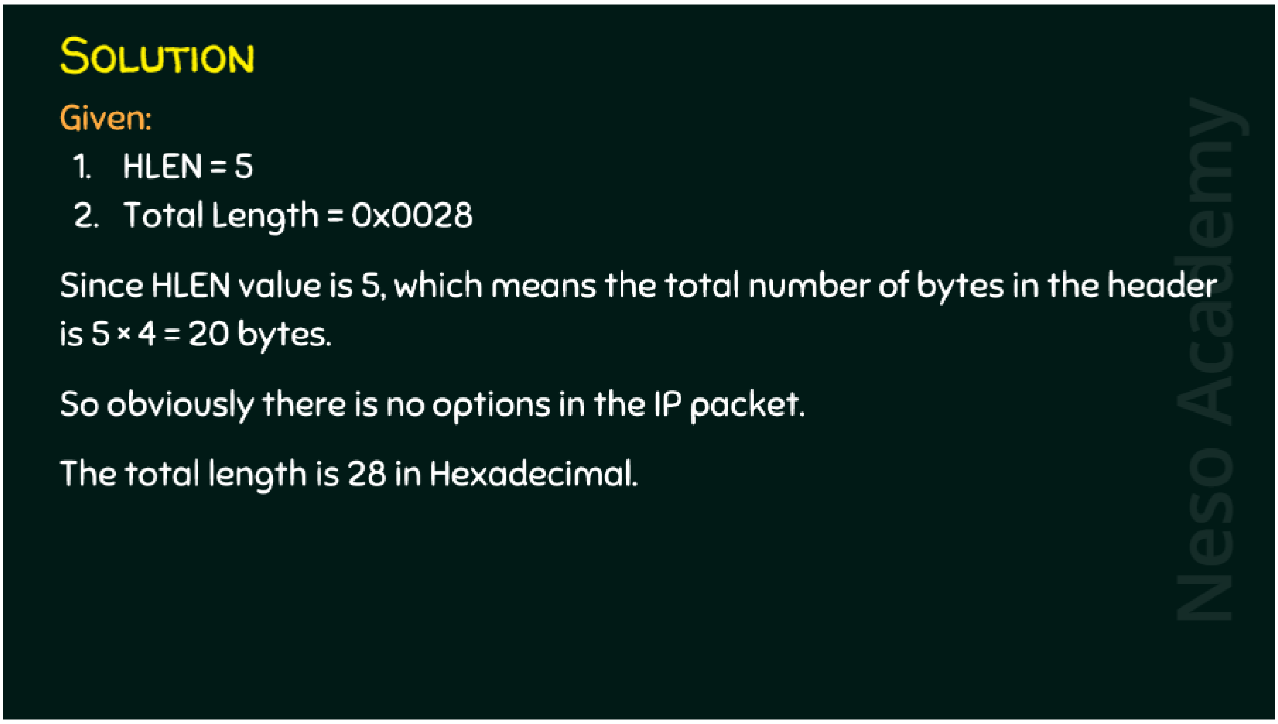
So obviously the next 12 bytes are the options.

SolutionNeso Academy

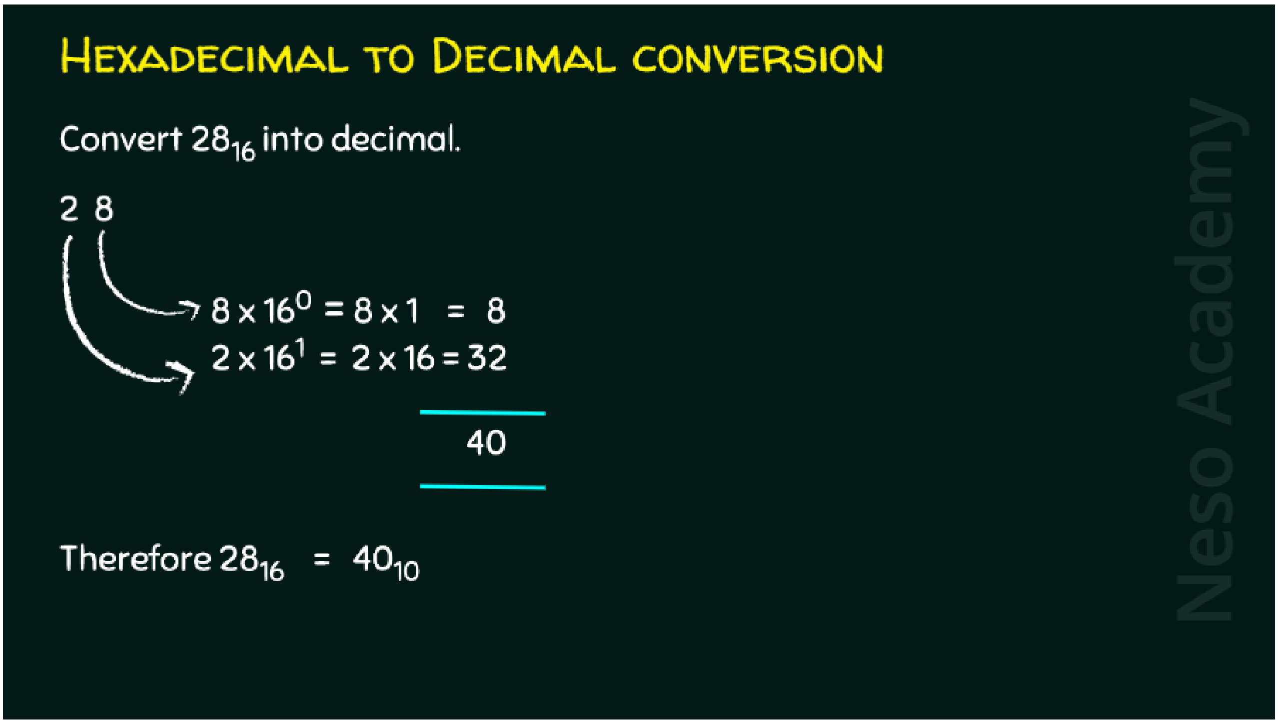
Question

In an IPv4 packet, the value of HLEN is 5, and the value of the total length field is 0x0028. How many bytes of data are being carried by this packet?

QuestionNeso Academy



SolutionNeso Academy



Hexadecimal to Decimal conversionNeso Academy

Solution

Given:

1. HLEN = 5
2. Total Length = 0x0028

Since HLEN value is 5, which means the total number of bytes in the header is 5 × 4 = 20 bytes.

So obviously there is no options in the IP packet.

The total length is 28 in Hexadecimal. In decimal it is 40 bytes.

This means the packet is carrying 20 bytes of data + 20 bytes header.

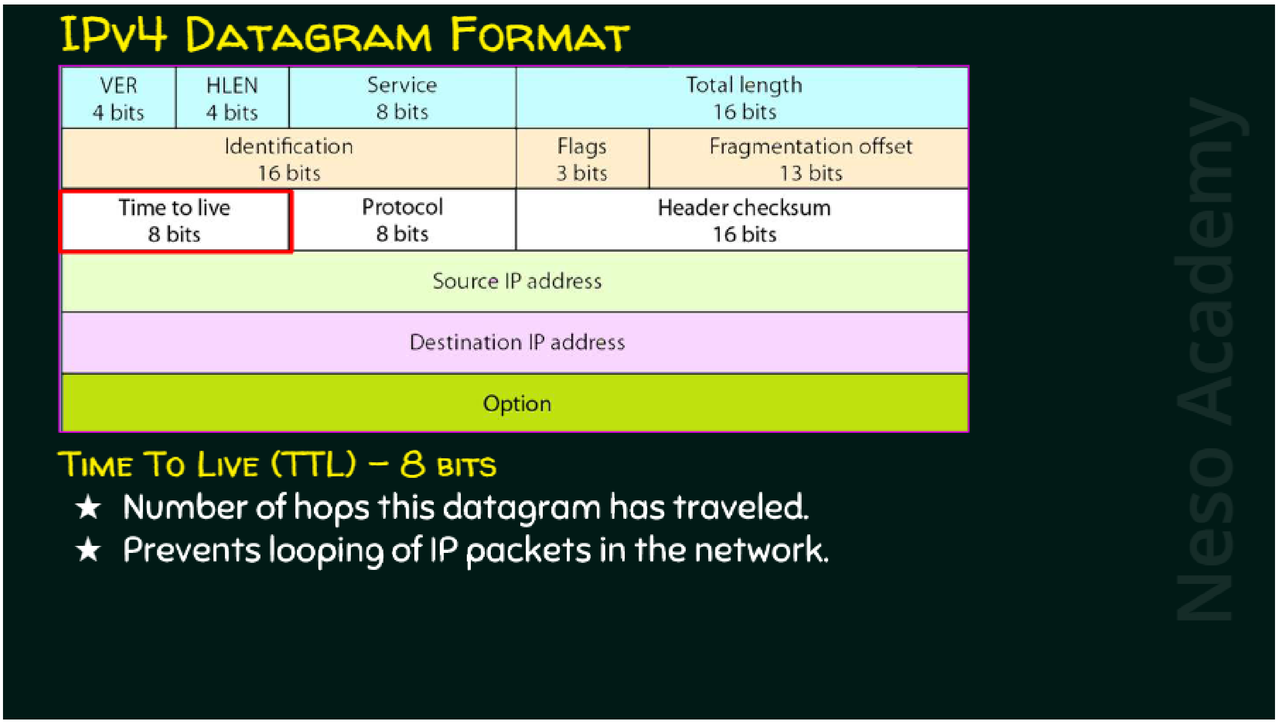
SolutionNeso Academy

Outcomes

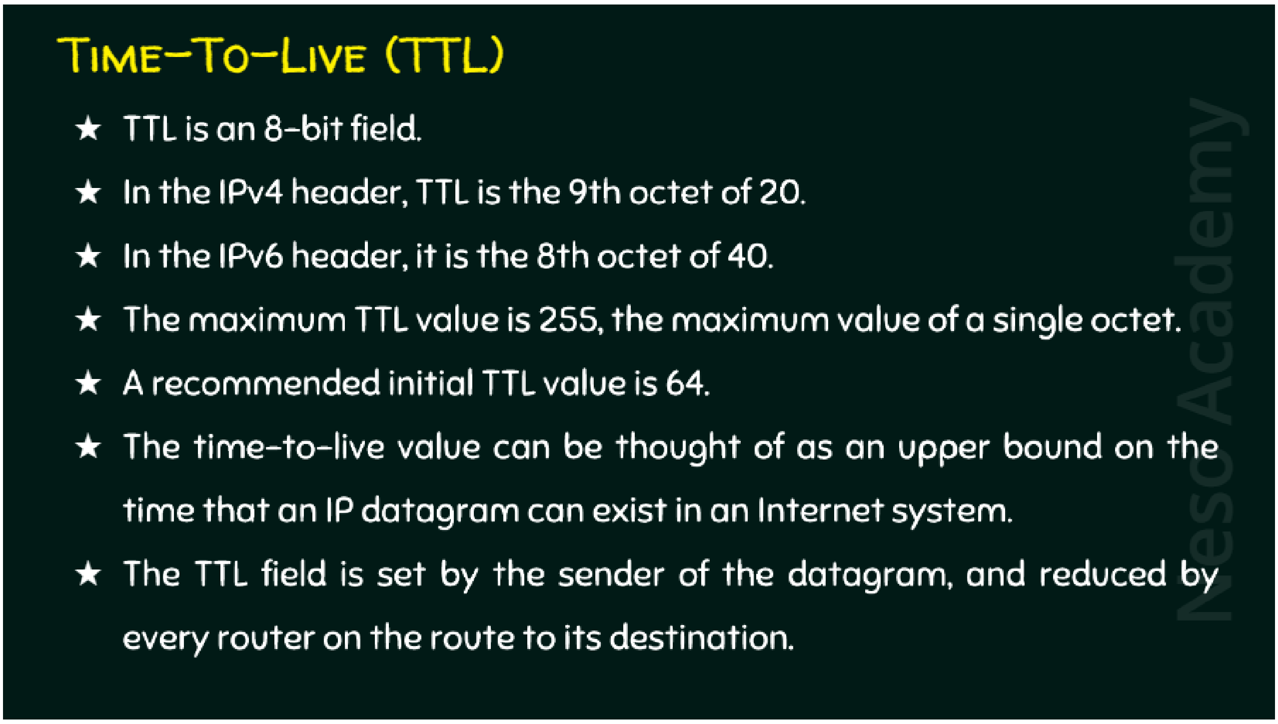
Upon the completion of this session, the learner will be able to

★ Understand the TTL field in IPv4 both theoretically and practically using Cisco Packet Tracer.

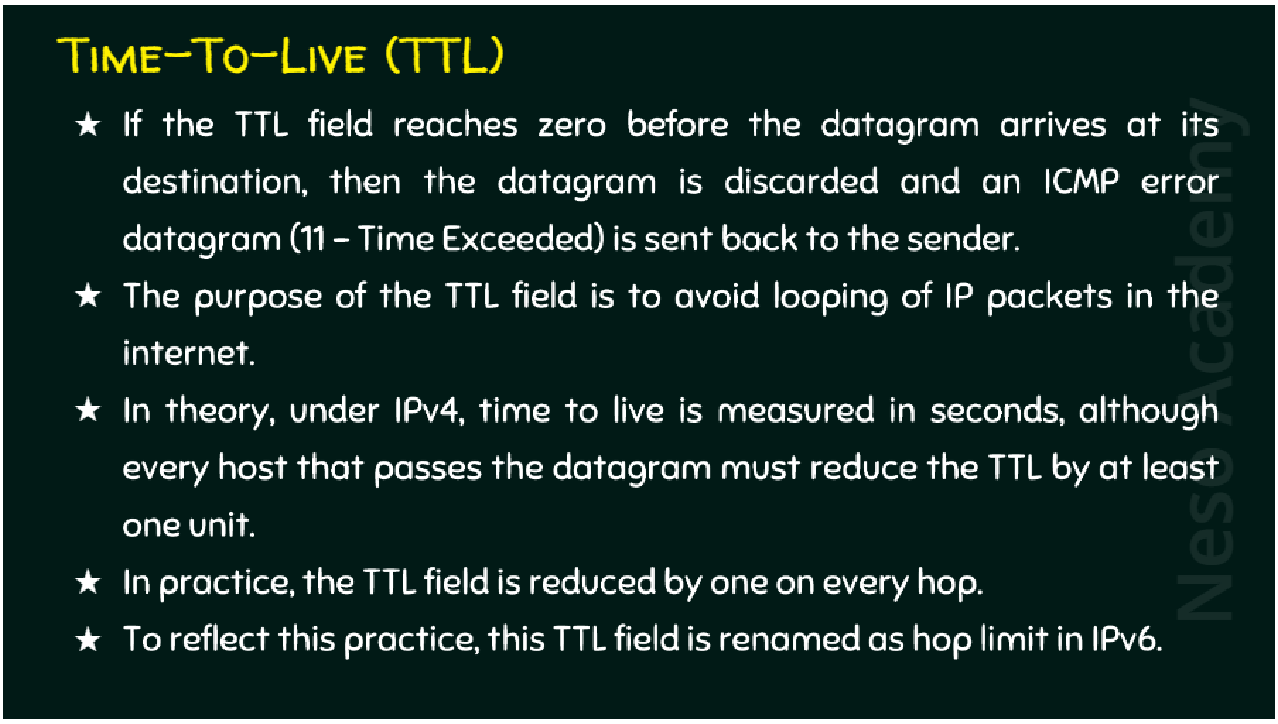
★OutcomesNeso Academy



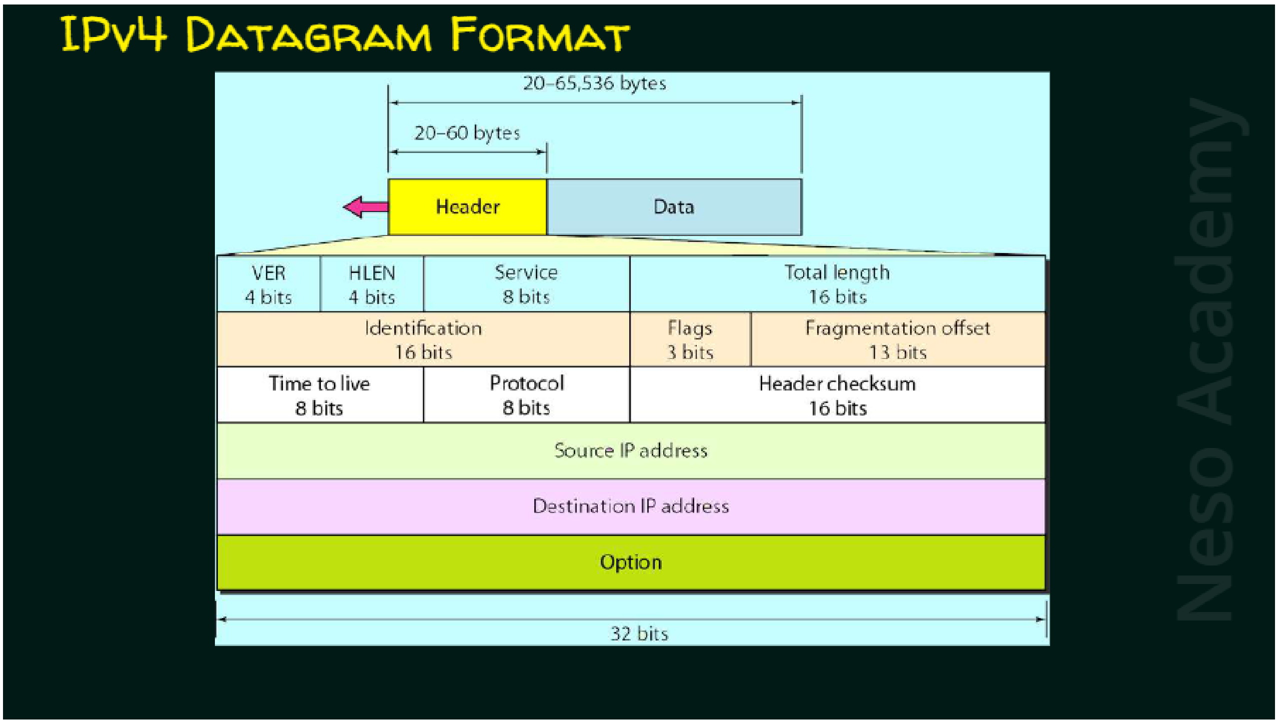
IPv4 Datagram FormatTime To Live (TTL) -8 bits★★Neso Academy



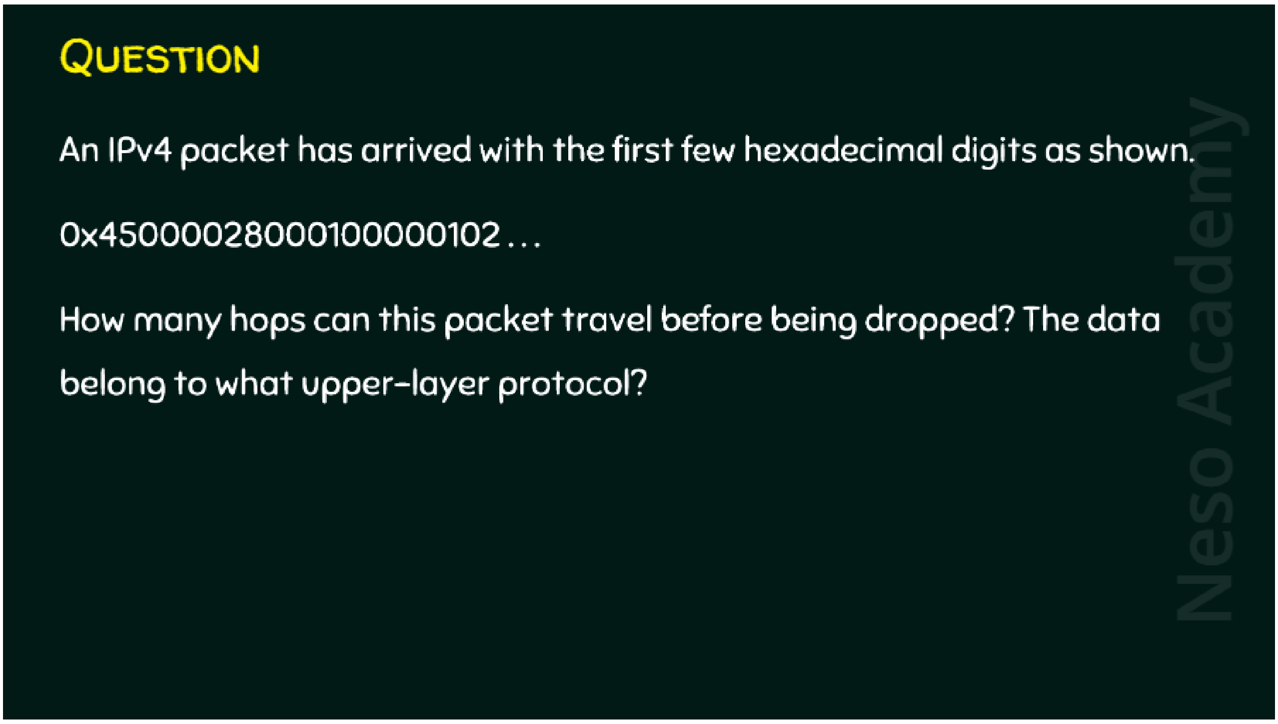
★★★★★★★Time-To-Live (TTL)Neso Academy



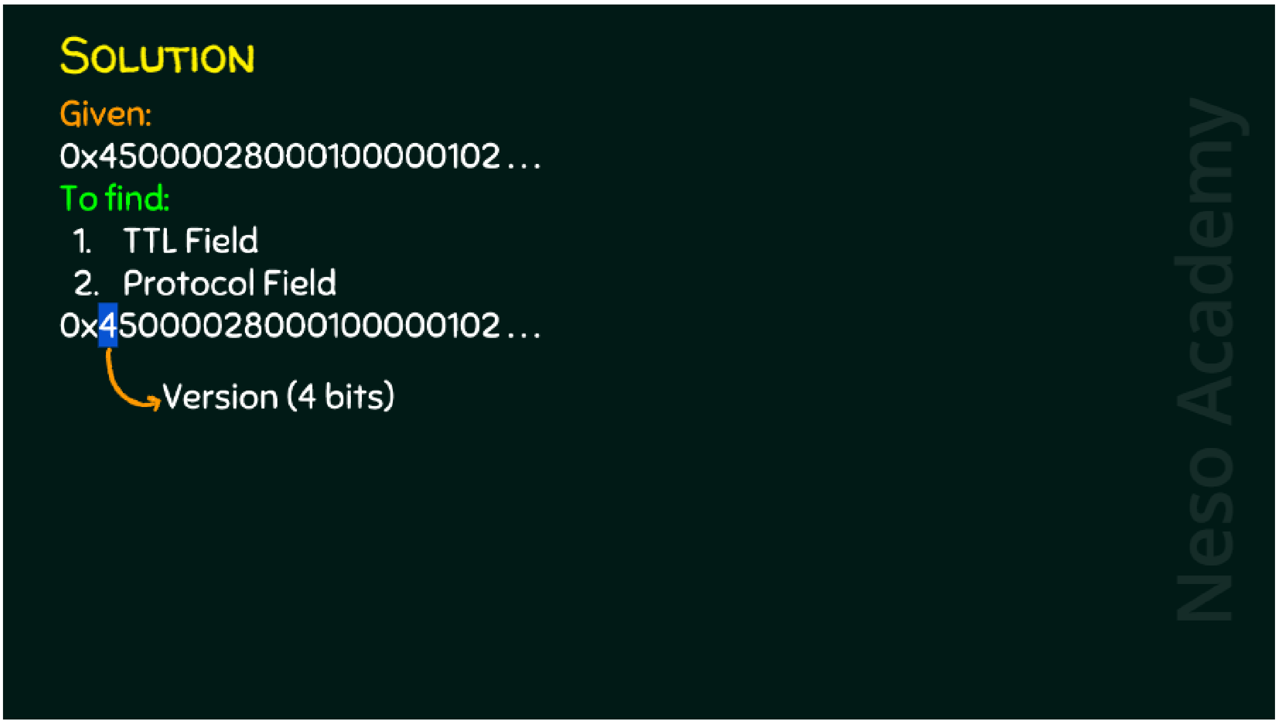
★★★★★Time-To-Live (TTL)Neso Academy



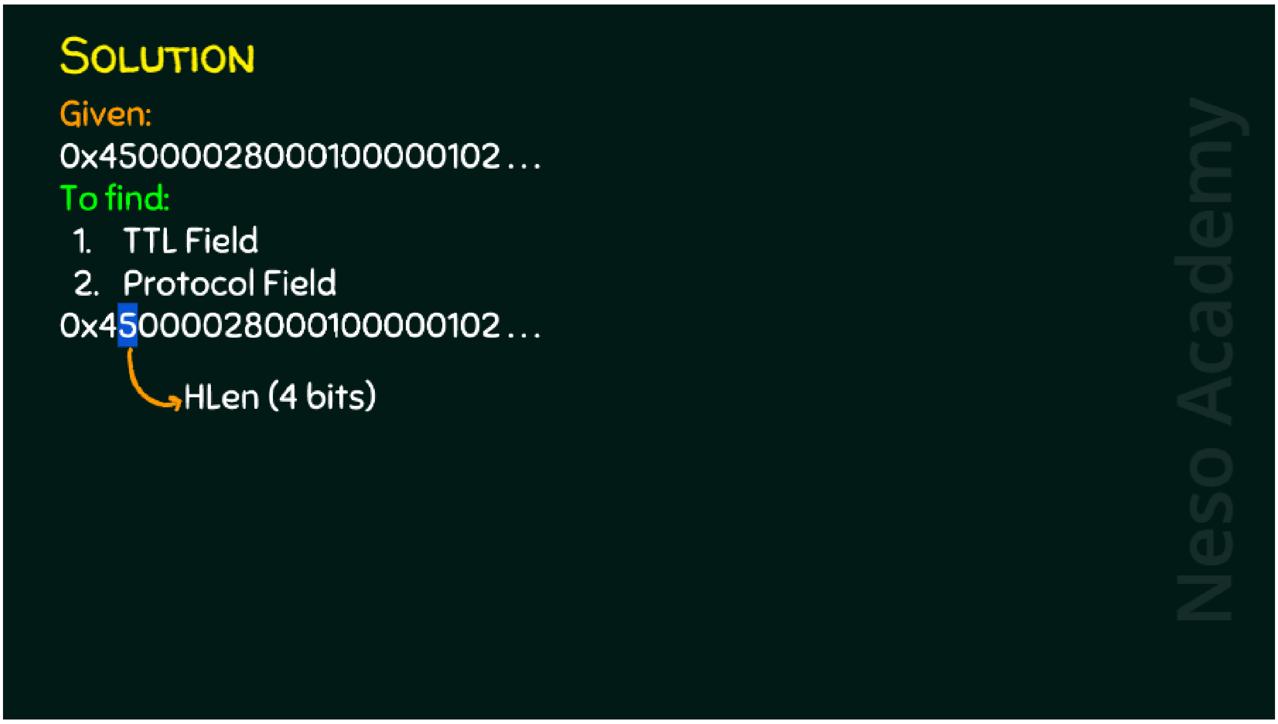
IPv4 Datagram FormatNeso Academy



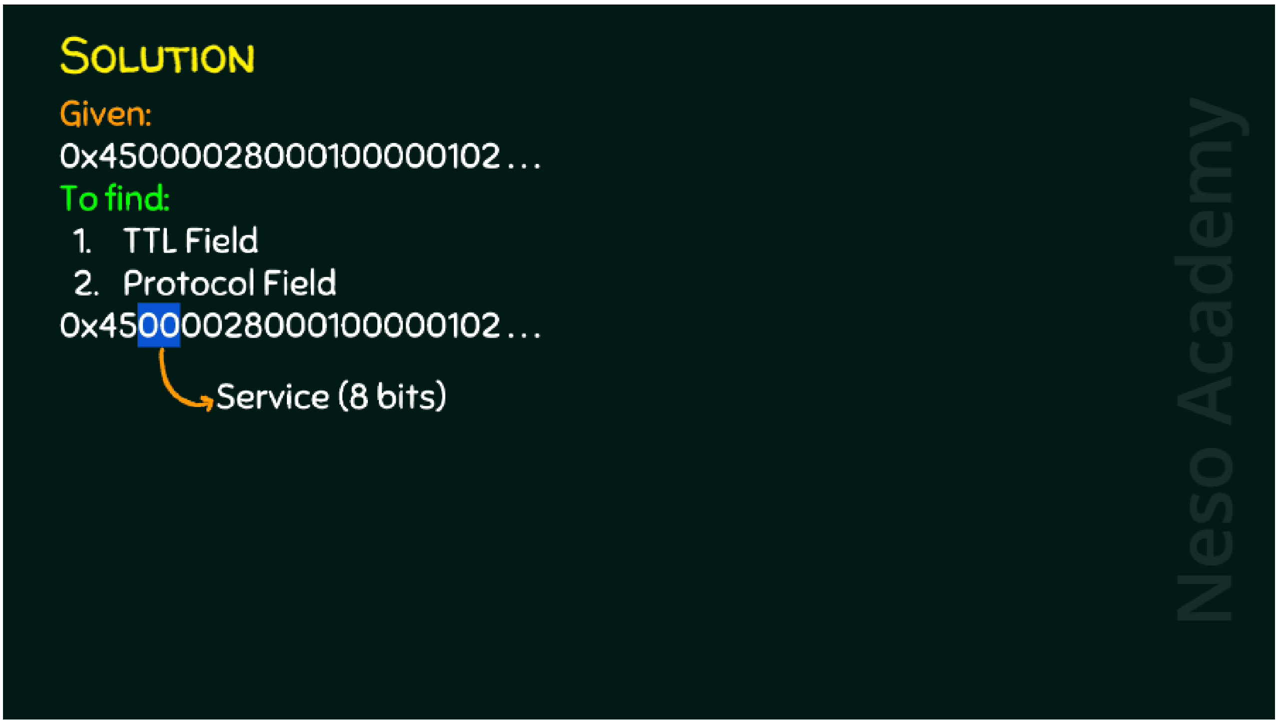
QuestionNeso Academy



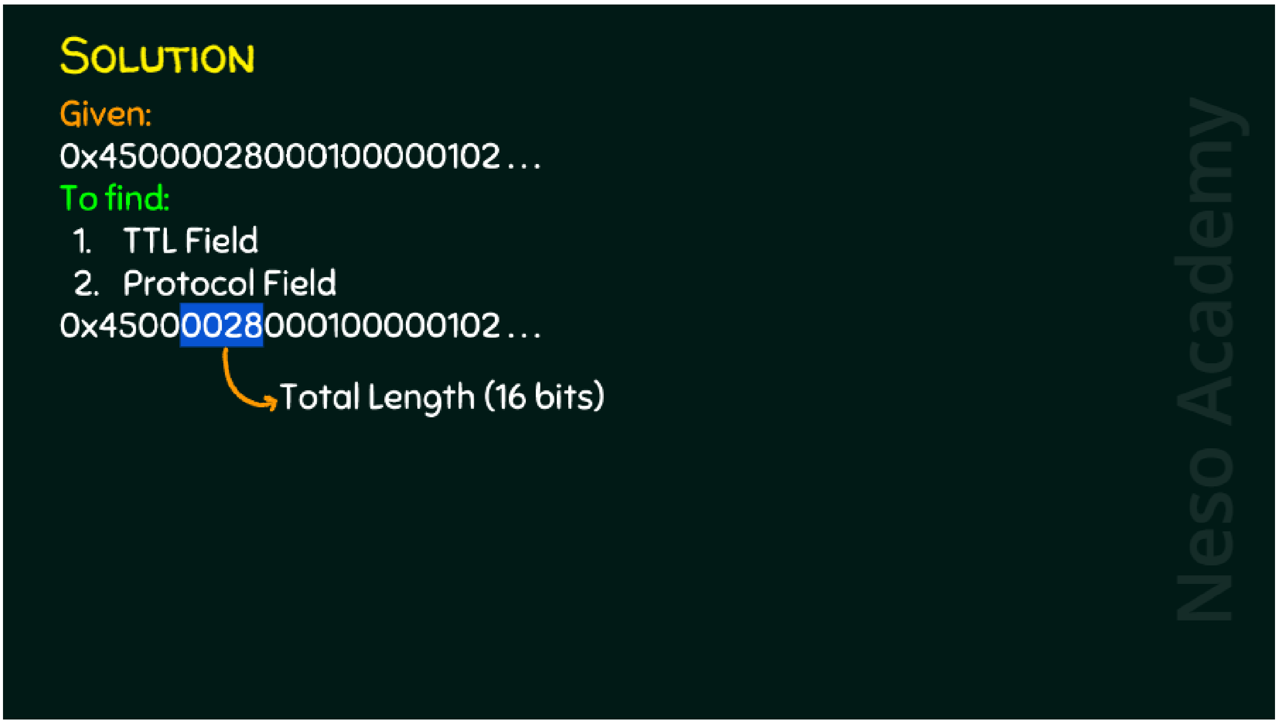
SolutionNeso Academy



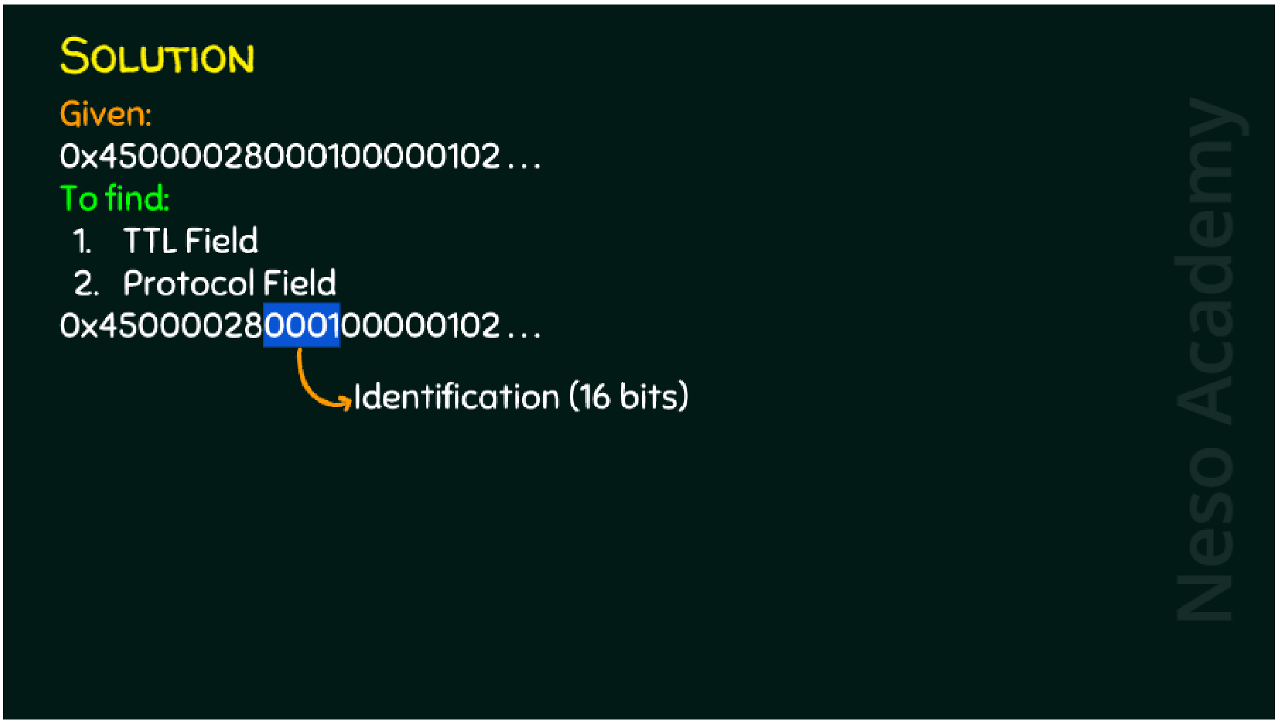
SolutionNeso Academy



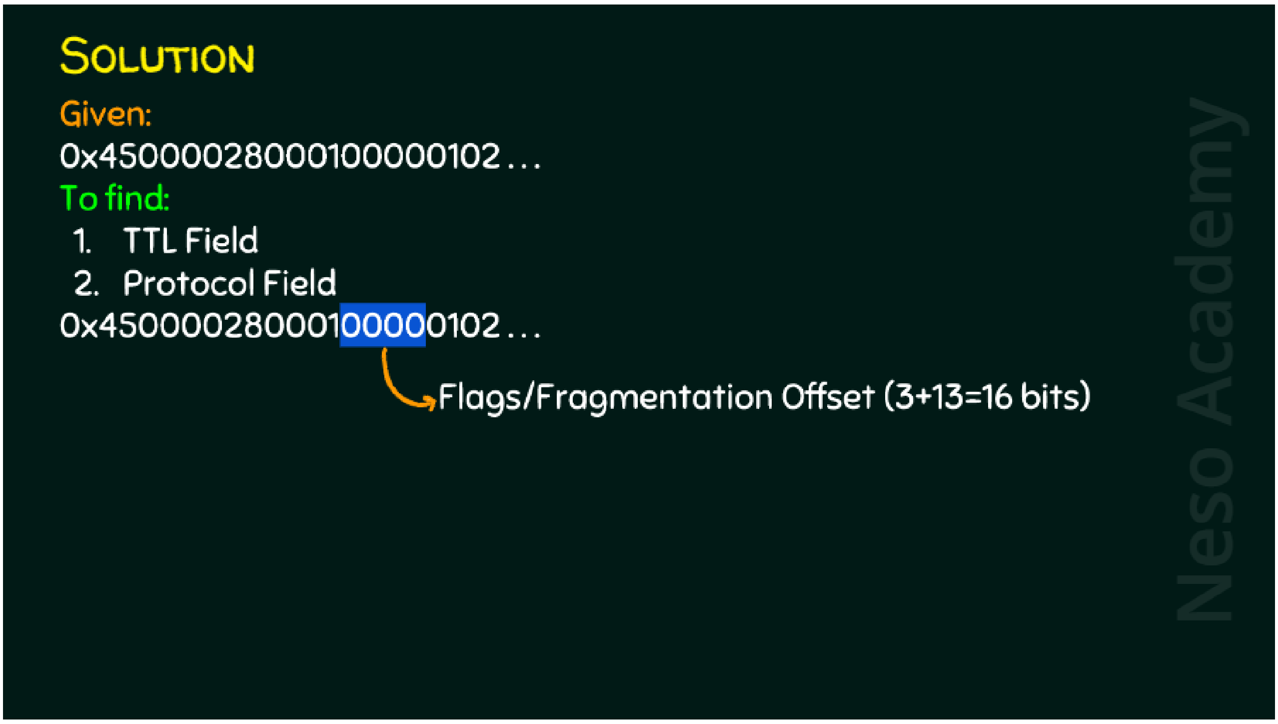
SolutionNeso Academy



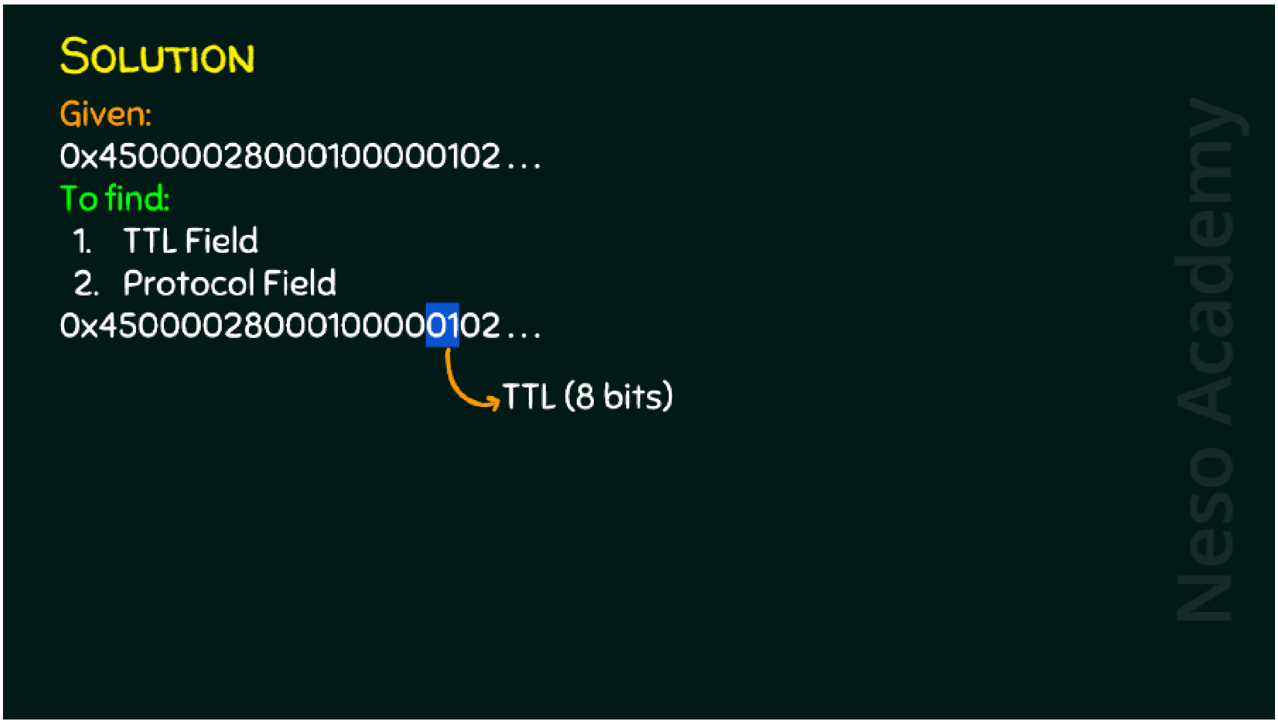
SolutionNeso Academy



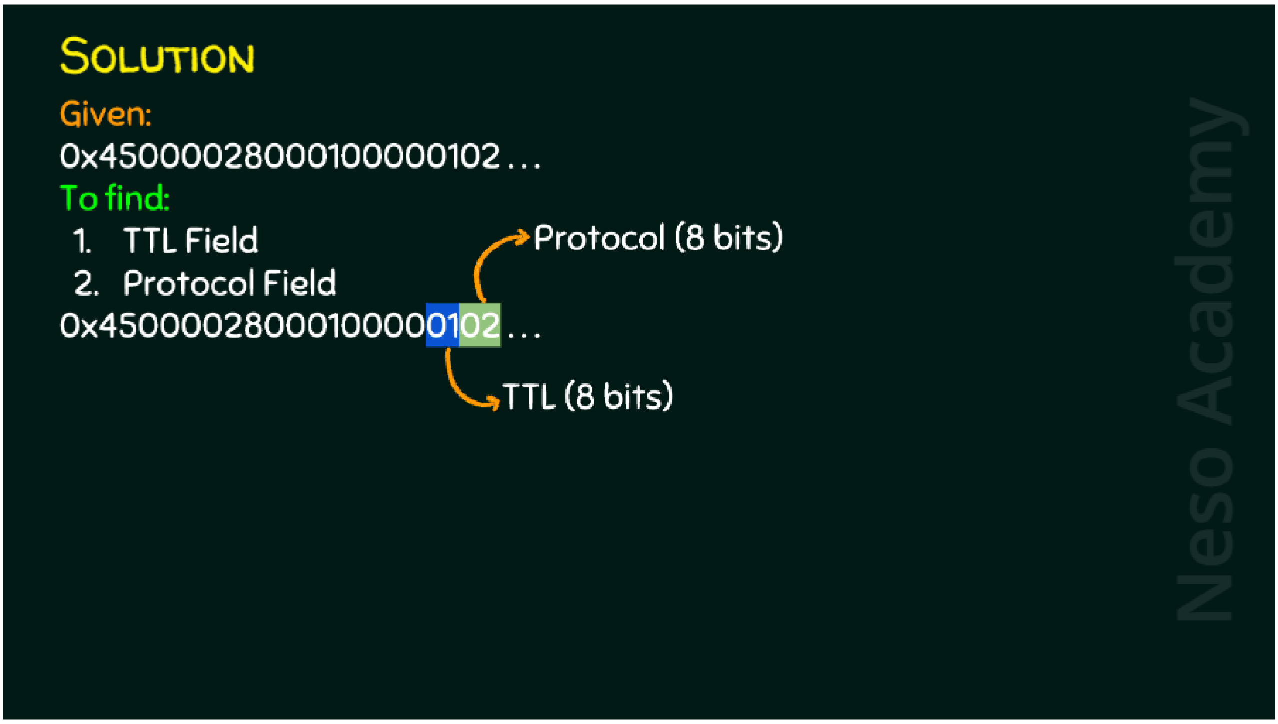
SolutionNeso Academy



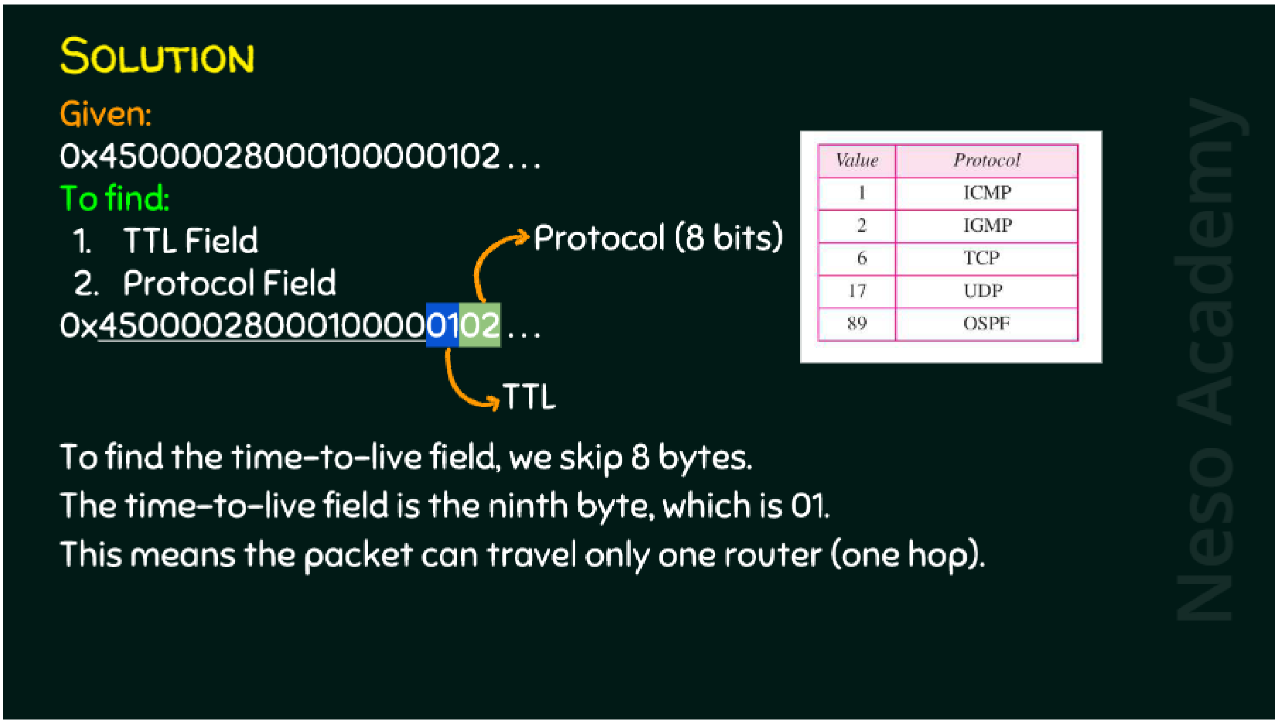
SolutionNeso Academy



SolutionNeso Academy



SolutionNeso Academy



SolutionNeso Academy

Solution

Given:

0x45000028000100000102 . . .

To find:

1. TTL Field
2. Protocol Field

Protocol (8 bits)

0x45000028000100000102 . . .

TTL

To find the time-to-live field, we skip 8 bytes.
The time-to-live field is the ninth byte, which is 01.
This means the packet can travel only one router (one hop).
The protocol field is the next byte (02), which means that the upper-layer protocol is IGMP.

SolutionNeso Academy

Outcomes

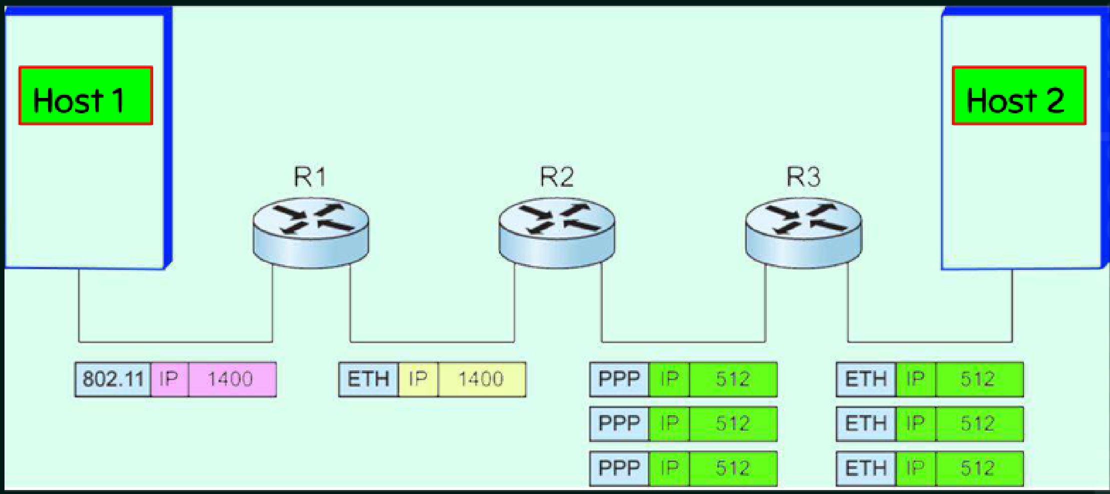
Upon the completion of this lecture, the learner will be able to

★ Understand the need for fragmentation.

★ Know about MTU.

Outcomes★★Neso Academy

Fragmentation



FragmentationNeso Academy

Fragmentation

- ★ A datagram can travel through different networks.
- ★ Each router decapsulates the IPv4 datagram from the frame it receives, processes it, and then encapsulates it in another frame.
- ★ The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled.
- ★ The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel.
- ★ For example, if a router connects a LAN to a WAN, it receives a frame in the LAN format and sends a frame in the WAN format.

Fragmentation★★★★★Neso Academy

Fragmentation

- Each data link layer protocol has its own frame format in most protocols.
- One of the fields defined in the format is the maximum size of the data field.
- In other words, when a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size, which is defined by the restrictions imposed by the hardware and software used in the network.

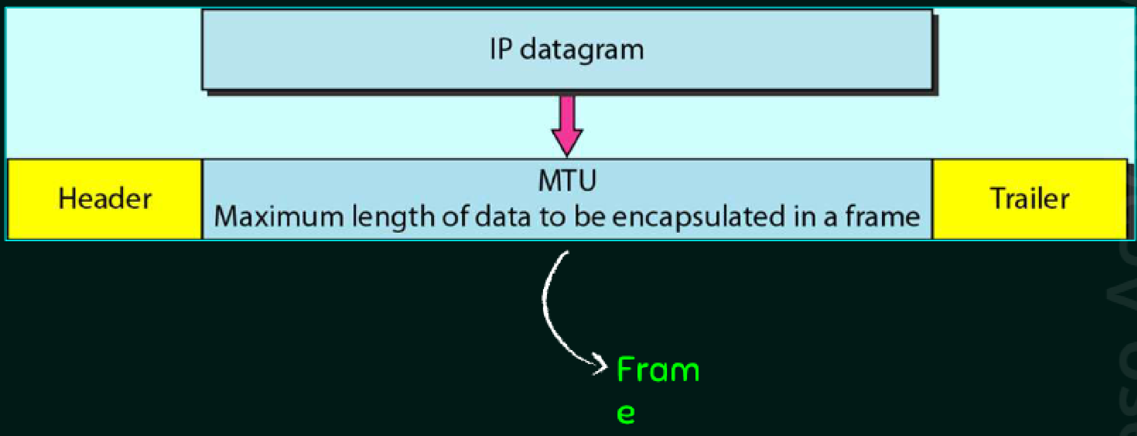
Fragmentation★★★Neso Academy

Fragmentation

- To make the IPv4 protocol independent of the physical network, the designers decided to make the maximum length of the IPv4 datagram equal to 65,535 bytes.
- This makes transmission more efficient if we use a protocol with an MTU of this size.
- However, for other physical networks, we must divide the datagram to make it possible to pass through these networks. This is called fragmentation.
- The source usually does not fragment the IPv4 packet. The transport layer will instead segment the data into a size that can be accommodated by IPv4 and the data link layer in use.

Fragmentation★★★★Neso Academy

Maximum Transfer Unit (MTU)



Maximum Transfer Unit (MTU)Neso Academy

Maximum Transfer Unit (MTU)

The value of the MTU depends on the physical network protocol.

Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

Maximum Transfer Unit (MTU)Neso Academy

FRAGMENTATION

★ When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but with some changed.

★ A fragmented datagram may itself be fragmented if it encounters a network with an even smaller MTU.

★ In other words, a datagram can be fragmented several times before it reaches the final destination.

★ In IPv4, fragmentation can be done by source host or any router. The reassembly is done only at the destination.

★ It is logical to do the reassembly at the final destination.

Fragmentation★★★★★Neso Academy

FRAGMENTATION

★ When a datagram is fragmented, required parts of the header must be copied by all fragments.

★ The host or router that fragments a datagram must change the values of three fields:

- Flags,
- Fragmentation offset and
- Total length.

★ The rest of the fields must be copied.

★ Of course, the value of the checksum must be recalculated regardless of fragmentation.

Fragmentation★★○○○★★Neso Academy

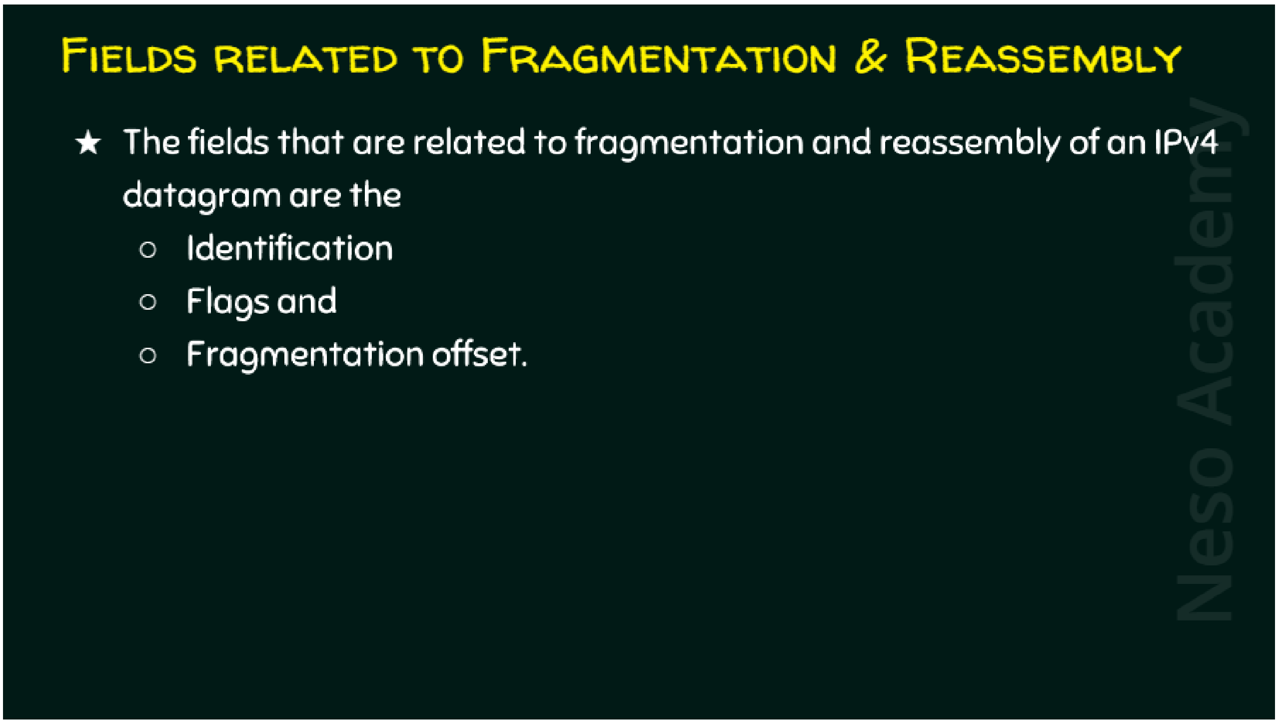
Outcomes

Upon the completion of this lecture, the learner will be able to

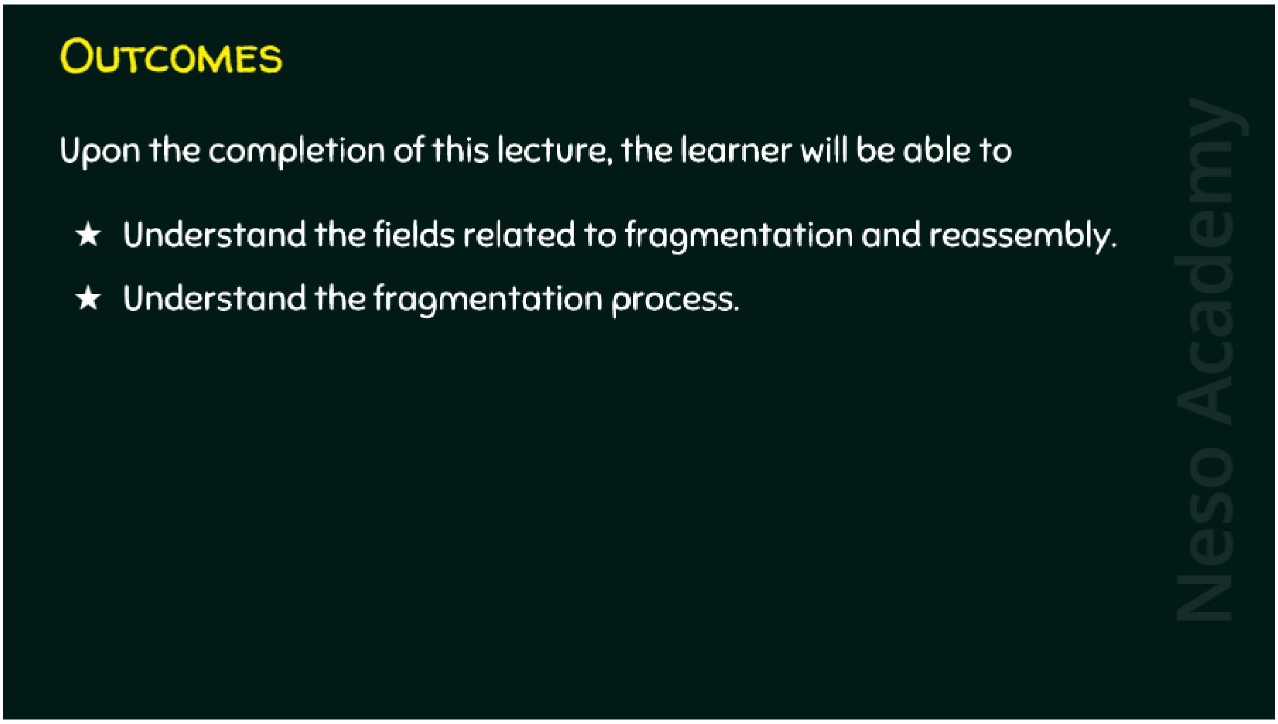
★ Understand the fields related to fragmentation and reassembly with the help of an analogy.

Outcomes★Neso Academy

Analogy!12 L14 L5 LNeso Academy



Fields related to Fragmentation & Reassembly★○○○Neso Academy



Outcomes★★Neso Academy

Fields related to Fragmentation & Reassembly

★ The fields that are related to fragmentation and reassembly of an IPv4 datagram are the
  - Identification
  - Flags and
  - Fragmentation offset.

Fields related to Fragmentation & Reassembly★○○○Neso Academy

1. Identification

★ This 16-bit field identifies a datagram originating from the source host.

★ The combination of the identification and source IPv4 address must uniquely define a datagram as it leaves the source host.

★ To guarantee uniqueness, the IPv4 protocol uses a counter to label the datagrams.

★ The counter is initialized to a positive number.

★ When the IPv4 protocol sends a datagram, it copies the current value of the counter to the identification field and increments the counter by 1.

1.Identification★★★★★Neso Academy

1. Identification

- ★ As long as the counter is kept in the main memory, uniqueness is guaranteed.
- ★ When a datagram is fragmented, the value in the identification field is copied to all fragments.
- ★ In other words, all fragments have the same identification number, the same as the original datagram.
- ★ The identification number helps the destination in reassembling the datagram.
- ★ It knows that all fragments having the same identification value must be assembled into one datagram.

1.Identification★★★★★Neso Academy

2. Flags

	D	M

- ★ This is a 3-bit field. The first bit is reserved.
- ★ The second bit is called the do not fragment bit.
- ★ If its value is 1, the machine must not fragment the datagram.
- ★ If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host.
- ★ If its value is 0, the datagram can be fragmented if necessary.
- ★ The third bit is called the more fragment bit.
- ★ If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one.
- ★ If its value is 0, it means this is the last or only fragment.

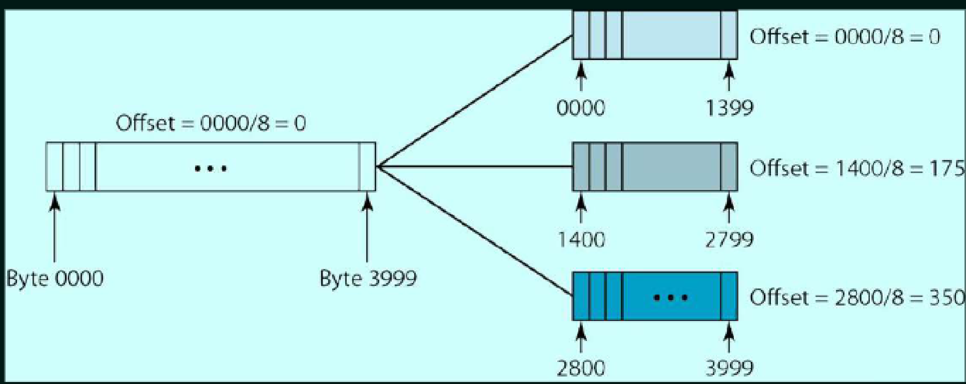
2. Flags★★★★★★★★Neso Academy

3. Fragmentation Offset

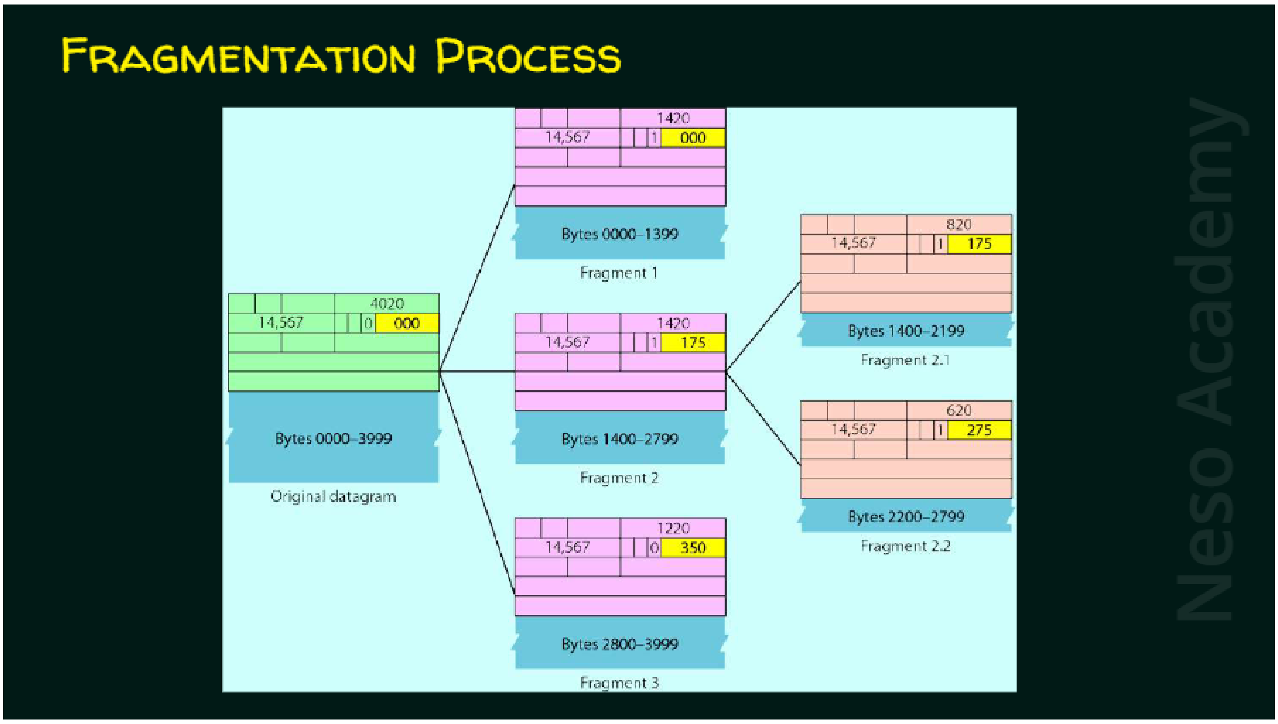
- ★ This 13-bit field shows the relative position of this fragment with respect to the whole datagram.
- ★ It is the offset of the data in the original datagram measured in units of 8 bytes.
- ★ This is done because the length of the offset field is only 13 bits and cannot represent a sequence of bytes greater than 8191.
- ★ This forces hosts or routers that fragment datagrams to choose a fragment size so that the first byte number is divisible by 8.

3. Fragmentation Offset★★★★Neso Academy

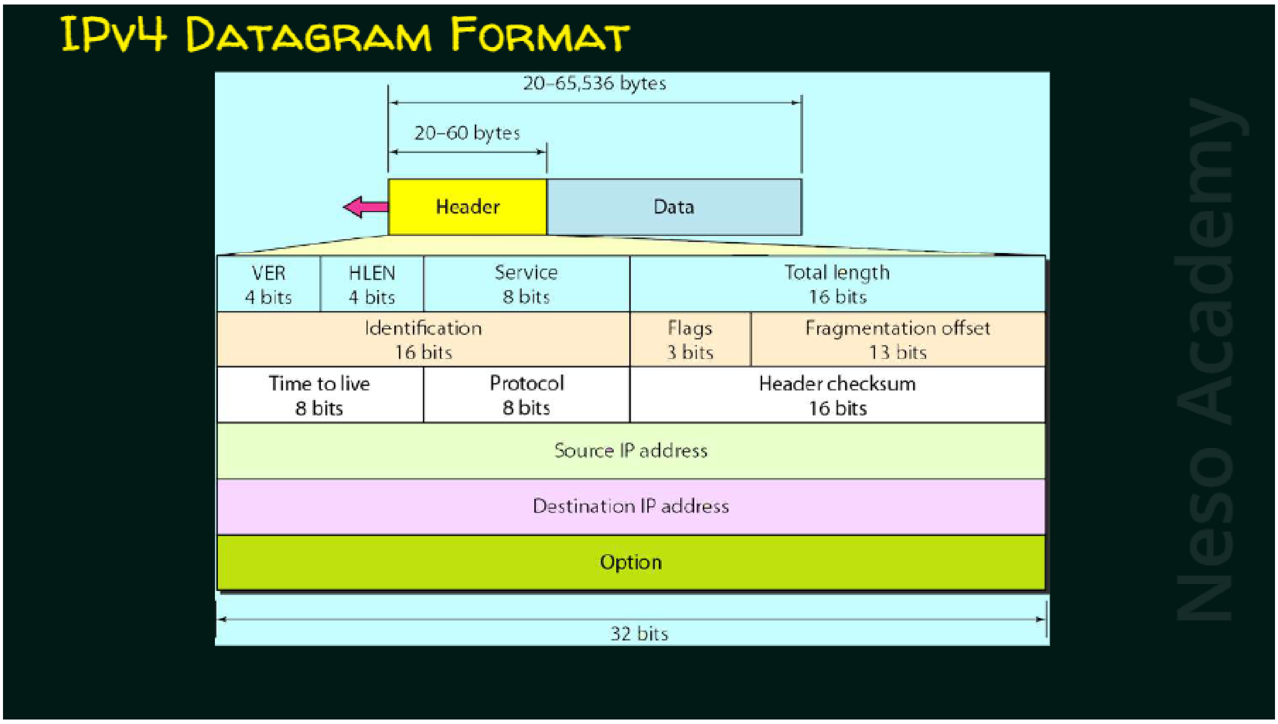
Fragmentation Process



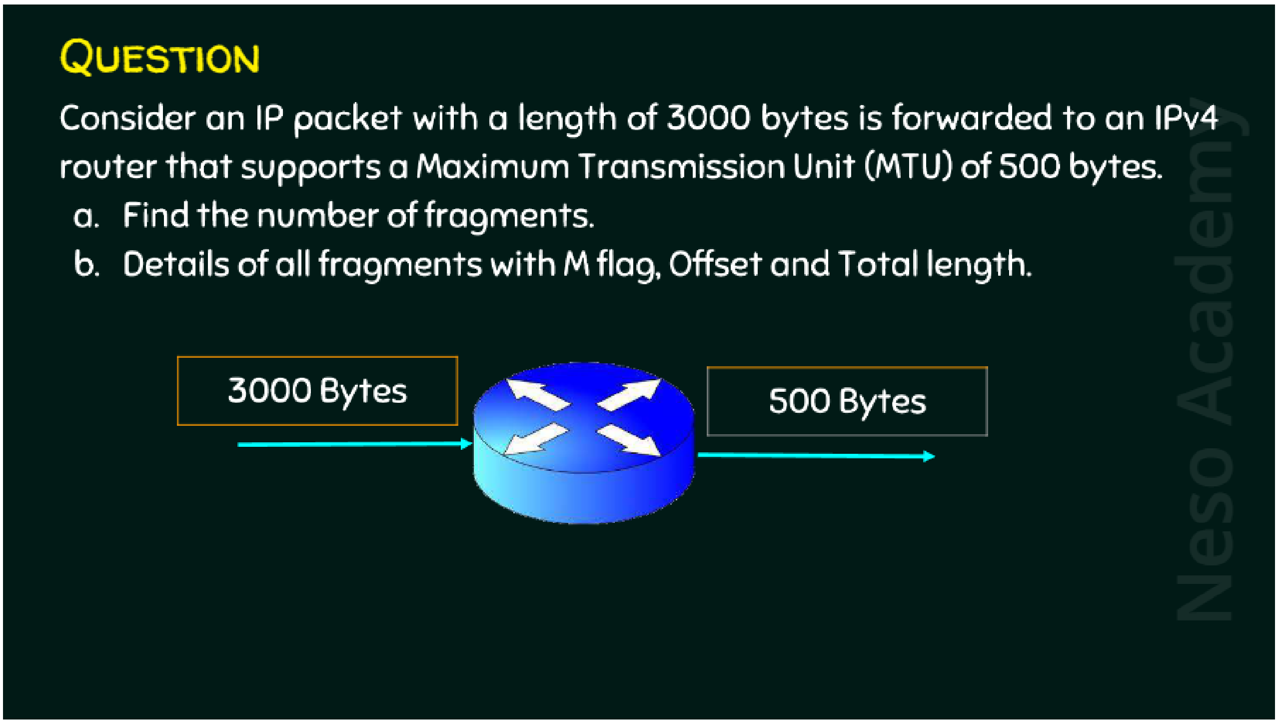
Fragmentation ProcessNeso Academy



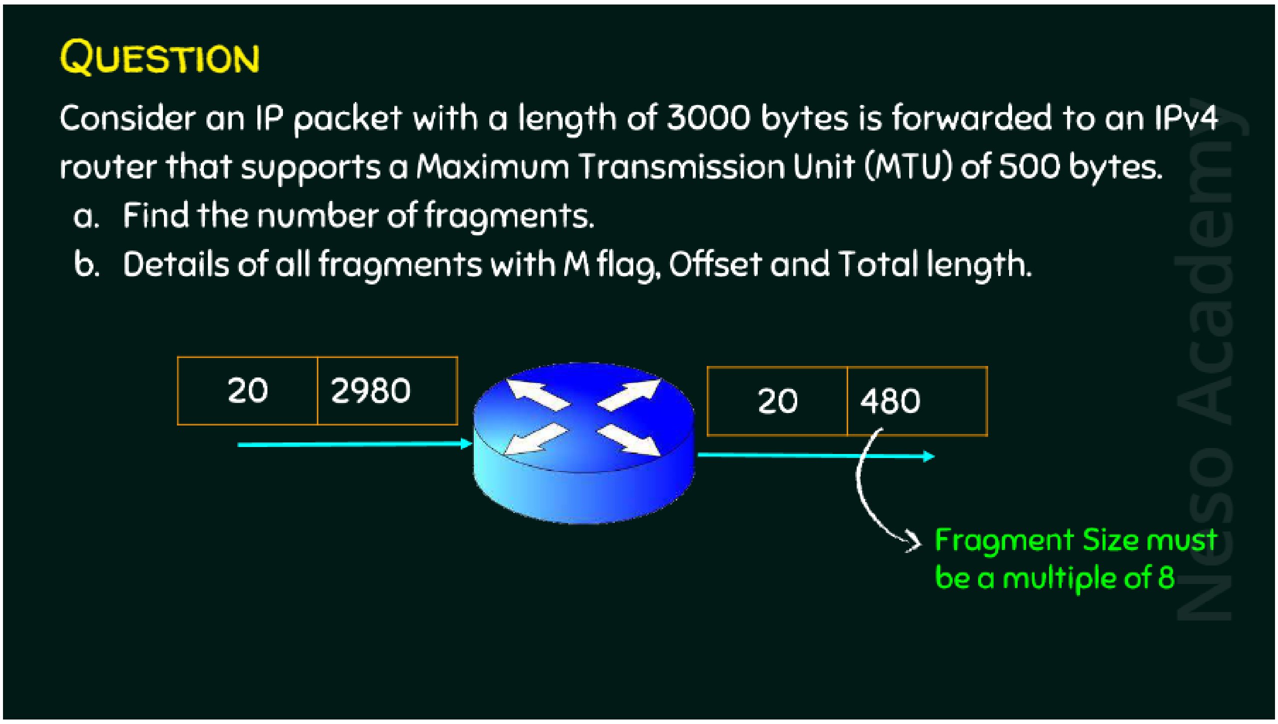
Fragmentation ProcessNeso Academy



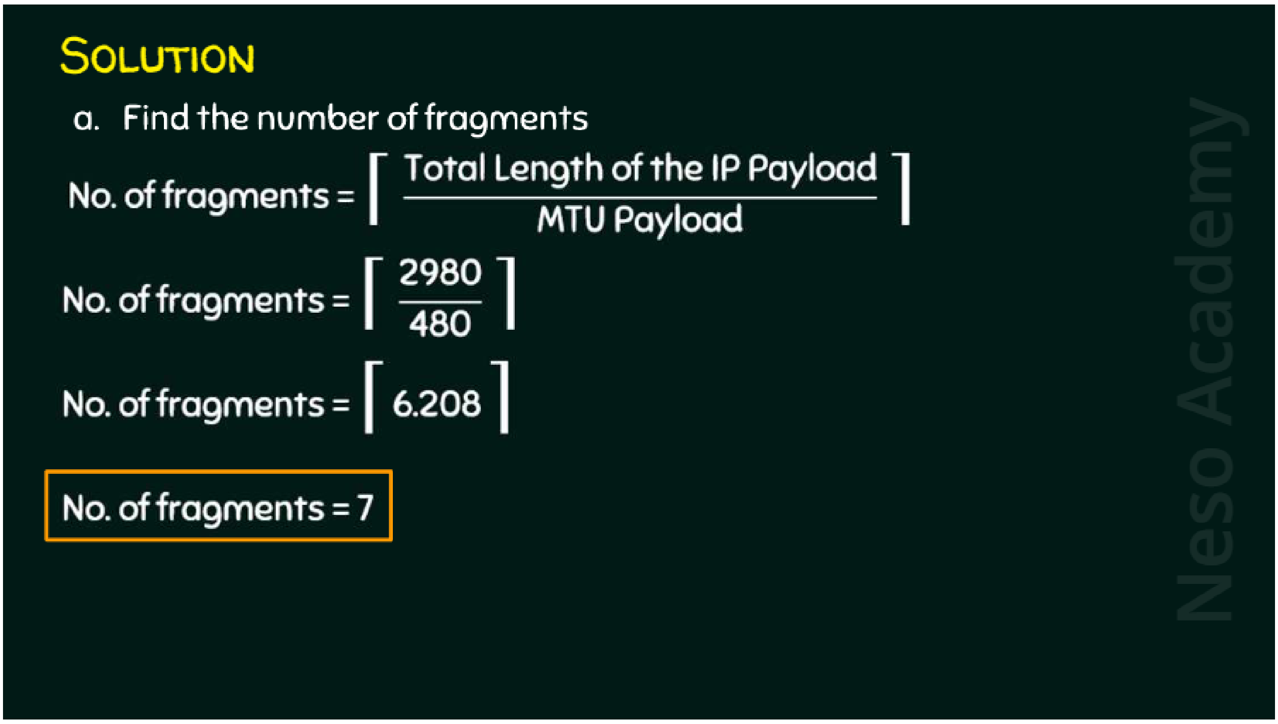
IPv4 Datagram FormatNeso Academy



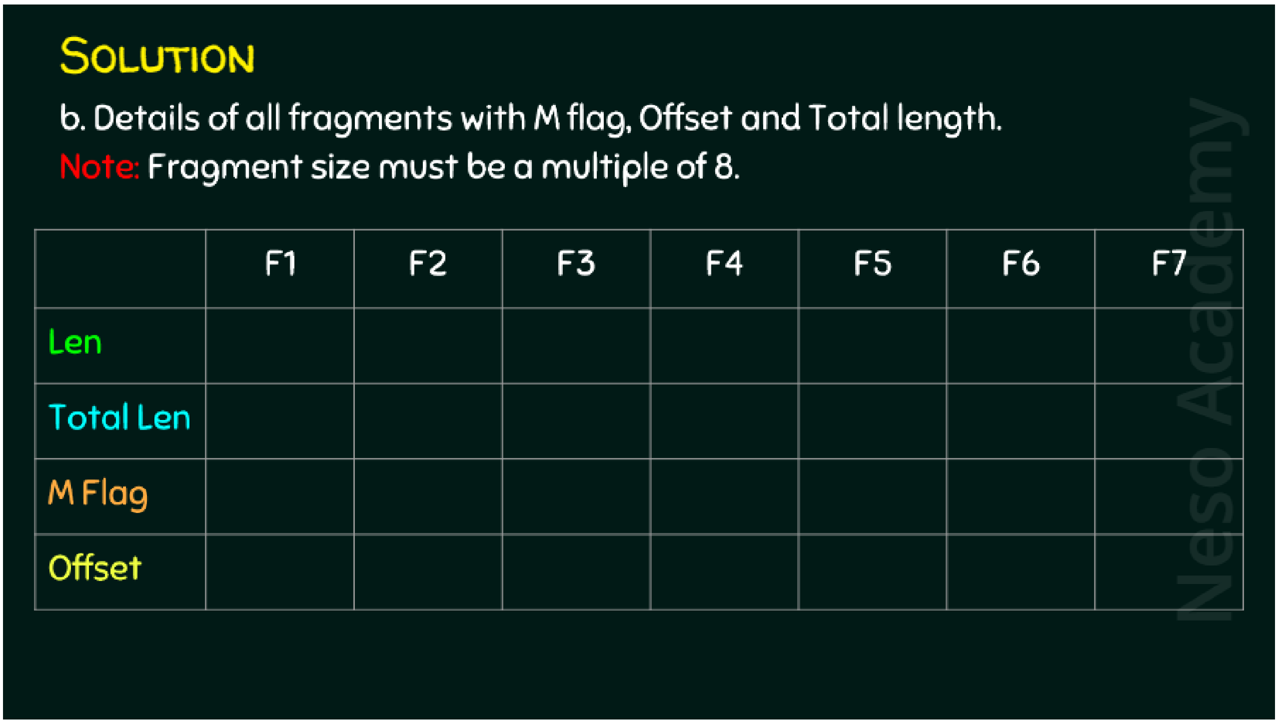
QuestionNeso Academy



QuestionNeso Academy



SolutionNeso Academy



SolutionNeso Academy

Solution

b. Details of all fragments with M flag, Offset and Total length.

	F1	F2	F3	F4	F5	F6	F7
Len	480+20	480+20	480+20	480+20	480+20	480+20	100+20
Total Len	500	500	500	500	500	500	120
M Flag	1	1	1	1	1	1	0
Offset							

SolutionNeso Academy

Solution

$$\text{Offset} = \frac{480}{8}$$

$$\text{Offset} = 60$$

SolutionNeso Academy

Solution

b. Details of all fragments with M flag, Offset and Total length.

	F1	F2	F3	F4	F5	F6	F7
Len	480+20	480+20	480+20	480+20	480+20	480+20	100+20
Total Len	500	500	500	500	500	500	120
M Flag	1	1	1	1	1	1	0
Offset	0	60	120	180	240	300	360

SolutionNeso Academy

Question

Consider an IP packet with a length of 4,500 bytes that includes a 20-byte IPv4 header and 40-byte TCP header. The packet is forwarded to an IPv4 router that supports a Maximum Transmission Unit (MTU) of 600 bytes. Assume that the length of the IP header in all the outgoing fragments of this packet is 20 bytes. Assume that the fragmentation offset value stored in the first fragment is 0. The fragmentation offset value stored in the third fragment is ____ .

[GATE CS 2018]

(A) 0
(B) 72
(C) 144
(D) 216

QuestionNeso Academy

Solution

Find the number of fragments

$$\text{No. of fragments} = \left\lceil \frac{\text{Total Length of the IP Payload}}{\text{MTU Payload}} \right\rceil$$

$$\text{No. of fragments} = \left\lceil \frac{4480}{576} \right\rceil$$

MTU = 600 B

MTU Payload = 600 B − 20 B = 580 B

We know MTU payload must be multiple of 8.

The number nearest to 580 and multiple of 8 is 576

Therefore MTU payload =576 B

SolutionNeso Academy

Solution

Find the number of fragments

$$\text{No. of fragments} = \left\lceil \frac{\text{Total Length of the IP Payload}}{\text{MTU Payload}} \right\rceil$$

$$\text{No. of fragments} = \left\lceil \frac{4480}{576} \right\rceil$$

$$\text{No. of fragments} = \left\lceil 7.7777 \right\rceil$$

$$\text{No. of fragments} = 8$$

SolutionNeso Academy

Solution

Details of all fragments with M flag, Offset and Total length.

	F1	F2	F3	F4	F5	F6	F7	F8
Len	576+20	576+20	576+20	576+20	576+20	576+20	576+20	448+20
Total Len	596	596	596	596	596	596	596	468
M Flag	1	1	1	1	1	1	1	0
Offset								

Solution48Neso Academy

Solution

$$\text{Offset} = \frac{576}{8}$$

$$\text{Offset} = 72$$

SolutionNeso Academy

Solution

Details of all fragments with M flag, Offset and Total length.

	F1	F2	F3	F4	F5	F6	F7	F8
Len	576+20	576+20	576+20	576+20	576+20	576+20	576+20	448+20
Total Len	596	596	596	596	596	596	596	468
M Flag	1	1	1	1	1	1	1	0
Offset	0	72	144	216	288	360	432	504

Solution48Neso Academy

Question

Consider an IP packet with a length of 4,500 bytes that includes a 20-byte IPv4 header and 40-byte TCP header. The packet is forwarded to an IPv4 router that supports a Maximum Transmission Unit (MTU) of 600 bytes. Assume that the length of the IP header in all the outgoing fragments of this packet is 20 bytes. Assume that the fragmentation offset value stored in the first fragment is 0. The fragmentation offset value stored in the third fragment is _____ .

[GATE CS 2018]

(A) 0
(B) 72
(C) 144 ✔
(D) 216

Question✓Neso Academy

Question

In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively are

[GATE CS 2013]

(A) Last fragment, 2400 and 2789

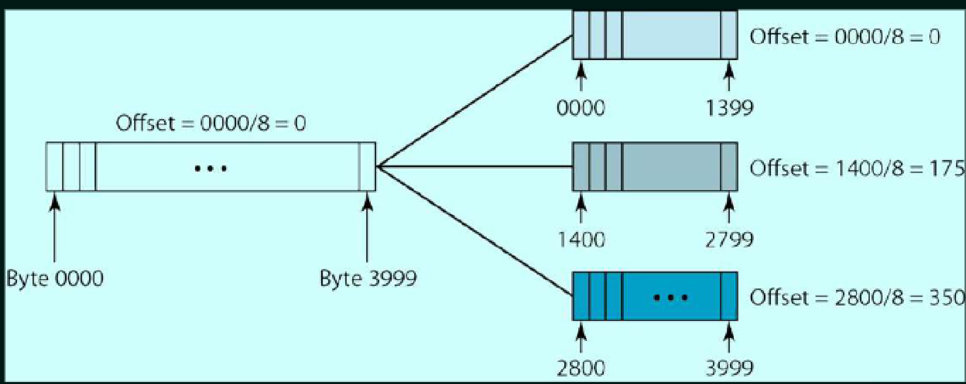
(B) First fragment, 2400 and 2759

(C) Last fragment, 2400 and 2759

(D) Middle fragment, 300 and 689

QuestionNeso Academy

Fragmentation Process



Fragmentation ProcessNeso Academy

Solution

The flag M=0 means there are no more fragments after this fragment.

Hence, it is the last fragment.

Header length = $10 \times 4 = 40$ B.

Total Length = 400 B.

$\therefore$ Payload size = Total length – Header length = $400 - 40 = 360$ B

Fragment offset = $300 \times 8 = 2400$ B. This represents how many Bytes are before this fragment.

The first byte number = 2400

The last byte number = first byte number + total bytes in payload – 1

$= 2400 + 360 - 1$

$= 2759$

Solution∴Neso Academy

Question

In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively are

[GATE CS 2013]

(A) Last fragment, 2400 and 2789

(B) First fragment, 2400 and 2759

(C) Last fragment, 2400 and 2759 ✓

(D) Middle fragment, 300 and 689

✓QuestionNeso Academy

Question

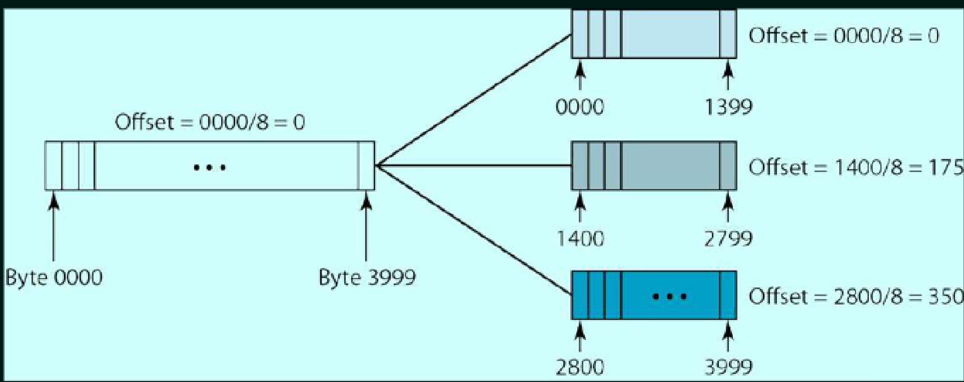
Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e. MTU = 1500 bytes). Size of UDP header is 8 bytes and size of IP header is 20 bytes. There is no option field in IP header. How many total number of IP fragments will be transmitted and what will be the contents of offset field in the last fragment?

[GATE CS 2015]

(A) 6 and 925
(B) 6 and 7400
(C) 7 and 1110
(D) 7 and 8880

QuestionNeso Academy

Fragmentation Process



Offset of F1 = (1400 x 0)/8	Offset of F2 = (1400 x 1)/8	Offset of F3 = (1400 x 2)/8

Fragmentation ProcessNeso Academy

Question

Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e. MTU = 1500 bytes). Size of UDP header is 8 bytes and size of IP header is 20 bytes. There is no option field in IP header. How many total number of IP fragments will be transmitted and what will be the contents of offset field in the last fragment?

[GATE CS 2015]

(A) 6 and 925
(B) 6 and 7400
(C) 7 and 1110 ✓
(D) 7 and 8880

✓QuestionNeso Academy

Question

Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e. MTU = 1500 bytes). Size of UDP header is 8 bytes and size of IP header is 20 bytes. There is no option field in IP header. How many total number of IP fragments will be transmitted and what will be the contents of offset field in the last fragment?

[GATE CS 2015]

(A) 6 and 925
(B) 6 and 7400
(C) 7 and 1110
(D) 7 and 8880 ✓

✓QuestionNeso Academy

Homework

An IP router with a Maximum Transmission Unit (MTU) of 1500 bytes has received an IP packet of size 4404 bytes with an IP header of length 20 bytes. The values of the relevant fields in the header of the third IP fragment generated by the router for this packet are

[GATE CS 2014]

(A) MF bit: 0, Datagram Length: 1444; Offset: 370

(B) MF bit: 1, Datagram Length: 1424; Offset: 185

(C) MF bit: 1, Datagram Length: 1500; Offset: 37

(D) MF bit: 0, Datagram Length: 1424; Offset: 2960

HomeworkNeso Academy

Outcomes

Upon the completion of this lecture, the learner will be able to

★ Understand IGMP.

★ Know the architecture of IGMP.

★ Know various messages in IGMP.

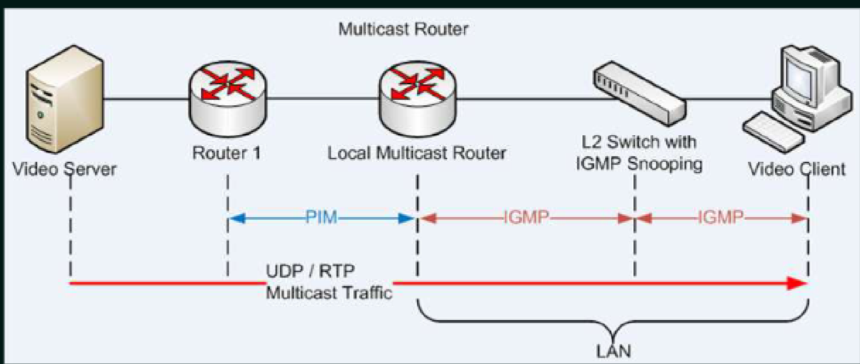
Outcomes★★★Neso Academy

IGMP

- ★ IGMP = Internet Group Management Protocol.
- ★ It is a network layer protocol.
- ★ The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships.
- ★ IGMP is an integral part of IP multicast.
- ★ It can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

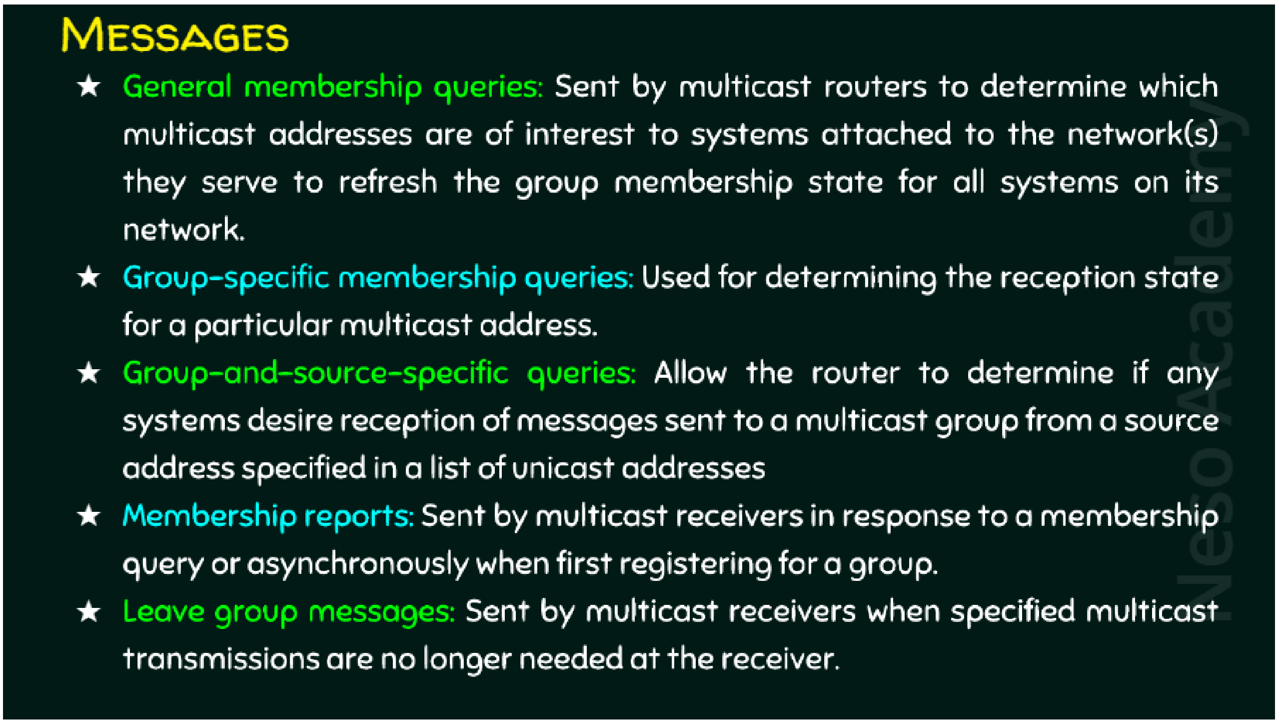
IGMP★★★★★Neso Academy

ARCHITECTURE



- ★ IGMP operates between a host and a local multicast router.
- ★ Switches featuring IGMP snooping derive useful information by observing these IGMP transactions.
- ★ Protocol Independent Multicast (PIM) is then used between the local and remote multicast routers, to direct multicast traffic from hosts sending multicasts to hosts that have registered through IGMP to receive them.

Architecture★★★Neso Academy



MESSAGES

★ General membership queries: Sent by multicast routers to determine which multicast addresses are of interest to systems attached to the network(s) they serve to refresh the group membership state for all systems on its network.

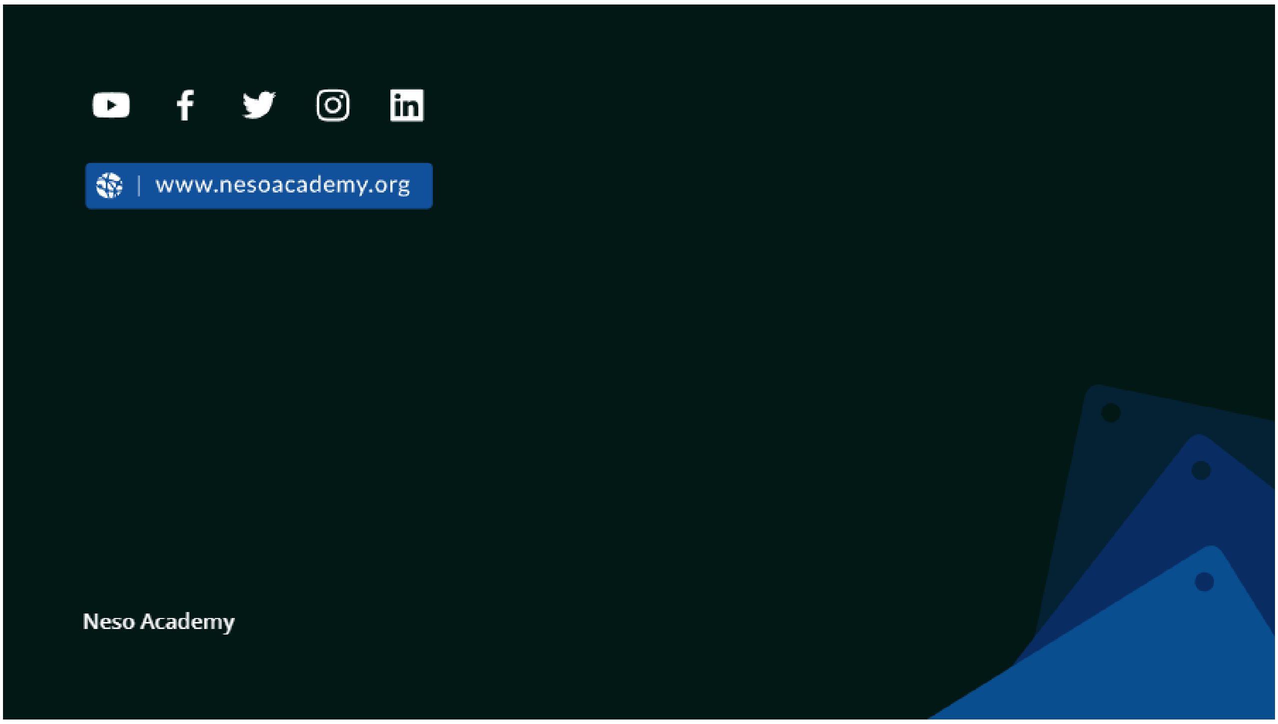
★ Group-specific membership queries: Used for determining the reception state for a particular multicast address.

★ Group-and-source-specific queries: Allow the router to determine if any systems desire reception of messages sent to a multicast group from a source address specified in a list of unicast addresses

★ Membership reports: Sent by multicast receivers in response to a membership query or asynchronously when first registering for a group.

★ Leave group messages: Sent by multicast receivers when specified multicast transmissions are no longer needed at the receiver.

Messages★★★★★Neso Academy



Neso Academy