

Network Layer Protocols | Neso Academy

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

CHAPTER - 4

Network Layer Protocols

Neso Academy

Network Layer Protocols | Neso Academy | CHAPTER - 4

OUTCOMES

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

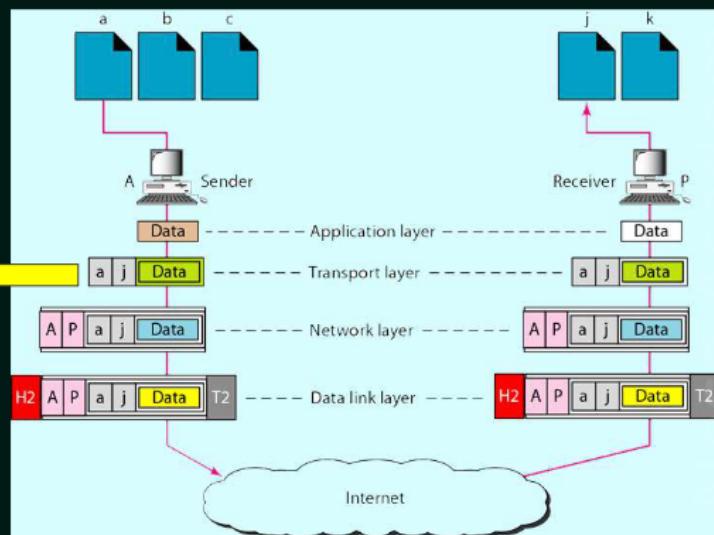
- ★ Understand the role of Port Address, IP address and MAC address.
- ★ Know the need for MAC address.
- ★ Know the Address Resolution Protocol (ARP).
- ★ Know the two functions of ARP.

Neso Academy

Outcomes ★★★★ Neso Academy

DIFFERENT ADDRESSES FOR COMMUNICATION

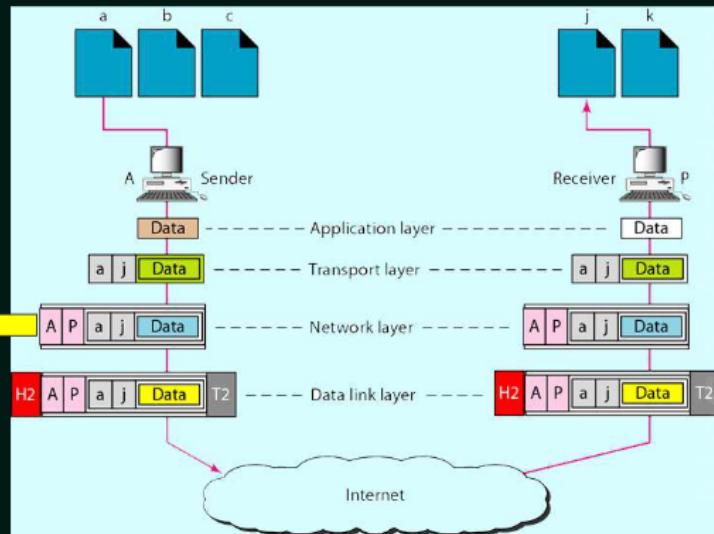
- ★ Port Numbers is of 16 bits (0 – 65535)
- ★ Well Known Ports (0 – 1023)
- ★ Registered Ports (1024 – 49151)
- ★ Dynamic or Private Ports (49152 – 65535)
- ★ Example: HTTP – 80



Different Addresses for communication ★★★★ Neso Academy

DIFFERENT ADDRESSES FOR COMMUNICATION

- ★ IP Address (IPv4 or IPv6)
- ★ IPv4 – 32 bits (Decimal)
- ★ IPv6 – 128 bits (Hexadecimal)
- ★ Either user provides the IP address or DNS resolves the names into IP address.

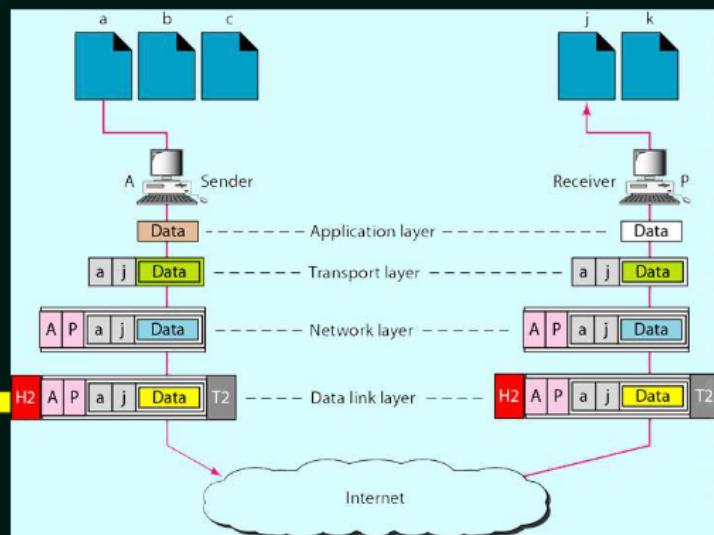


Different Addresses for communication ★★★★ Neso Academy

DIFFERENT ADDRESSES FOR COMMUNICATION

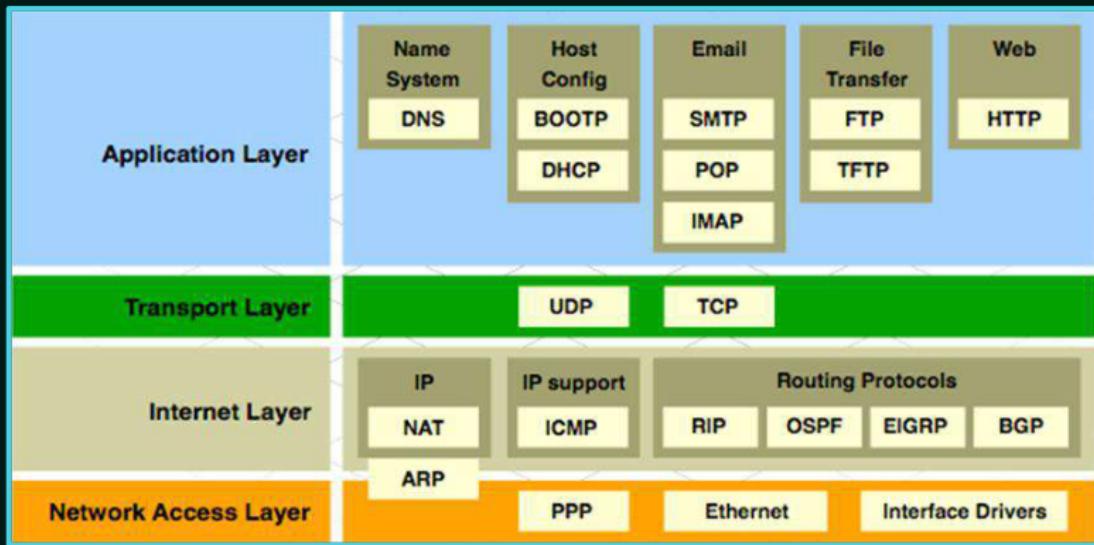
- ★ MAC Address
- ★ 48 bits (Hexadecimal)
- ★ Assigned by manufacturer.
- ★ Usually won't be changed.

★ ARP protocol



★★★★★ Different Addresses for communication Neso Academy

THE TCP/IP PROTOCOL SUITE



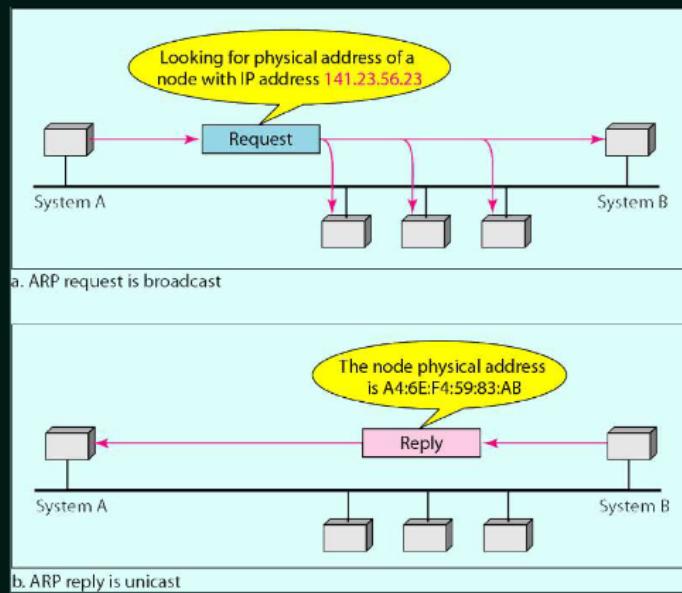
The TCP/IP protocol suite Neso Academy

ARP PROCESS IS EASY



ARP process is easy Neso Academy

ADDRESS RESOLUTION PROTOCOL



Address Resolution Protocol Neso 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 Protocol|Neso 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.

Homework|Neso 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.

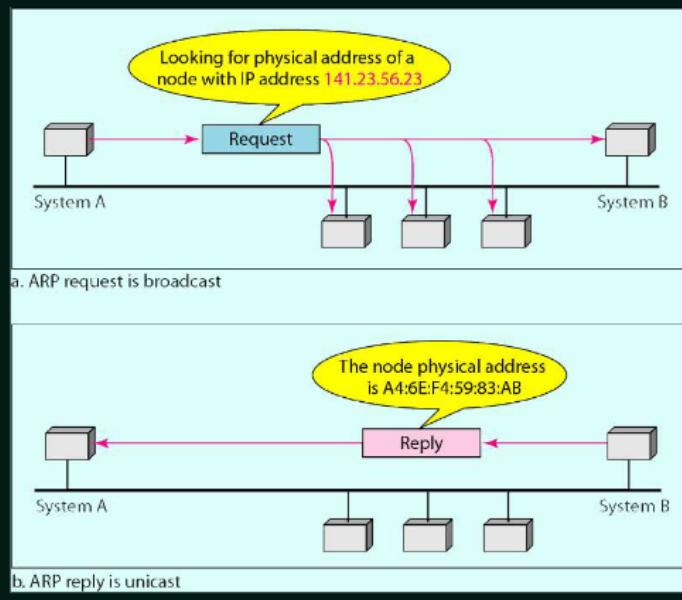
```
C:\WINDOWS\system32>arp -a

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 PROTOCOL



Working of Address Resolution Protocol Neso Academy

HOMEWORK

Which of the following is true about ARP?

- A. ARP request is broadcast and ARP reply is also broadcast.
- B. ARP request is unicast and ARP reply is also unicast.
- C. ARP request is broadcast and ARP reply is unicast.
- D. ARP request is unicast and ARP reply is broadcast.

Homework Neso Academy

QUESTION

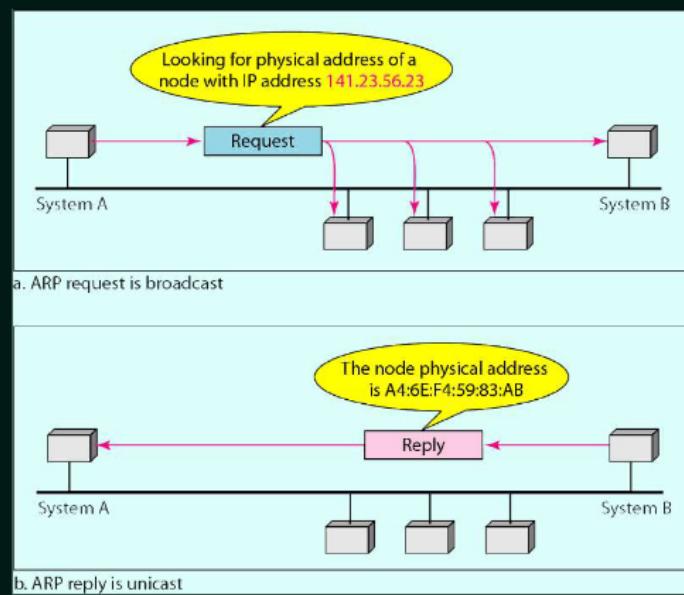
Suppose that in an IP-over-Ethernet network, a machine X wishes to find the MAC address of another machine Y in its subnet. Which one of the following techniques can be used for this?

[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

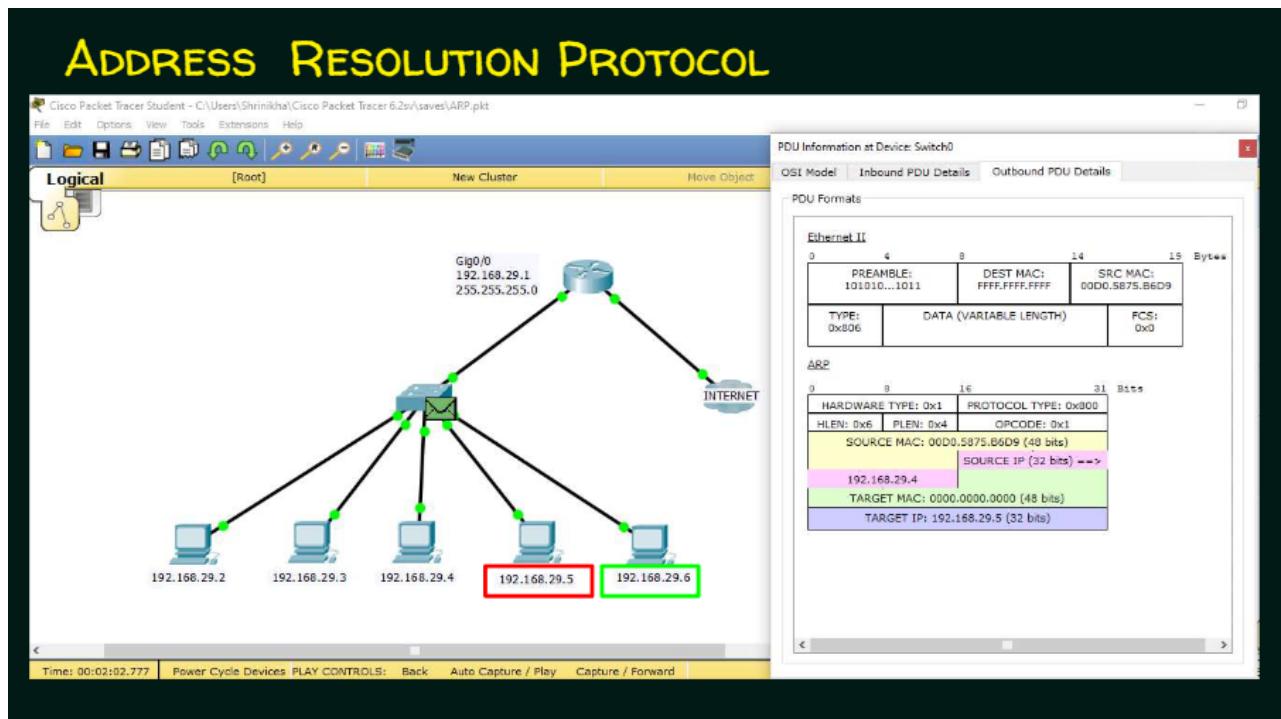
- ★ Know the ARP Header Format and its various fields.
- ★ See the ARP Header and other headers in Cisco Packet Tracer.

Outcomes★★Neso Academy

ADDRESS RESOLUTION PROTOCOL

| 0 | 8 | 16 | 31 |
|--------------------------------|--------------------------------|-----------|----|
| Hardware type=1 | ProtocolType=0x0800 | | |
| HLen=48 | PLen=32 | Operation | |
| SourceHardwareAddr (bytes 0–3) | | | |
| SourceHardwareAddr (bytes 4–5) | SourceProtocolAddr (bytes 0–1) | | |
| SourceProtocolAddr (bytes 2–3) | TargetHardwareAddr (bytes 0–1) | | |
| TargetHardwareAddr (bytes 2–5) | | | |
| TargetProtocolAddr (bytes 0–3) | | | |

Address Resolution Protocol|Neso Academy



Address Resolution Protocol|Neso Academy

ADDRESS RESOLUTION PROTOCOL

| 0 | 8 | 16 | 31 | | |
|--------------------------------|---------|--------------------------------|----|--|--|
| Hardware type=1 | | ProtocolType=0x0800 | | | |
| HLen=48 | PLen=32 | Operation | | | |
| SourceHardwareAddr (bytes 0–3) | | | | | |
| SourceHardwareAddr (bytes 4–5) | | SourceProtocolAddr (bytes 0–1) | | | |
| SourceProtocolAddr (bytes 2–3) | | TargetHardwareAddr (bytes 0–1) | | | |
| TargetHardwareAddr (bytes 2–5) | | | | | |
| TargetProtocolAddr (bytes 0–3) | | | | | |

Hardware Type: Type of physical network (e.g., Ethernet)

Address Resolution Protocol|Neso Academy

ADDRESS RESOLUTION PROTOCOL

| 0 | 8 | 16 | 31 | | |
|--------------------------------|---------|--------------------------------|----|--|--|
| Hardware type=1 | | ProtocolType=0x0800 | | | |
| HLen=48 | PLen=32 | Operation | | | |
| SourceHardwareAddr (bytes 0–3) | | | | | |
| SourceHardwareAddr (bytes 4–5) | | SourceProtocolAddr (bytes 0–1) | | | |
| SourceProtocolAddr (bytes 2–3) | | TargetHardwareAddr (bytes 0–1) | | | |
| TargetHardwareAddr (bytes 2–5) | | | | | |
| TargetProtocolAddr (bytes 0–3) | | | | | |

Protocol Type: Type of upper layer protocol (e.g., IP)

Address Resolution Protocol|Neso Academy

ADDRESS RESOLUTION PROTOCOL

| | | | | | |
|--------------------------------|---------|--------------------------------|----|--|--|
| 0 | 8 | 16 | 31 | | |
| Hardware type=1 | | ProtocolType=0x0800 | | | |
| HLen=48 | PLen=32 | Operation | | | |
| SourceHardwareAddr (bytes 0–3) | | | | | |
| SourceHardwareAddr (bytes 4–5) | | SourceProtocolAddr (bytes 0–1) | | | |
| SourceProtocolAddr (bytes 2–3) | | TargetHardwareAddr (bytes 0–1) | | | |
| TargetHardwareAddr (bytes 2–5) | | | | | |
| TargetProtocolAddr (bytes 0–3) | | | | | |

HLEN and PLEN: Length of Physical Address and Protocol Address

Neso Academy

Address Resolution Protocol Neso Academy

ADDRESS RESOLUTION PROTOCOL

| | | | | | |
|--------------------------------|---------|--------------------------------|----|--|--|
| 0 | 8 | 16 | 31 | | |
| Hardware type=1 | | ProtocolType=0x0800 | | | |
| HLen=48 | PLen=32 | Operation | | | |
| SourceHardwareAddr (bytes 0–3) | | | | | |
| SourceHardwareAddr (bytes 4–5) | | SourceProtocolAddr (bytes 0–1) | | | |
| SourceProtocolAddr (bytes 2–3) | | TargetHardwareAddr (bytes 0–1) | | | |
| TargetHardwareAddr (bytes 2–5) | | | | | |
| TargetProtocolAddr (bytes 0–3) | | | | | |

Operation: Request or Reply

Neso Academy

Address Resolution Protocol Neso Academy

ADDRESS RESOLUTION PROTOCOL

| 0 | 8 | 16 | 31 |
|--------------------------------|---------|--------------------------------|----|
| Hardware type=1 | | ProtocolType=0x0800 | |
| HLen=48 | PLen=32 | Operation | |
| SourceHardwareAddr (bytes 0–3) | | | |
| SourceHardwareAddr (bytes 4–5) | | SourceProtocolAddr (bytes 0–1) | |
| SourceProtocolAddr (bytes 2–3) | | TargetHardwareAddr (bytes 0–1) | |
| TargetHardwareAddr (bytes 2–5) | | | |
| TargetProtocolAddr (bytes 0–3) | | | |

Source Physical/Protocol addresses & Target Physical/Protocol addresses

Address Resolution Protocol|Neso Academy

OUTCOMES

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

- ★ Understand RARP.
- ★ Know the difference between ARP and RARP.
- ★ Understand about the protocols resolving address from one form to another.

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

Which one of the following protocols is NOT used to resolve one form of address to another one?

[GATE CS 2019]

- (A) DNS
- (B) ARP
- (C) DHCP ✓
- (D) RARP

Question✓Neso Academy

OUTCOMES

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

- ★ Understand the basics of DHCP.

Outcomes★Neso Academy

YOU ARE A NETWORK ADMINISTRATOR!



You are a Network administrator!Neso Academy

DHCP

- ★ DHCP = Dynamic Host Configuration Protocol.
- ★ The MAC addresses are configured into network by manufacturer and they are expected to be unique.
- ★ IP addresses must be unique on any internetwork.
- ★ Most Operating Systems provide a way to manually configure the IP information for the host.
- ★ Drawbacks of manual configuration:
 - A lot of work to configure all the hosts in a large network.
 - Configuration process is error-prone.
- ★ Hence automated IP configuration is required.

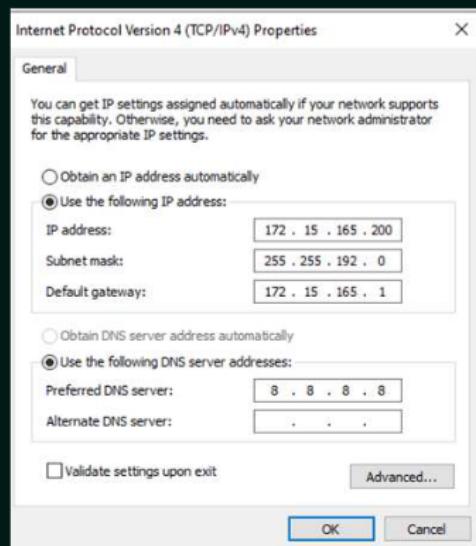
DHCP★★★★○○★Neso Academy

DHCP

- ★ Automated IP Configuration Process is required.
- ★ DHCP server is responsible for providing configuration information to hosts.
- ★ There is at least one DHCP server for an administrative domain.
- ★ DHCP server maintains a pool of available IP addresses.
- ★ So when requested by a host, DHCP allows the host to obtain an IP address dynamically.
- ★ DHCP “leases” the IP information to the host for a set period.

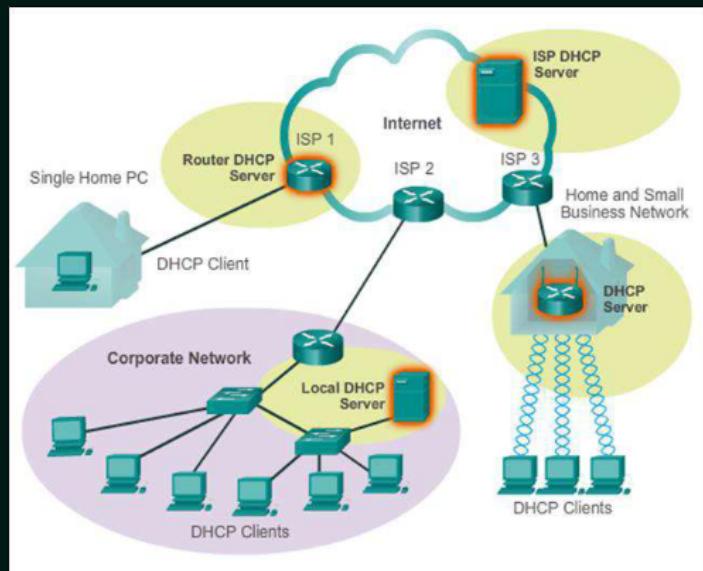
DHCP★★★★★Neso Academy

DHCP



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

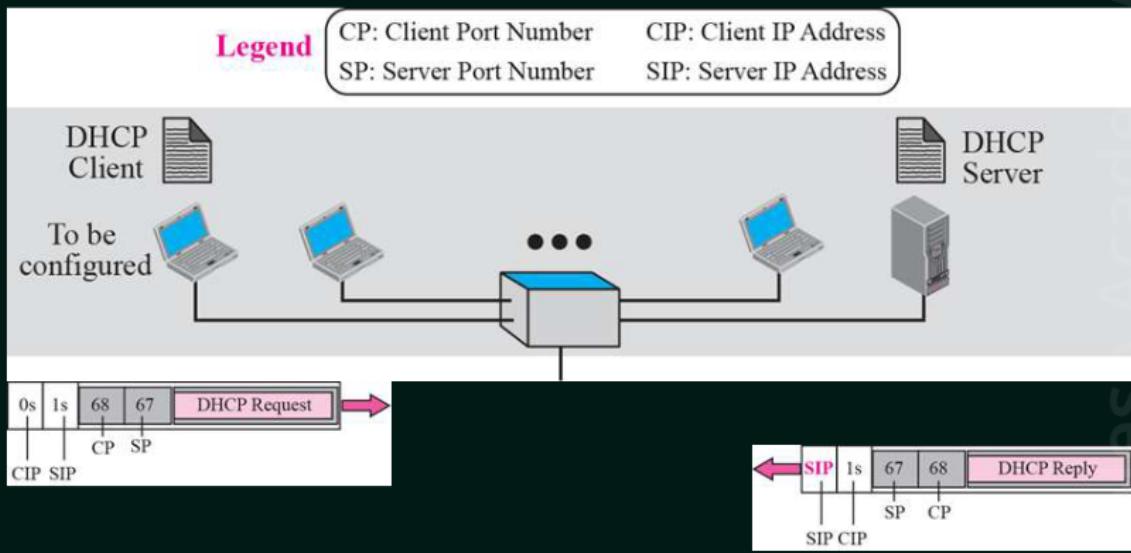
METHODS OF IP ADDRESS ALLOCATION

Depending on implementation, the DHCP server may have three methods of allocating IP addresses

1. Dynamic allocation
2. Automatic allocation
3. Static allocation

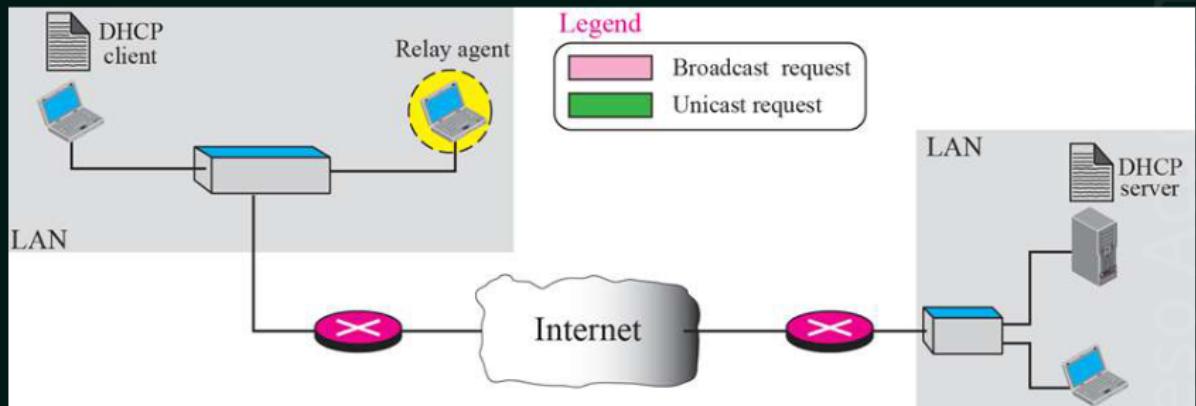
Methods of IP address allocationNeso Academy

DHCP CLIENT AND SERVER IN SAME NETWORK



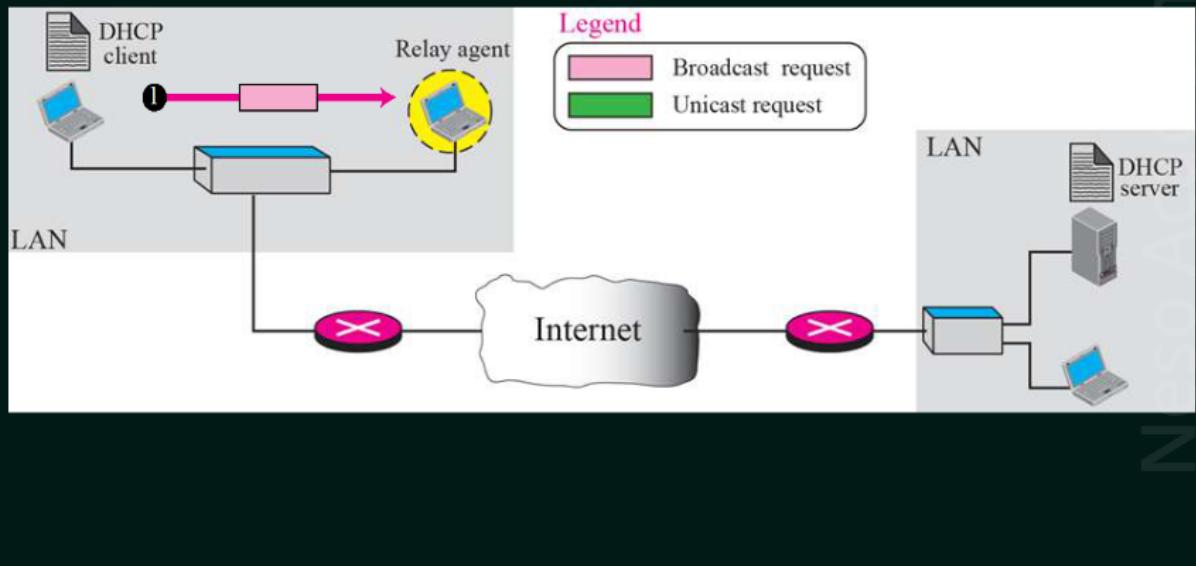
DHCP client and server in same networkNeso Academy

DHCP CLIENT AND SERVER IN DIFFERENT NETWORK



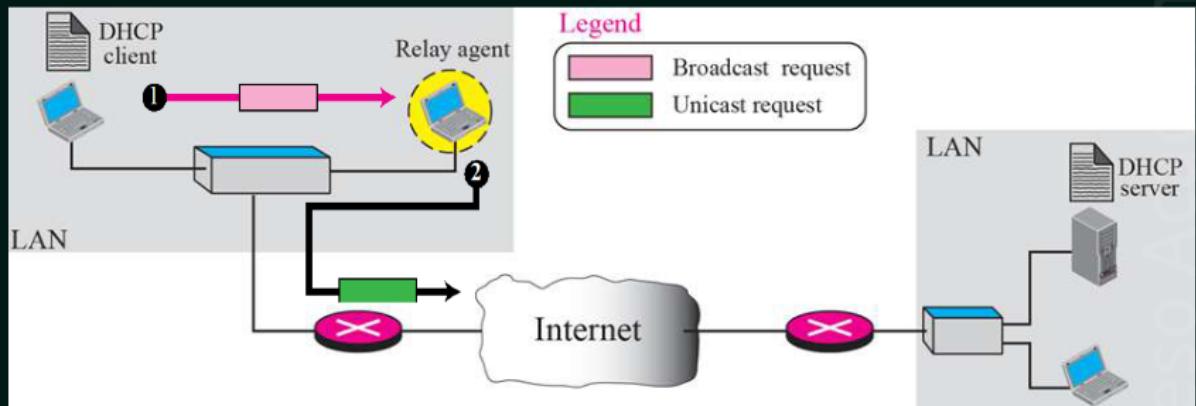
DHCP client and server in different network
Neso Academy

DHCP CLIENT AND SERVER IN DIFFERENT NETWORK



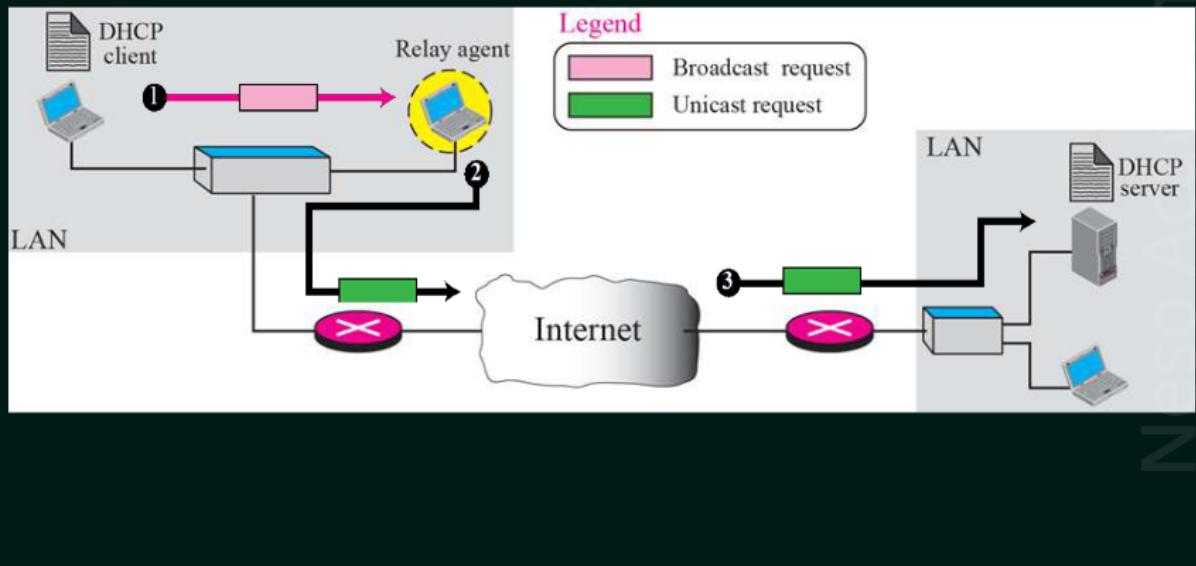
DHCP client and server in different network
Neso Academy

DHCP CLIENT AND SERVER IN DIFFERENT NETWORK



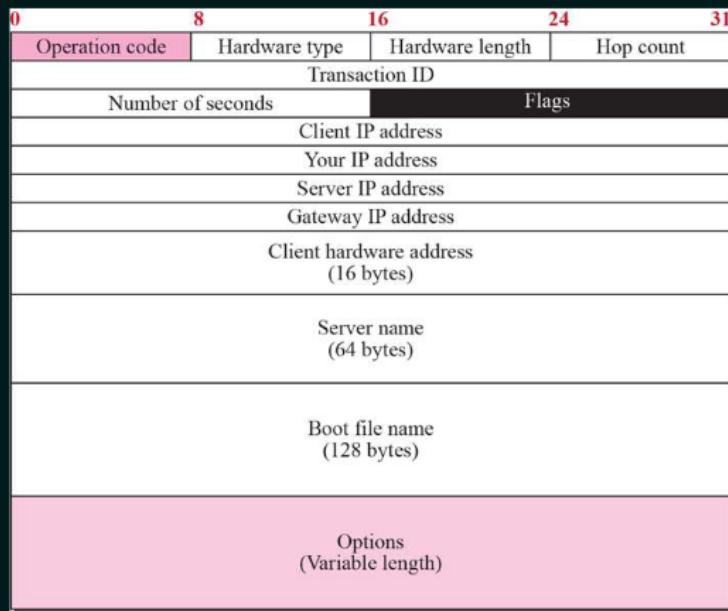
DHCP client and server in different network
Neso Academy

DHCP CLIENT AND SERVER IN DIFFERENT NETWORK



DHCP client and server in different network
Neso Academy

DHCP PACKET FORMAT



DHCP Packet Format Neso 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 |

Length in bytes defined in the length field.

DHCP Packet Format Neso 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

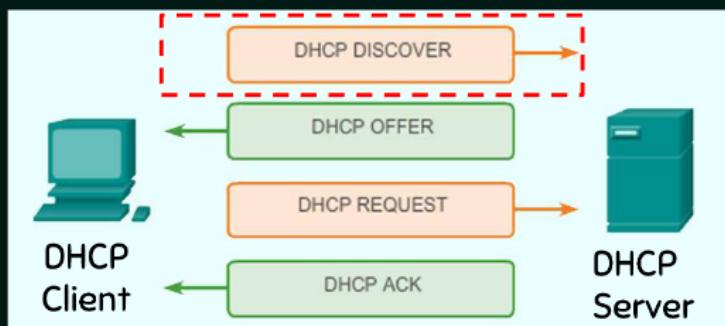
OUTCOMES

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

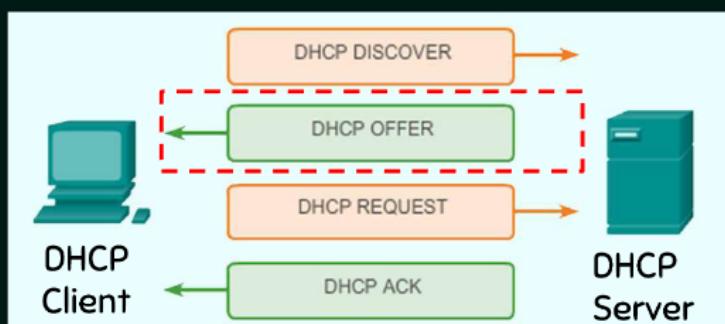


DHCP DISCOVER:

- ★ The DHCP client broadcasts a DHCPDISCOVER message on the network subnet using the destination address 255.255.255.255 (limited broadcast) or the specific subnet broadcast address (directed broadcast) DHCP Client.
- ★ A DHCP client may also request its last known IP address.

DHCP Operation in a nutshell ★★Neso Academy

DHCP OPERATION IN A NUTSHELL

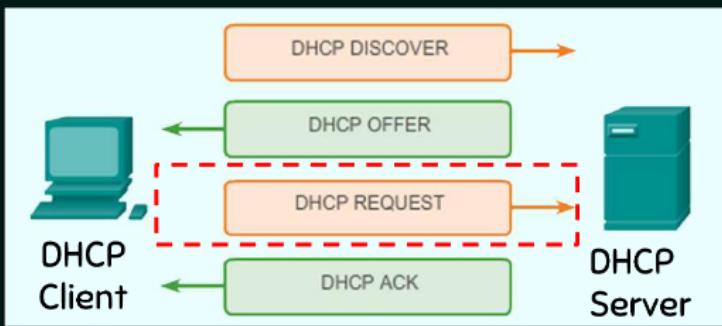


DHCP OFFER:

- ★ When a DHCP server receives a DHCPDISCOVER message from a client, which is an IP address lease request, the DHCP server reserves an IP address for the client and makes a lease offer by sending a DHCPOFFER message to the client.
- ★ This message contains the client's client id (traditionally a MAC address), the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer.

DHCP Operation in a nutshell ★★Neso Academy

DHCP OPERATION IN A NUTSHELL

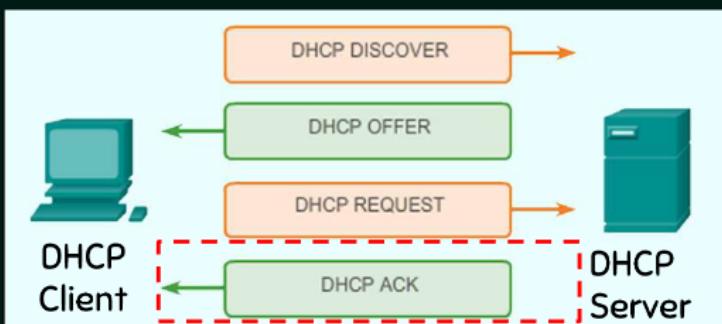


DHCP REQUEST:

- ★ In response to the DHCP offer, the client replies with a DHCPREQUEST message, broadcast to the server, requesting the offered address.
- ★ A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer.
- ★ Based on required server identification option in the request and broadcast messaging, servers are informed whose offer the client has accepted.

DHCP Operation in a nutshell★★★Neso Academy

DHCP OPERATION IN A NUTSHELL



DHCP ACK:

- ★ When the DHCP server receives the DHCPREQUEST message from the client, the configuration process enters its final phase.
- ★ The acknowledgement phase involves sending a DHCPACK packet to the client.
- ★ This packet includes the lease duration and any other configuration information that the client might have requested.
- ★ At this point, the IP configuration process is completed.

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

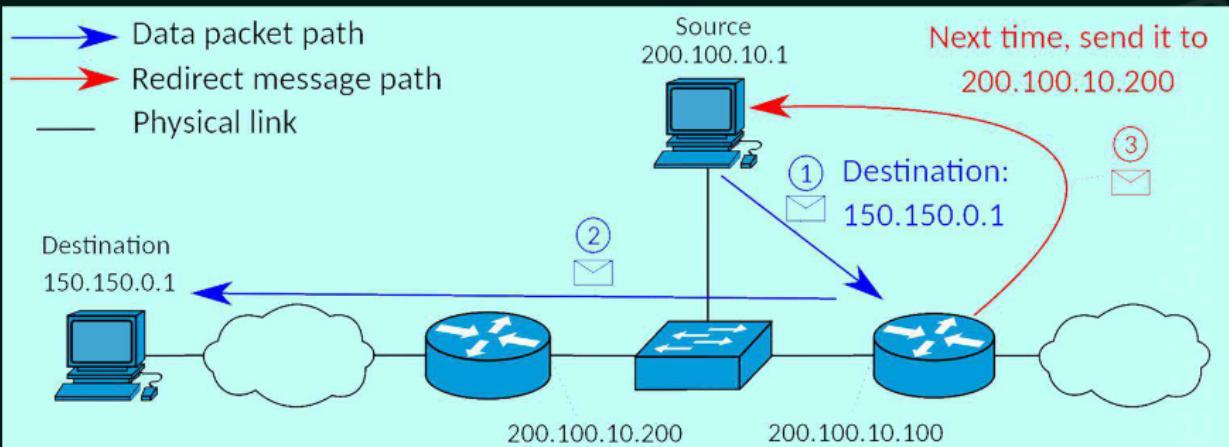
★★★★★○○○○ ICMPv4 Neso Academy

ICMPv4

- ★ ICMP messages are typically used for diagnostic or control purposes or generated in response to errors in IP operations.
- ★ ICMP errors are directed to the source IP address of the originating packet.
- ★ This protocol defines a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP packet successfully.
- ★ ICMP-Redirect
 - From router to a source host
 - With a better route information

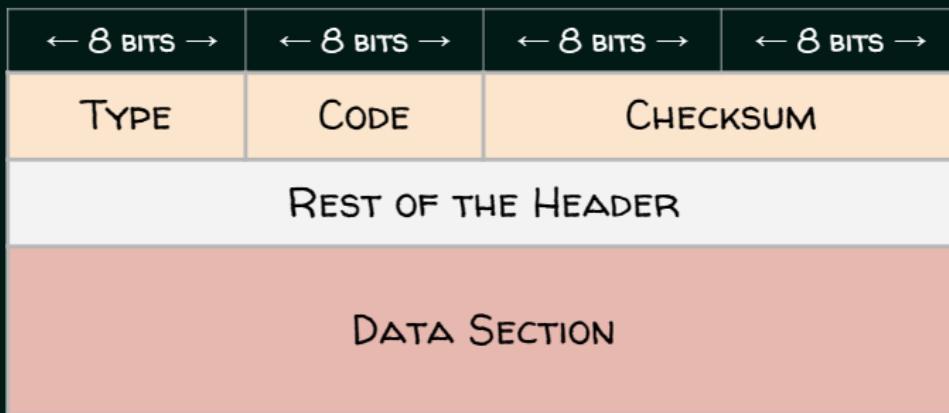
★★★★○ ICMPv4 Neso Academy

ICMP REDIRECT



ICMP Redirect Neso Academy

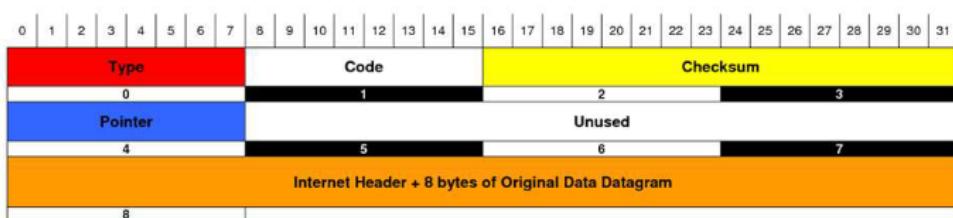
ICMPv4 PACKET FORMAT



ICMPv4 Packet Format ← 8 bits → ← 8 bits → ← 8 bits → ← 8 bits →
 → Type Code Checksum Rest of the Header Data Section Neso Academy

ICMPv4 PACKET FORMAT

ICMP Parameter Message Format



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

| Type | Code | Meaning |
|------|------|---|
| 5 | 0 | Redirect datagram for the network |
| 1 | 0 | Redirect datagram for the host |
| 2 | 0 | Redirect datagram for the TOS & Network |
| 3 | 0 | 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 | 0 | Fragment reassemble time exceeded |
| 12 | 0 | Pointer indicates the error (Parameter Problem) |
| 1 | 1 | Missing a required option (Parameter Problem) |
| 2 | 0 | Bad length (Parameter Problem) |
| 13 | 0 | Time Stamp |
| 14 | 0 | Time Stamp Reply |
| 15 | 0 | Information Request |
| 16 | 0 | Information Reply |
| 17 | 0 | Address Mask Request |
| 18 | 0 | Address Mask Reply |
| 30 | 0 | Traceroute (Tracert) |

ICMPv4 Packet Format Neso Academy

OUTCOMES

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

- ★ Understand the checksum calculation for ICMPv4.

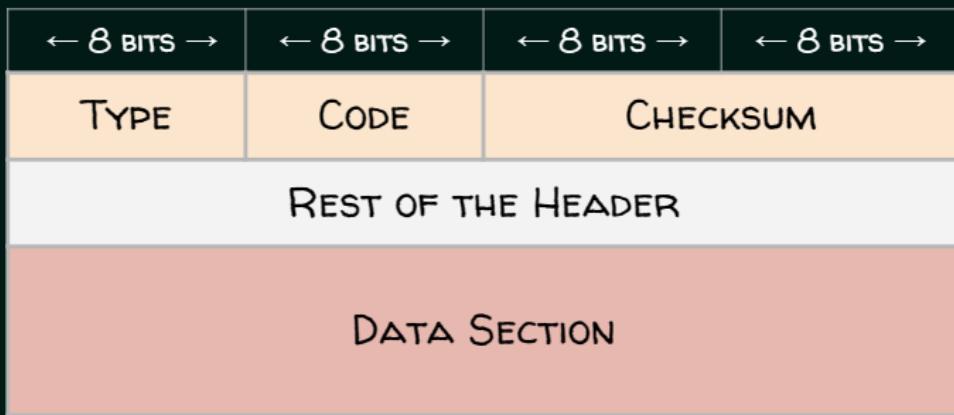
Outcomes ★ Neso Academy

QUESTION

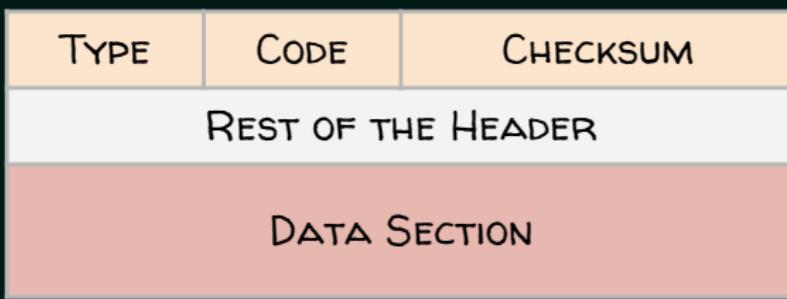
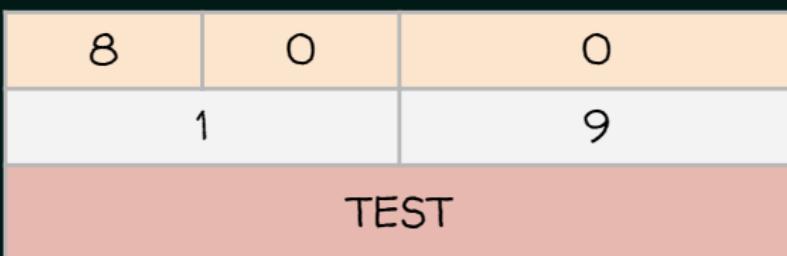
Calculate the checksum for the following ICMPv4 packet.

| | | |
|------|---|---|
| 8 | 0 | 0 |
| 1 | | 9 |
| TEST | | |

Question80019TESTNeso Academy

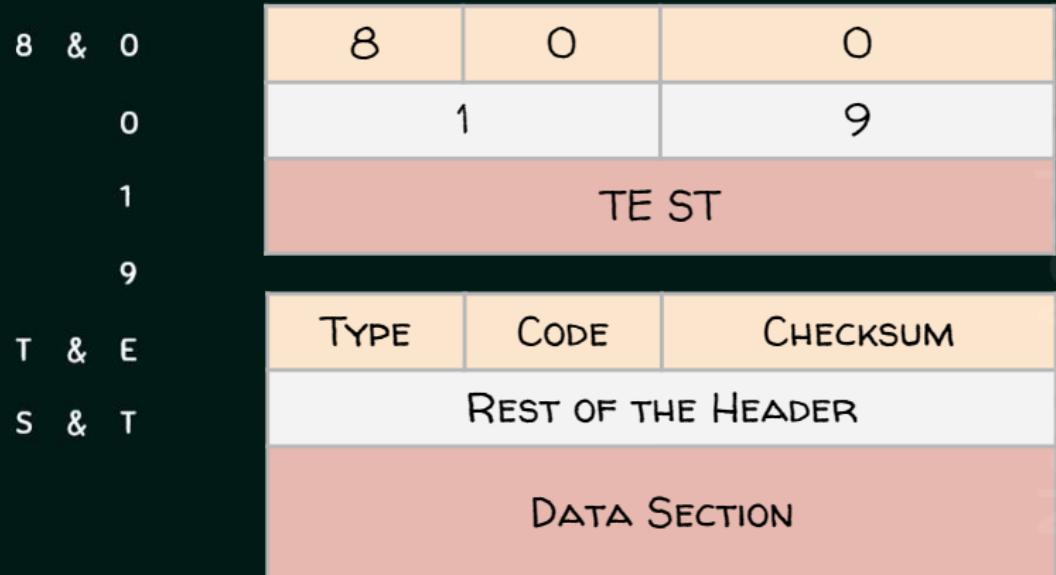
SOLUTION

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

SOLUTION

Solution80019TESTTypeCodeChecksumRest of the HeaderData SectionNeso Academy

SOLUTION



Solution80019TE STTypeCodeChecksumRest of the HeaderData SectionNeso Academy

SOLUTION

| | |
|----------------------------|-------------------|
| 8 & 0 → 0 0 0 0 1 0 0 0 | 0 0 0 0 0 0 0 0 0 |
| 0 → 0 0 0 0 0 0 0 0 | 0 0 0 0 0 0 0 0 0 |
| 1 → 0 0 0 0 0 0 0 0 | 0 0 0 0 0 0 0 0 1 |
| 9 → 0 0 0 0 0 0 0 0 | 0 0 0 0 1 0 0 1 |
| T & E → 0 1 0 1 0 1 0 0 | 0 1 0 0 0 1 0 1 |
| S & T → 0 1 0 1 0 0 1 1 | 0 1 0 1 0 1 0 0 |
| <hr/> | |
| Sum → 1 0 1 0 1 1 1 1 | 1 0 1 0 0 0 1 1 |
| Checksum → 0 1 0 1 0 0 0 0 | 0 1 0 1 1 1 0 0 |

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 LAYER

It is responsible for delivery of data from the original source to the destination network.

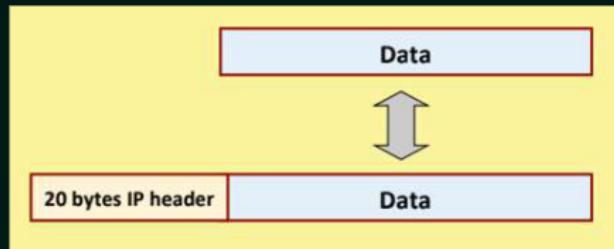
SERVICES PROVIDED BY NETWORK LAYER

- ★ Logical addressing.
- ★ Routing.



★★Need for network layerNeso Academy

INTERNET PROTOCOL (IP)



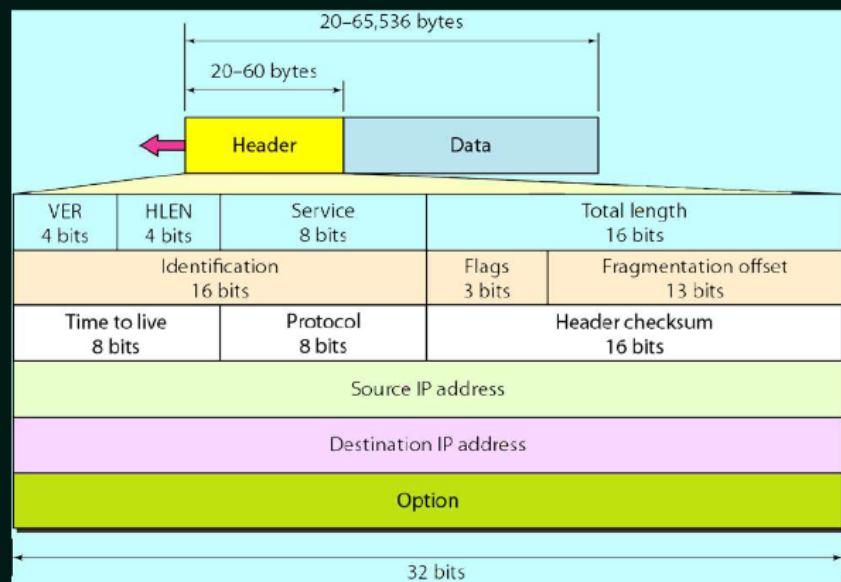
Internet Protocol (IP)Neso Academy

INTERNET PROTOCOL (IP)

- ★ IPv4 and IPv6.
- ★ Switching at the network layer in the Internet uses the datagram approach to packet switching.
- ★ Communication at the network layer in the Internet is connectionless.
- ★ The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols.
- ★ Best-effort delivery (unreliable service)
 - packets are lost
 - packets are delivered out of order
 - duplicate copies of a packet are delivered
 - packets can be delayed for a long time

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

IPv4 HEADER FORMAT



IPv4 Header FormatNeso Academy

IPv4 HEADER FORMAT

| | | | | | | | | | |
|---------------------------|--------------------|----------------------------|---------------------------------|--|--|--|--|--|--|
| VER 4 bits | HLEN 4 bits | Service 8 bits | Total length 16 bits | | | | | | |
| Identification 16 bits | | Flags 3 bits | Fragmentation offset 13 bits | | | | | | |
| Time to live 8 bits | Protocol 8 bits | Header checksum 16 bits | | | | | | | |
| Source IP address | | | | | | | | | |
| Destination IP address | | | | | | | | | |
| Option | | | | | | | | | |
| DATA (Variable Size) | | | | | | | | | |

IPv4 Header Format DATA (Variable Size) Neso Academy

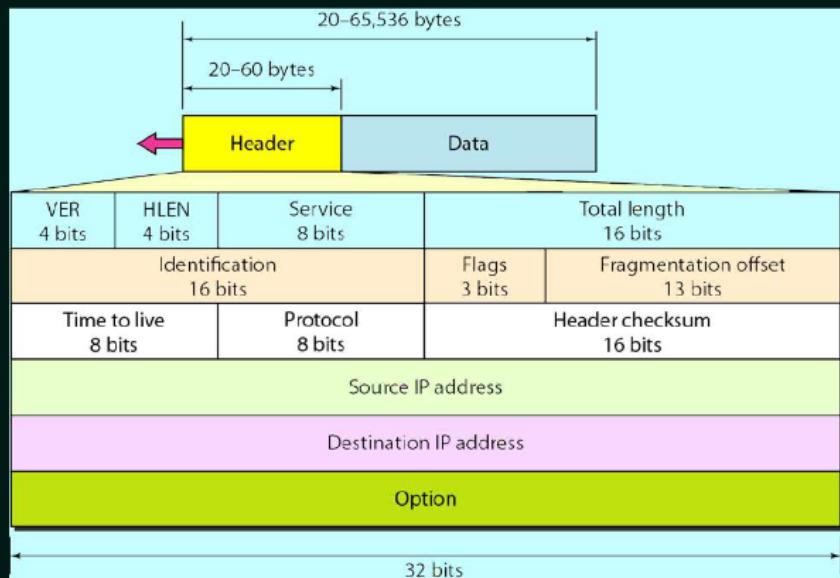
OUTCOMES

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

- ★ Understand the various fields of the IPv4 header format.

★ Outcomes Neso Academy

IPv4 DATAGRAM FORMAT



IPv4 Datagram Format Neso Academy

IPv4 DATAGRAM FORMAT

| | | | |
|---------------------------|--------------------|----------------------------|---------------------------------|
| VER 4 bits | HLEN 4 bits | Service 8 bits | Total length 16 bits |
| Identification 16 bits | | Flags 3 bits | Fragmentation offset 13 bits |
| Time to live 8 bits | Protocol 8 bits | Header checksum 16 bits | |
| Source IP address | | | |
| Destination IP address | | | |
| Option | | | |

VERSION – 4 Bits

Ver = 0100 (Decimal: 4) means it is IPv4.

IPv4 Datagram Format Version -4 Bits Neso Academy

IPv4 DATAGRAM FORMAT

| | | | | | | | | | |
|---------------------------|--------------------|----------------------------|---------------------------------|--|--|--|--|--|--|
| VER 4 bits | HLEN 4 bits | Service 8 bits | Total length 16 bits | | | | | | |
| Identification 16 bits | | Flags 3 bits | Fragmentation offset 13 bits | | | | | | |
| Time to live 8 bits | Protocol 8 bits | Header checksum 16 bits | | | | | | | |
| Source IP address | | | | | | | | | |
| Destination IP address | | | | | | | | | |
| Option | | | | | | | | | |

HLEN – 4 Bits

- ★ HLEN = Number of 32 bit words in the header.
- ★ If HLEN = 6 (0110), it means the IP header is 192 bits (32×6) long.

IPv4 Datagram Format HLEN -4 Bits ★★ Neso Academy

IPv4 DATAGRAM FORMAT

| | | | | | | | | | |
|---------------------------|--------------------|----------------------------|---------------------------------|--|--|--|--|--|--|
| VER 4 bits | HLEN 4 bits | Service 8 bits | Total length 16 bits | | | | | | |
| Identification 16 bits | | Flags 3 bits | Fragmentation offset 13 bits | | | | | | |
| Time to live 8 bits | Protocol 8 bits | Header checksum 16 bits | | | | | | | |
| Source IP address | | | | | | | | | |
| Destination IP address | | | | | | | | | |
| Option | | | | | | | | | |

SERVICE – 8 Bits

- ★ Type of Service (TOS)
- ★ Not widely used

| TOS Bits | Description |
|----------|----------------------|
| 0000 | Normal (default) |
| 0001 | Minimize cost |
| 0010 | Maximize reliability |
| 0100 | Maximize throughput |
| 1000 | Minimize delay |

IPv4 Datagram Format Service -8 Bits ★★ Neso Academy

IPv4 DATAGRAM FORMAT

| | | | | | | | | | |
|---------------------------|--------------------|----------------------------|---------------------------------|--|--|--|--|--|--|
| VER 4 bits | HLEN 4 bits | Service 8 bits | Total length 16 bits | | | | | | |
| Identification 16 bits | | Flags 3 bits | Fragmentation offset 13 bits | | | | | | |
| Time to live 8 bits | Protocol 8 bits | Header checksum 16 bits | | | | | | | |
| Source IP address | | | | | | | | | |
| Destination IP address | | | | | | | | | |
| Option | | | | | | | | | |

TOTAL LENGTH – 16 Bits

- ★ Number of bytes in this datagram.
- ★ This field defines the total length of the datagram including the header.



IPv4 Datagram Format Total Length -16 Bits ★★ Neso Academy

IPv4 DATAGRAM FORMAT

| | | | | | | | | | |
|---------------------------|--------------------|----------------------------|---------------------------------|--|--|--|--|--|--|
| VER 4 bits | HLEN 4 bits | Service 8 bits | Total length 16 bits | | | | | | |
| Identification 16 bits | | Flags 3 bits | Fragmentation offset 13 bits | | | | | | |
| Time to live 8 bits | Protocol 8 bits | Header checksum 16 bits | | | | | | | |
| Source IP address | | | | | | | | | |
| Destination IP address | | | | | | | | | |
| Option | | | | | | | | | |

IDENTIFICATION – 16 Bits

Used by fragmentation.

IPv4 Datagram Format Identification -16 Bits Neso Academy

IPv4 DATAGRAM FORMAT

| | | | | | | | | | |
|---------------------------|--------------------|----------------------------|---------------------------------|--|--|--|--|--|--|
| VER 4 bits | HLEN 4 bits | Service 8 bits | Total length 16 bits | | | | | | |
| Identification 16 bits | | Flags 3 bits | Fragmentation offset 13 bits | | | | | | |
| Time to live 8 bits | Protocol 8 bits | Header checksum 16 bits | | | | | | | |
| Source IP address | | | | | | | | | |
| Destination IP address | | | | | | | | | |
| Option | | | | | | | | | |

FLAGS (3 BITS) / FRAGMENTATION OFFSET (13 BITS)



- ★ Used by fragmentation.
- ★ D – Do Not Fragment & M – More Fragments.

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

IPv4 DATAGRAM FORMAT

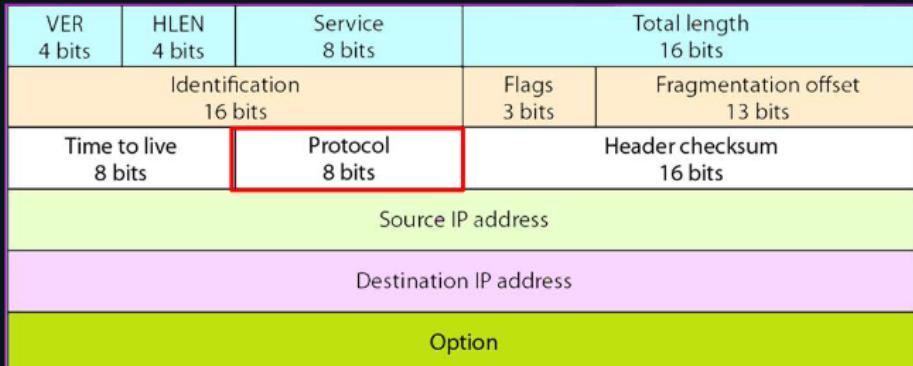
| | | | | | | | | | |
|---------------------------|--------------------|----------------------------|---------------------------------|--|--|--|--|--|--|
| VER 4 bits | HLEN 4 bits | Service 8 bits | Total length 16 bits | | | | | | |
| Identification 16 bits | | Flags 3 bits | Fragmentation offset 13 bits | | | | | | |
| Time to live 8 bits | Protocol 8 bits | Header checksum 16 bits | | | | | | | |
| Source IP address | | | | | | | | | |
| Destination IP address | | | | | | | | | |
| Option | | | | | | | | | |

TIME TO LIVE (TTL) – 8 BITS

- ★ Number of hops this datagram has traveled.
- ★ Prevents looping of IP packets in the network.

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

IPv4 DATAGRAM FORMAT



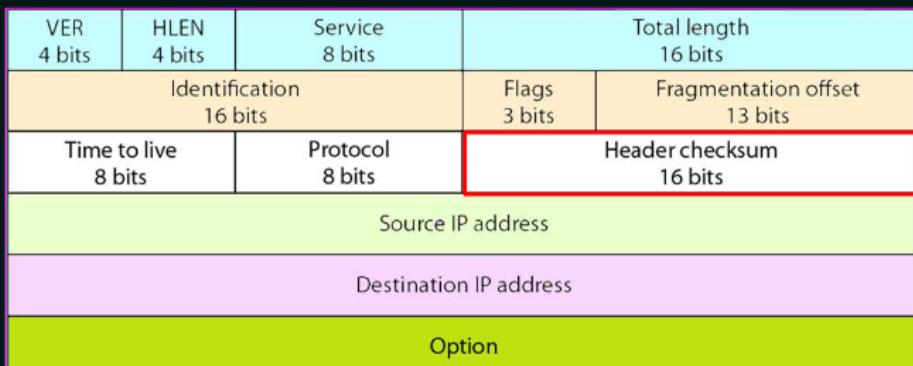
PROTOCOL – 8 BITS

- ★ Demux Key (TCP = 6, UDP = 17).
- ★ The value of the protocol field defines to which protocol that data belong.

| Value | Protocol |
|-------|----------|
| 1 | ICMP |
| 2 | IGMP |
| 6 | TCP |
| 17 | UDP |
| 89 | OSPF |

IPv4 Datagram Format Protocol -8 bits ★★ Neso Academy

IPv4 DATAGRAM FORMAT

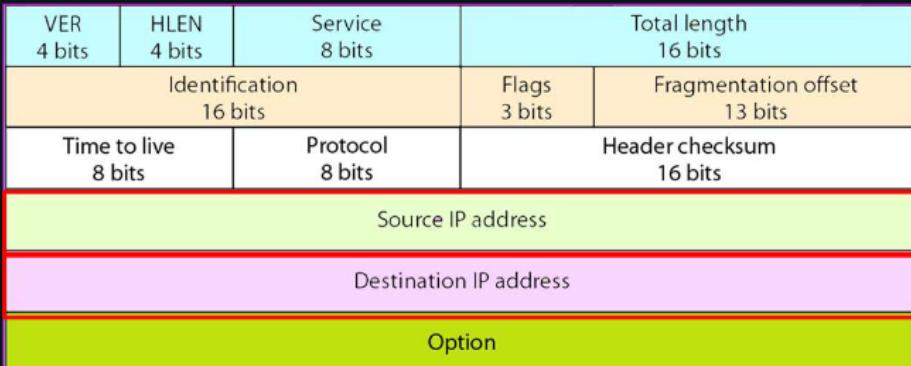


HEADER CHECKSUM – 16 BITS

Used for Error Detection

IPv4 Datagram Format Header Checksum -16 bits Neso Academy

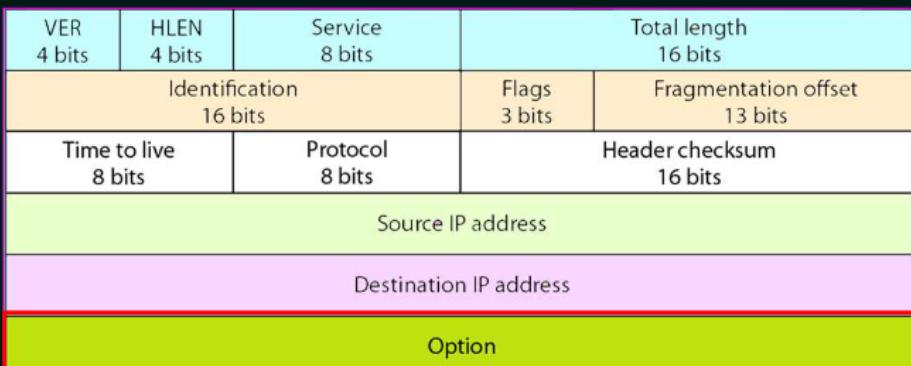
IPv4 DATAGRAM FORMAT



SOURCE AND DESTINATION IP ADDRESS – 32 BITS

IPv4 Datagram Format Source and Destination IP Address -32 bits Neso Academy

IPv4 DATAGRAM FORMAT



OPTIONS, DATA AND PADDING

IPv4 Datagram Format Options, Data and Padding Neso Academy

QUESTION

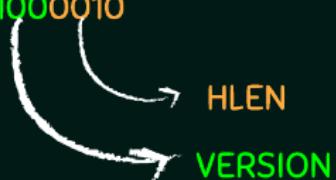
An IPv4 packet has arrived with the first 8 bits as shown: 01000010. The receiver discards the packet. Why?

Neso Academy

QuestionNeso Academy

SOLUTION

Given: The first 8 bits of IP Packet is 01000010



Neso Academy

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 $8 \times 4 = 32$ 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

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 $5 \times 4 = 20$ bytes.

So obviously there is no options in the IP packet.

The total length is 28 in Hexadecimal.

SolutionNeso Academy

HEXADECIMAL TO DECIMAL CONVERSION

Convert 28_{16} into decimal.

$$\begin{array}{r} 2 \ 8 \\ \curvearrowright \end{array} \quad \begin{aligned} 8 \times 16^0 &= 8 \times 1 = 8 \\ 2 \times 16^1 &= 2 \times 16 = 32 \\ \hline & 40 \end{aligned}$$

Therefore $28_{16} = 40_{10}$

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 $5 \times 4 = 20$ 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 FORMAT

| | | | | | | | | | |
|---------------------------|--------------------|----------------------------|---------------------------------|--|--|--|--|--|--|
| VER 4 bits | HLEN 4 bits | Service 8 bits | Total length 16 bits | | | | | | |
| Identification 16 bits | | Flags 3 bits | Fragmentation offset 13 bits | | | | | | |
| Time to live 8 bits | Protocol 8 bits | Header checksum 16 bits | | | | | | | |
| Source IP address | | | | | | | | | |
| Destination IP address | | | | | | | | | |
| Option | | | | | | | | | |

TIME TO LIVE (TTL) – 8 BITS

- ★ Number of hops this datagram has traveled.
- ★ Prevents looping of IP packets in the network.

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

TIME-TO-LIVE (TTL)

- ★ TTL is an 8-bit field.
- ★ In the IPv4 header, TTL is the 9th octet of 20.
- ★ In the IPv6 header, it is the 8th octet of 40.
- ★ The maximum TTL value is 255, the maximum value of a single octet.
- ★ A recommended initial TTL value is 64.
- ★ The time-to-live value can be thought of as an upper bound on the time that an IP datagram can exist in an Internet system.
- ★ The TTL field is set by the sender of the datagram, and reduced by every router on the route to its destination.

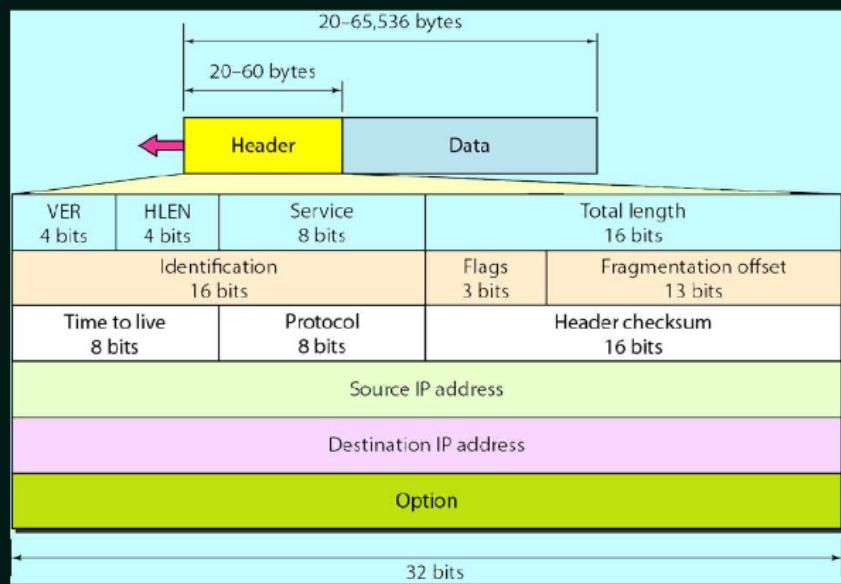
★★★★★ Time-To-Live (TTL) Neso Academy

TIME-TO-LIVE (TTL)

- ★ If the TTL field reaches zero before the datagram arrives at its destination, then the datagram is discarded and an ICMP error datagram (11 - Time Exceeded) is sent back to the sender.
- ★ The purpose of the TTL field is to avoid looping of IP packets in the internet.
- ★ In theory, under IPv4, time to live is measured in seconds, although every host that passes the datagram must reduce the TTL by at least one unit.
- ★ In practice, the TTL field is reduced by one on every hop.
- ★ To reflect this practice, this TTL field is renamed as hop limit in IPv6.

★★★★★ Time-To-Live (TTL) Neso Academy

IPv4 DATAGRAM FORMAT



IPv4 Datagram Format Neso Academy

QUESTION

An IPv4 packet has arrived with the first few hexadecimal digits as shown.

0x45000028000100000102 ...

How many hops can this packet travel before being dropped? The data belong to what upper-layer protocol?

QuestionNeso Academy

SOLUTION

Given:

0x45000028000100000102 ...

To find:

1. TTL Field

2. Protocol Field

0x45000028000100000102 ...

Version (4 bits)

SolutionNeso Academy

SOLUTION

Given:

0x45000028000100000102 ...

To find:

1. TTL Field
2. Protocol Field

0x45000028000100000102 ...

HLen (4 bits)

Neso Academy

SolutionNeso Academy

SOLUTION

Given:

0x45000028000100000102 ...

To find:

1. TTL Field
2. Protocol Field

0x45000028000100000102 ...

Service (8 bits)

Neso Academy

SolutionNeso Academy

SOLUTION

Given:

0x45000028000100000102 ...

To find:

1. TTL Field
2. Protocol Field

0x45000028000100000102 ...

 Total Length (16 bits)

Neso Academy

SOLUTION

Given:

0x45000028000100000102 ...

To find:

1. TTL Field
2. Protocol Field

0x45000028000100000102 ...

 Identification (16 bits)

Neso Academy

SolutionNeso Academy

SOLUTION

Given:

0x45000028000100000102 ...

To find:

1. TTL Field
2. Protocol Field

0x45000028000100000102 ...

↳ Flags/Fragmentation Offset (3+13=16 bits)

SolutionNeso Academy

SOLUTION

Given:

0x45000028000100000102 ...

To find:

1. TTL Field
2. Protocol Field

0x45000028000100000102 ...

↳ TTL (8 bits)

SolutionNeso Academy

SOLUTION

Given:

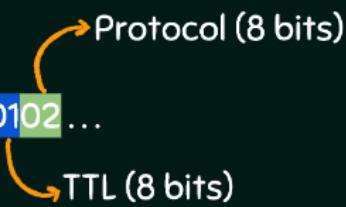
0x45000028000100000102 ...

To find:

1. TTL Field

2. Protocol Field

0x45000028000100000102 ...



SolutionNeso Academy

SOLUTION

Given:

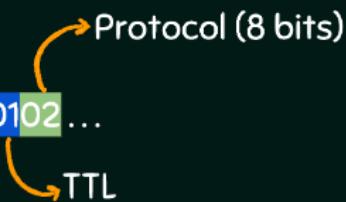
0x45000028000100000102 ...

To find:

1. TTL Field

2. Protocol Field

0x45000028000100000102 ...



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).

SolutionNeso Academy

SOLUTION

Given:

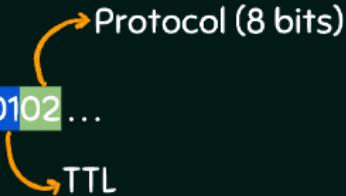
0x45000028000100000102 ...

To find:

1. TTL Field

2. Protocol Field

0x45000028000100000102 ...



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.

Solution★ Neso Academy

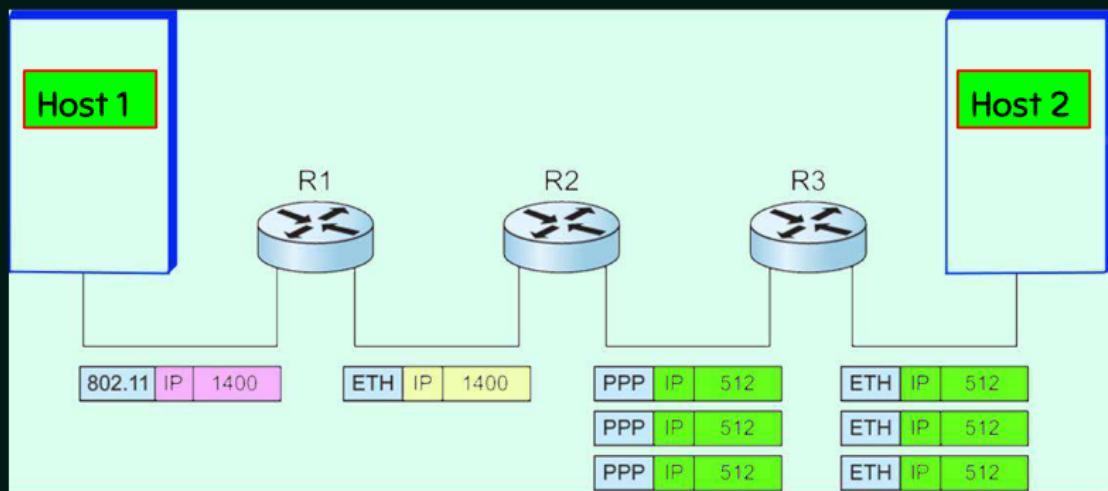
OUTCOMES

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.

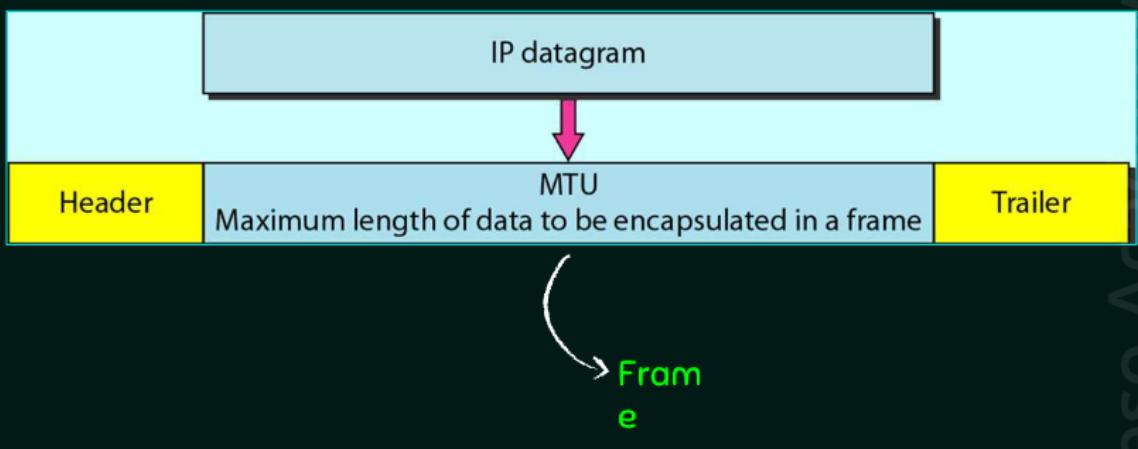
Fragmentation★★★Neso Academy

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!



Analogy! 12 L 14 L 5 L 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

OUTCOMES

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

- ★ Understand the fields related to fragmentation and reassembly.
- ★ Understand the fragmentation process.

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

- ★ 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.



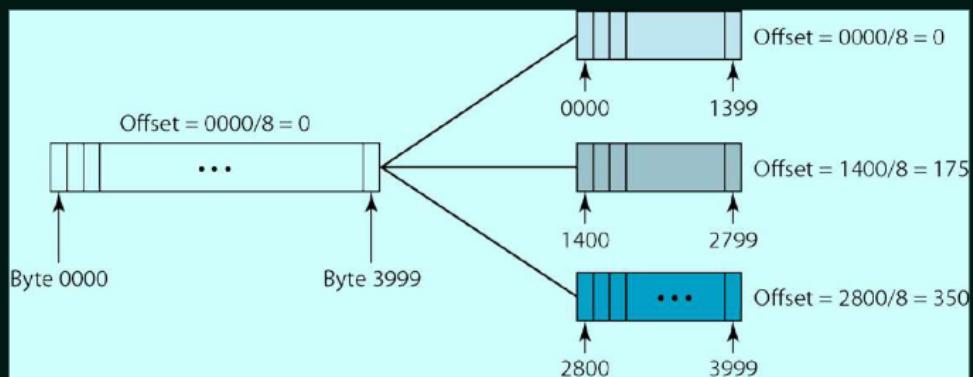
2. Flags★★★★★★★★Neso Academy

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.

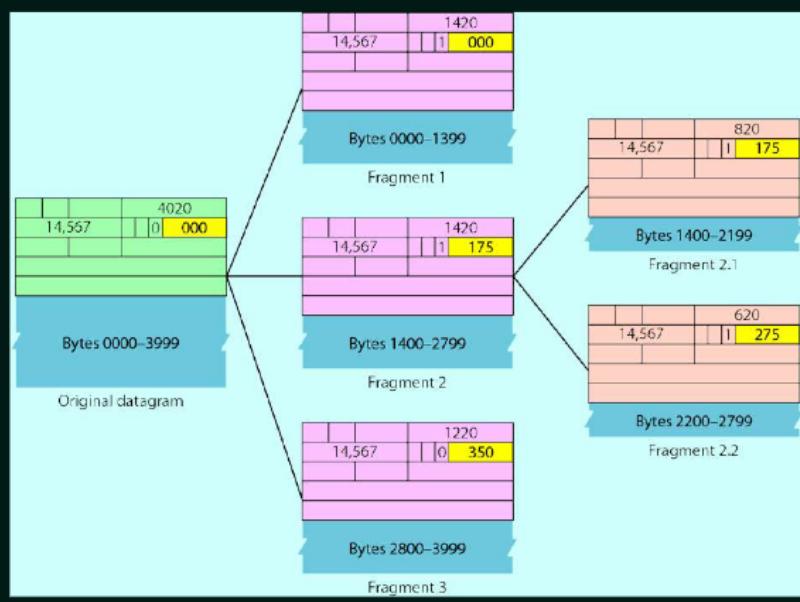
3. Fragmentation Offset ★★★★ Neso Academy

FRAGMENTATION PROCESS



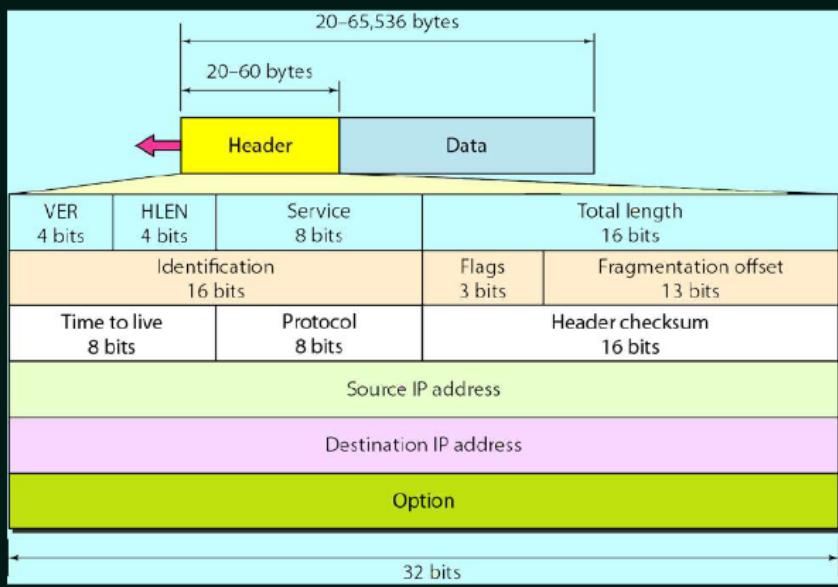
Fragmentation Process Neso Academy

FRAGMENTATION PROCESS



Fragmentation ProcessNeso Academy

IPv4 DATAGRAM FORMAT

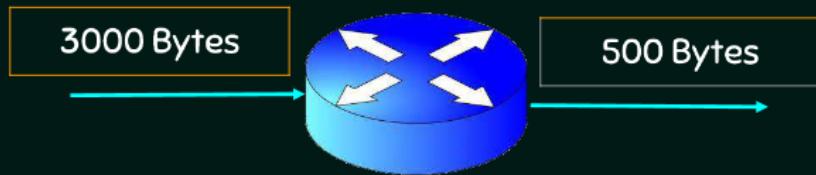


IPv4 Datagram FormatNeso Academy

QUESTION

Consider an IP packet with a length of 3000 bytes is forwarded to an IPv4 router that supports a Maximum Transmission Unit (MTU) of 500 bytes.

- Find the number of fragments.
- Details of all fragments with M flag, Offset and Total length.

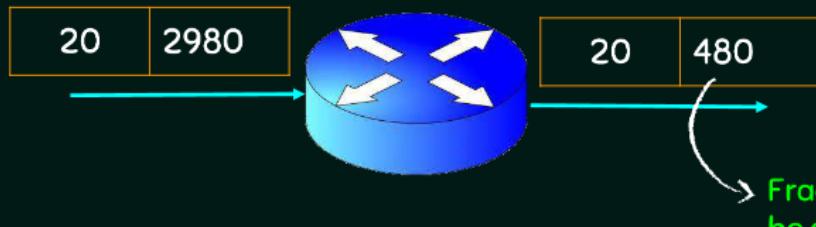


QuestionNeso Academy

QUESTION

Consider an IP packet with a length of 3000 bytes is forwarded to an IPv4 router that supports a Maximum Transmission Unit (MTU) of 500 bytes.

- Find the number of fragments.
- Details of all fragments with M flag, Offset and Total length.



QuestionNeso Academy

SOLUTION

a. Find the number of fragments

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

$$\text{No. of fragments} = \left\lceil \frac{2980}{480} \right\rceil$$

$$\text{No. of fragments} = \left\lceil 6.208 \right\rceil$$

$$\text{No. of fragments} = 7$$

Neso Academy

SolutionNeso Academy

SOLUTION

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

Note: Fragment size must be a multiple of 8.

| | F1 | F2 | F3 | F4 | F5 | F6 | F7 |
|-----------|----|----|----|----|----|----|----|
| Len | | | | | | | |
| Total Len | | | | | | | |
| M Flag | | | | | | | |
| Offset | | | | | | | |

Neso 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

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

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

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

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 | 4468 |
| 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

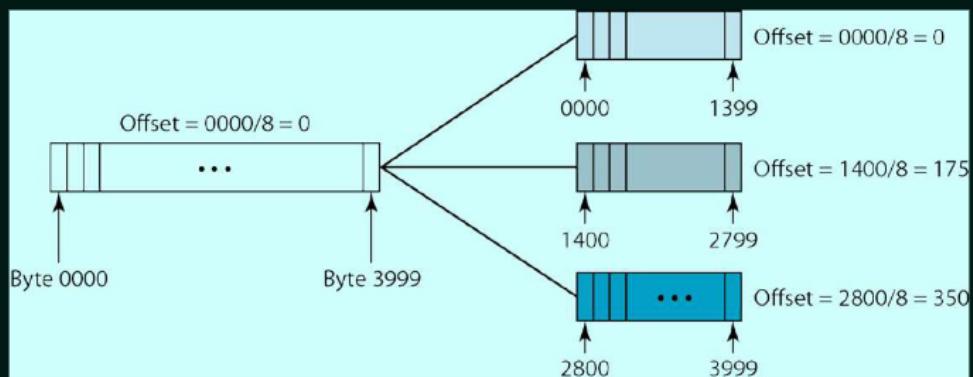
In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively are

[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.

∴ 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

$$\begin{aligned}\text{The last byte number} &= \text{first byte number} + \text{total bytes in payload} - 1 \\ &= 2400 + 360 - 1 \\ &= 2759\end{aligned}$$

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

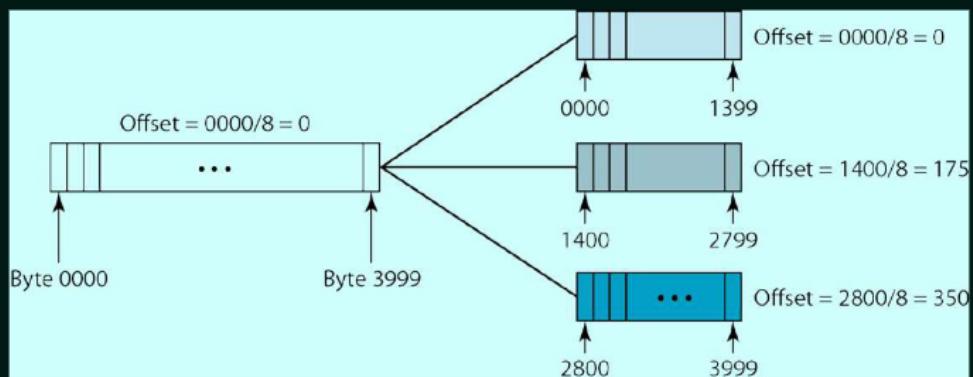
Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e. MTU = 1500 bytes). Size of UDP header is 8 bytes and size of IP header is 20 bytes. There is no option field in IP header. How many total number of IP fragments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



$$\text{Offset of F1} = (1400 \times 0)/8$$

$$\text{Offset of F2} = (1400 \times 1)/8$$

$$\text{Offset of F3} = (1400 \times 2)/8$$

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.

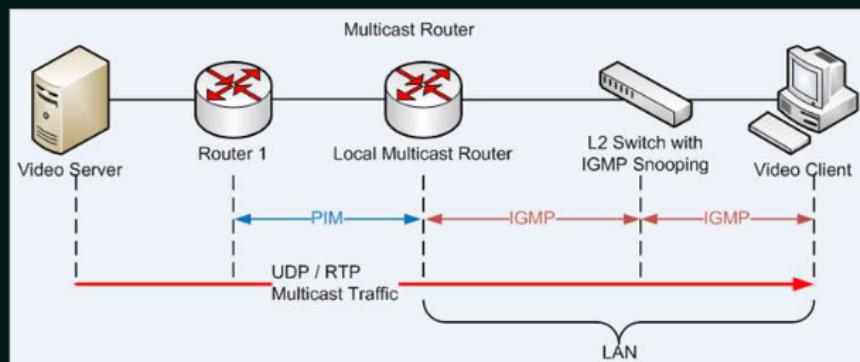
Outcomes★★★Neso Academy

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



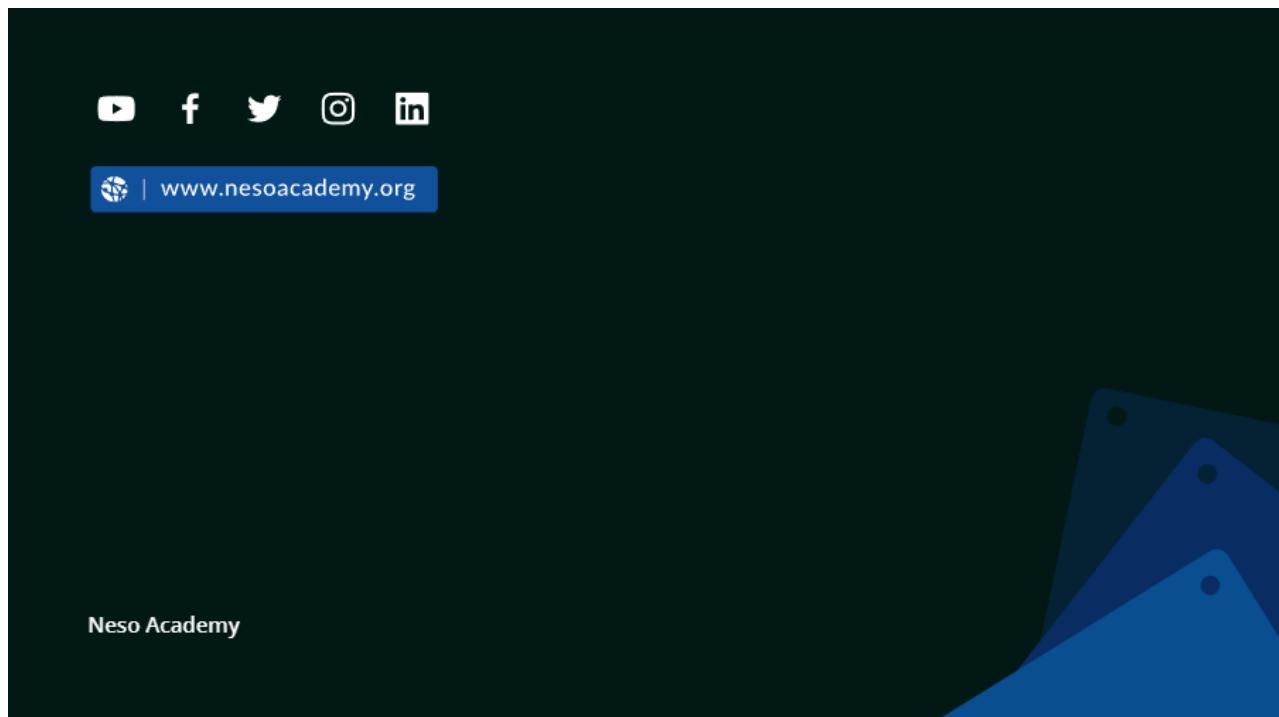
- ★ IGMP operates between a host and a local multicast router.
- ★ Switches featuring IGMP snooping derive useful information by observing these IGMP transactions.
- ★ Protocol Independent Multicast (PIM) is then used between the local and remote multicast routers, to direct multicast traffic from hosts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