1. Write the difference between IPv4 an IPv6.

IPv4	IPv6
The address length is 32 bits	The address length is 128 bits.
The IPv4 header length is variable 20 to 60 bytes.	The IPv6 header length is fixed 40 bytes.
It can be represented in dotted-decimal, hexadecimal, or binary notations.	It can be represented in binary notation or colon hexadecimal notations.
It supports broadcasting.	It does not support broadcasting.
It does not have inbuilt security feature.	It has in-built security feature. IPSec protocol is in built in the IPv6
Sender and intermediate router both can fragment the datagram.	Sender can only fragment the datagram which intermediate router cannot.
Options field is present in the IPv4 datagram header.	Options field is not present in the IPv6 datagram header but all the facilities of it are provided by the six-extension headers.
The checksum field is present in the IPv4 datagram header	The checksum field is not present in the datagram header.
IPv4 consists of 4 fields which are separated by addresses dot (.)	Pv6 consists of 8 fields, which are separated by a colon (:)
IPv4's IP addresses are divided into five different classes. Class A, Class B, Class C, Class D, Class E.	IPv6 does not have any classes of the IP address.
IPv4 supports VLSM (Variable Length subnet mask).	IPv6 does not support VLSM.
Example: 192.168.1.1	Example: 2001:0000:3238: DFE1:0063:0000:0000:FEFB

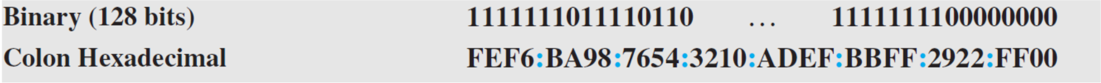
2. Explain the advantages of IPv6 when compared to IPv4.

- **Larger address space**
  - IPv6 has larger address space i.e., 128 bits than the IPv4.
- **Better header format.**
  - IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the data.
  - This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
- **New options.**
  - IPv6 has new options to allow for additional functionalities.
- **Allowance for extension.**
  - IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
- **Support for resource allocation.**

  - In IPv6, the type-of-service field has been removed, but two new fields, traffic class and flow label, have been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.
- **Support for more security.**
  - The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

3. Explain two different representation of IPv6 address .

- An IPv6 address is 128 bits or 16 bytes (octets) long, four times the address length in IPv4.
- The following notations have been proposed to represent IPv6 addresses when they are handled by humans.
  - binary
  - colon hexadecimal



Binary (128 bits)	**1111111011110110 . . . 1111111100000000**
Colon Hexadecimal	**FEF6:BA98:7654:3210:ADEF:BBFF:2922:FF00**

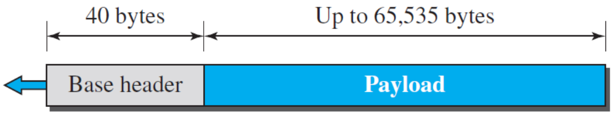
- Binary notation is used when the addresses are stored in a computer.
- The colon hexadecimal notation (or colon hex for short) divides the address into eight sections, each made of four hexadecimal digits separated by colons.

4. Write a short note on three destination address types of IPv6 address.

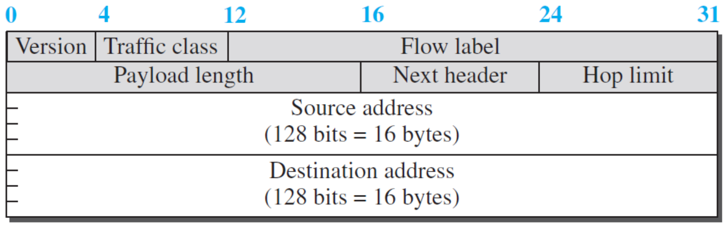
- In IPv6, a destination address can belong to one of three categories:
  - Unicast
  - Anycast
  - multicast.
- Unicast Address
  - A unicast address defines a single interface (computer or router).
  - The packet sent to a unicast address will be routed to the intended recipient.
- Anycast Address
  - An anycast address defines a group of computers that all share a single address.
  - A packet with an anycast address is delivered to only one member of the group, the most reachable one.
  - An anycast communication is used, for example, when there are several servers that can respond to an inquiry. The request is sent to the one that is most reachable.
  - IPv6 does not designate a block for any casting; the addresses are assigned from the unicast block.
- Multicast
  - A multicast address also defines a group of computers. In multicasting each member of the group receives a copy of the message from the sender.
  - IPv6 has designated a block for multicasting from which the same address is assigned to the members of the group.
  - It is interesting that IPv6 does not define broadcasting, even in a limited version.
  - IPv6 considers broadcasting as a special case of multicasting.

5. Explain IPv6 header packet format.

- The IPv6 packet format is shown in the figure below.



a. IPv6 packet



b. Base header

- Each packet is composed of a base header followed by the payload.
- The base header occupies 40 bytes, whereas payload can be up to 65,535 bytes of information.
- The description of fields is as follows.
- **Version.**
  - The 4-bit version field defines the version number of the IP. For IPv6, the value is 6.
- **Traffic class.**
  - The 8-bit traffic class field is used to distinguish different payloads with different delivery requirements.
  - It replaces the type-of-service field in IPv4.
- **Flow label.**
  - The flow label is a 20-bit field that is designed to provide special handling for a particular flow of data.
- **Payload length.**
  - The 2-byte payload length field defines the length of the IP datagram excluding the header.
  - Note that IPv4 defines two fields related to the length: header length and total length.
  - In IPv6, the length of the base header is fixed (40 bytes); only the length of the payload needs to be defined.
- **Next header.**
  - The next header is an 8-bit field defining the type of the first extension header (if present) or the type of the data that follows the base header in the datagram.
  - This field is similar to the protocol field in IPv4.
- **Hop limit.**
  - The 8-bit hop limit field serves the same purpose as the TTL field in IPv4.
- **Source and destination addresses.**
  - The source address field is a 16-byte (128-bit) Internet address that identifies the original source of the datagram.
  - The destination address field is a 16-byte (128-bit) Internet address that identifies the destination of the datagram.
- **payload.**
  - Compared to IPv4, the payload field in IPv6 has a different format and meaning, as shown in Figure below.

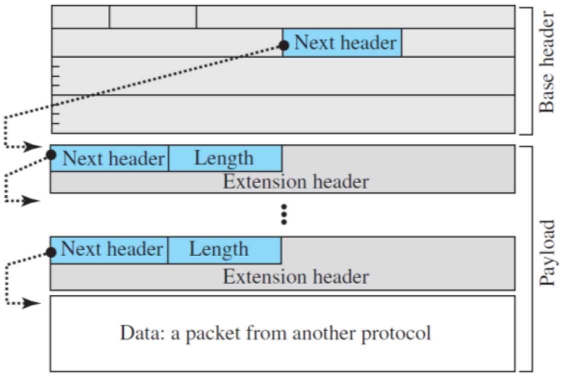
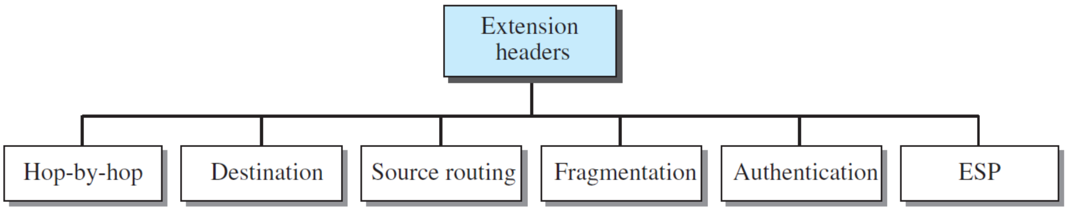


Figure 2.2.1.2 Payload in IPv6 datagram

- The payload in IPv6 means a combination of zero or more extension headers (options) followed by the data from other protocols (UDP, TCP, and so on).

6. List and explain all types of extension header IPv6.

- An IPv6 packet is made of a base header and some extension headers.
- The length of the base header is fixed at 40 bytes. However, to give more functionality to the IP datagram, the base header can be followed by up to six extension headers.
- These six types of extension headers are shown in the following figure.

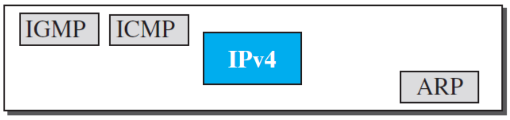


- **Hop-by-hop option**
  - The hop-by-hop option is used when the source needs to pass information such as debugging, datagram length etc. to all routers visited by the datagram.
  - There are three hop-by- hop options have been defined: Pad1, PadN, and jumbo payload.
- **Destination Option**
  - The destination option is used when the source needs to pass information to the destination only.
  - The format of the destination option is the same as the hop-by-hop option.
  - So far, only the Pad1 and PadN options have been defined.
- **Source routing**
  - The source routing extension header combines the concepts of the strict source route and the loose source route options of IPv4.
- **Fragmentation**
  - The Fragmentation extension header in IPv6 is used to fragment packets that are larger than the maximum transmission unit (MTU) of the network over which they are to be transmitted. The MTU is the largest packet size that can be transmitted over a given network without fragmentation.
- **Authentication**
  - The authentication extension header has a dual purpose: Sender Authentication and Data integrity.

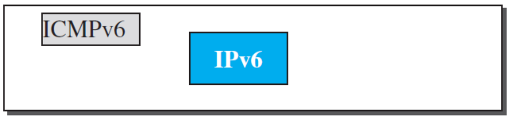
- **Encrypted security payload**
    - The encrypted security payload (ESP) is an extension that provides confidentiality and guards against eavesdropping.

7. Write a short note on ICMPv6.

- Internet Control Message Protocol version 6 (ICMPv6), follows the same strategy and purposes of version 4 i.e. error reporting and diagnostics functions.
- ICMPv6, however, is more complicated than ICMPv4: some protocols that were independent in version 4 are now part of ICMPv6 and some new messages have been added to make it more useful.
- Following Figure compares the network layer of version 4 to that of version 6. The ICMP, ARP, and IGMP protocols in version 4 are combined into one single protocol, ICMPv6.



Network layer in version 4



Network layer in version 6

- The messages in ICMPv6 can be categorized into four groups:
    - Error-reporting messages
    - Informational messages
    - Neighbor-discovery messages which fulfils the functionalities of the ARP and RARP protocols.
    - Group-membership messages which fulfil the functionalities of IGMP protocol.

8. Explain different categories of ICMPv6 messages.

- The messages in ICMPv6 can be categorized into four groups:
    - Error-reporting messages
    - Informational messages
    - Neighbor-discovery messages
    - Group-membership messages
- Error-Reporting Messages
    - The main responsibilities of ICMPv6 is to report errors.
    - Four types of errors are handled:
        - destination unreachable
            - When a router cannot forward a datagram or a host cannot deliver the content of the datagram to the upper layer protocol, the router or the host discards the datagram and sends a destination-unreachable error message to the source host.
        - packet-too-Big
            - Since IPv6 does not fragment at the router, if a router receives a datagram that is larger than the maximum transmission unit (MTU) size of the network through which the datagram should pass, it discards the datagram and send ICMP error packet – a packet-too-big message to the source.
        - time exceeded

            - A time-exceeded error message is generated in two cases: When the time to live value becomes zero and when not all fragments of a datagram have arrived in the time limit.
        - parameter problems.
            - If a router or the destination host discovers any ambiguous or missing value in any field, it discards the datagram and sends a parameter message to the source.

- Informational Messages
    - Two of the ICMPv6 messages can be categorized as informational messages:
        - echo request
        - echo reply messages.
    - The echo-request and echo-reply messages are designed to check whether two devices in the Internet can communicate with each other.
    - A host or router can send an echo-request message to another host; the receiving computer or router can reply using the echo-reply message.
- Neighbor-Discovery Messages
    - Several messages in ICMPv4 have been redefined in ICMPv6 to handle the issue of neighbor discovery. Some new messages have also been added to provide extension.
    - Router-Solicitation Message
        - A host uses the router-solicitation message to find a router in the network that can forward an IPv6 datagram for the host.
    - Router-Advertisement Message
        - The router-advertisement message is sent by a router in response to a router solicitation message.
    - Neighbor-Solicitation Message
        - The neighbor solicitation message has the same duty as the ARP request message.
        - The neighbor-solicitation message is used to find the data-link address of the neighbor from the IP address.
    - Neighbor-Advertisement Message
        - The neighbor-advertisement message is sent in response to the neighbor-solicitation message.
    - Redirection Message
        - This type of message is generated for the wrong route address and inform the source.
    - Inverse-Neighbor-Solicitation Message
        - The inverse-neighbor-solicitation message is sent by a node that knows the link-layer address of a neighbor, but not the neighbor’s IP address.
    - Neighbor-Advertisement Message
        - The inverse-neighbor-advertisement message is sent in response to the inverse-neighbor discovery message.
- Group Membership Messages
    - There are two types of group membership messages.
    - Membership-Query Message
        - A membership-query message is sent by a router to find active group members in the network.

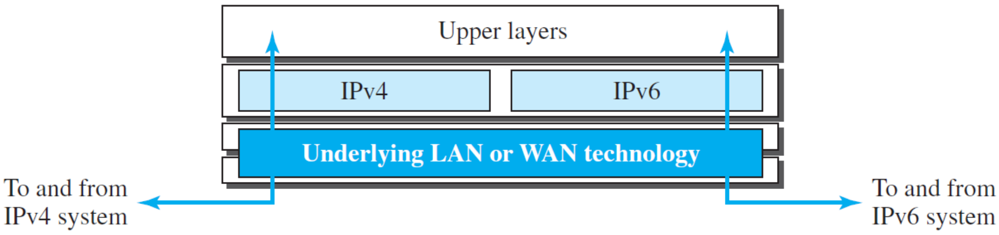
- Membership-Report Message
  - A membership-report message is the response generated by the router for the membership-query message. It indicates that particular router is the member of the particular group.

9. Explain three strategies of transition from IPv4 to IPv6.

- Because of the huge number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen suddenly.
- It will take a considerable amount of time before every system on the Internet can move from IPv4 to IPv6.
- The transition must be smooth to prevent any problems between IPv4 and IPv6 systems.
- There are three strategies have been devised for transition:
  - Dual stack,
  - Tunnelling,
  - Header translation.
- One or all of these three strategies can be implemented during the transition period.

Dual Stack

- It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols during the transition. In other words, a station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6.
- The layout of a dual-stack configuration is shown in the figure below.

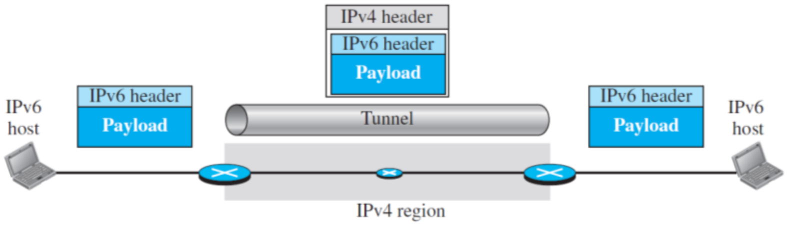


Dual Stack Strategy

- To determine which version to use when sending a packet to a destination, the source host queries the DNS.
- If the DNS returns an IPv4 address, the source host sends an IPv4 packet.
- If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

Tunnelling

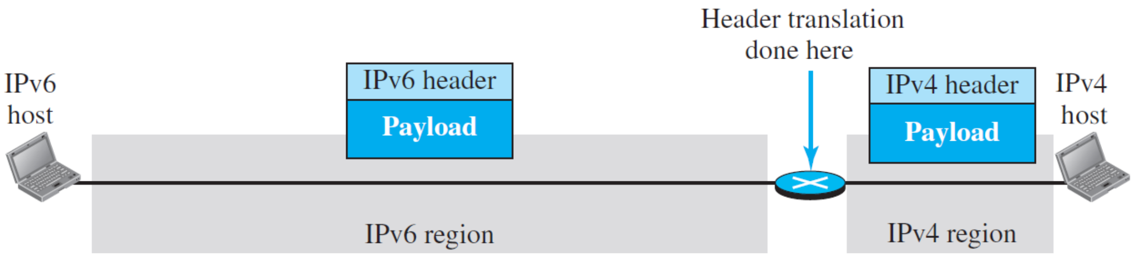
- Tunnelling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4.
- To pass through this region, the packet must have an IPv4 address.
- So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region.
- It seems as if the IPv6 packet enters a tunnel at one end and emerges at the other end.
- Tunnelling is shown in the figure below.



Tunnelling Strategy

Header Translation

- Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4.
- The sender wants to use IPv6, but the receiver does not understand IPv6.
- Tunneling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver.
- In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header
- The header translation strategy is shown in the figure below.



Header Translation Strategy

10. Explain the use of the flow field in IPv6. What is the potential application of this field?

- The flow label is a 20-bit field that is designed to provide special handling for a particular flow of data.
- The flow label makes the IPv6 protocol as connection oriented.
- A router that supports the handling of flow labels has a flow label table.
- When the router receives a packet, it consults its flow label table to find the corresponding entry for the flow label value defined in the packet.
- In its simplest form, a flow label can be used to speed up the processing of a packet by a router.
- a flow label can be used to support the transmission of real-time audio and video. Real-time audio or video, particularly in digital form, requires resources such as high bandwidth, large buffers, long processing time, and so on.

11. Distinguish between compatible and mapped addresses and explain their applications.

Compatible Address	Mapped Address
A compatible address is an address of 96 bits of 0s followed by 32 bits of an IPv4 address.	A mapped address is an address of 80 bits of 0s followed by 16 bits of 1s and followed by 32 bits of an IPv4 address.

A compatible address is used when a computer using IPv6 wants to send a packet to another computer using IPv6.	A mapped address is used when a computer using IPv6 wants to send a packet to a computer still using IPv4.

12. **List three protocols in the IPv4 network layer that are combined into a single protocol in IPv6.**

- The three companion protocols ARP, IGMP and ICMP of IPv4 protocol are combined into single protocol IPv6.

13. **What is the purpose of including the IP header and the first 8 bytes of datagram data in the error-reporting ICMP messages?**

- The IP header is included because it contains the IP address of the original source.
- The first 8 bytes of the data are included because they contain the first section of the TCP or UDP header which contains information about the port numbers (TCP and UDP) and sequence number (TCP).
- This information allows the source to direct the ICMP message to the correct application.

14. **If you are assigned an IPv6 address by your ISP for your personal computer at home, what should be the first (leftmost) three bits of this address?**

- The ISP assigns an IPv6 address from the global unicast address block of IPv6. So, the first(leftmost) three bits of this address should be 001.

15. **Find the size of the global unicast block from Table given below.**

Block Prefix	CIDR	Block Assignment	Fraction
001	2000::/3	Global Unicast	1/8

- The prefix length is 3. So, the block size is N = 2^{128-3}=2^{125}

16. **Find the size of the special address block from Table given below.**

Block Prefix	CIDR	Block Assignment	Fraction
0000 0000	0000::/8	Special Address	1/256

- The prefix length is 8. So, the block size is N = 2^{128-8}=2^{120}

17. **Find the size of the unique local unicast block from Table given below.**

Block Prefix	CIDR	Block Assignment	Fraction
1111 110	FC00::/7	Unique local unicast	1/128

- The prefix length is 7. So, the block size is N = 2^{128-7}=2^{121}

18. **Find the size of the multicast block from Table given below.**

Block Prefix	CIDR	Block Assignment	Fraction
1111 1111	FF00::/8	Multicast Addresses	1/256

- The prefix length is 8. So, the block size is N = 2^{128-8}=2^{120}

19. **Explain autoconfiguration in the IPv6.**

- In IPv6, DHCP protocol can still be used to allocate an IPv6 address to a host, but a host can also configure itself.

- When a host in IPv6 joins a network, it can configure itself using the following process:
  1. The host first creates a link local address for itself. This is done by taking the 10-bit link local prefix (1111 1110 10), adding 54 zeros, and adding the 64-bit interface identifier, which any host knows how to generate from its interface card. The result is a 128-bit link local address.
  2. The host then tests to see if this link local address is unique and not used by other hosts. The host sends a neighbor solicitation message and waits for a neighbor advertisement message. If any host in the subnet is using this link local address, the process fails, and the host cannot autoconfigure itself; it needs to use other means such as DHCP for this purpose.
  3. If the uniqueness of the link local address is passed, the host stores this address as its link local address (for private communication), but it still needs a global unicast address. The host then sends a router solicitation message to a local router. If there is a router running on the network, the host receives a router advertisement message that includes the global unicast prefix and the subnet prefix that the host needs to add to its interface identifier to generate its global unicast address. If the router cannot help the host with the configuration, it informs the host in the router advertisement message (by setting a flag). The host then needs to use other means for configuration.
- Autoconfiguration in IPv6 provides the following benefits:
  - Reduced administrative overhead.
  - Improved scalability.
  - Increased reliability.
  - Improved security.

20. What is renumbering in IPv6.

- Renumbering in IPv6 is the process of changing the IPv6 address prefix of a device or network. This may be necessary for a number of reasons, such as:
  - Changing internet service providers (ISPs)
  - Merging or acquiring another company
  - Expanding into a new geographic region
  - Implementing a new network design
- IPv6 renumbering can be a complex process, and it is important to carefully plan and execute it in order to avoid disruptions to services.

21. Which field in the IPv6 packet is responsible for multiplexing and demultiplexing?

- The next header field is responsible for multiplexing and demultiplexing in IPv6. It is similar to the protocol field in IPv4.

22. Assume a datagram carries no option. Do we still need a value for the next header field in IPv6 header?

- Yes, we still need a value for the Next Header field in the IPv6 header, even if the datagram carries no options.
- The Next Header field identifies the next header in the packet, either an upper layer protocol (such as TCP or UDP) or an extension header (such as fragmentation header or routing header).
- If there are no options in the datagram, then the value of the Next Header field is simply the next header in the packet. For example, if the datagram contains a TCP segment, then the value of the Next Header field is 6 (TCP).
- The Next Header field is a required field in the IPv6 header, and it must be set to a valid value, even if there are no options in the datagram.

23. Which message in version 6 replaces the ARP request message in version 4? Which replaces the ARP reply message?

- The neighbor-solicitation message in ICMPv6 replaces the ARP request message in version 4.
- The neighbor-advertisement message in ICMPv6 replaces the ARP reply message in version 4.

24. In which transition strategy do we need to encapsulate IPv6 packets in the IPv4 packets?

- We need to encapsulate IPv6 packets in IPv4 packets in the tunneling strategy.

25. In which transition strategy do we need to have both IPv4 and IPv6 in the path?

- We need to have both IPv4 and IPv6 protocol in the dual stack transition strategy.

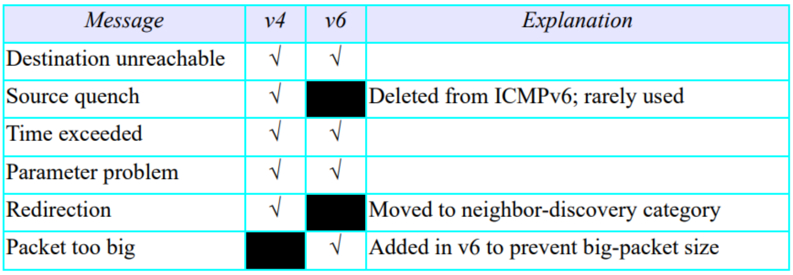
26. Compare and contrast the IPv4 header with the IPv6 header. Create a table to compare each field.

The following table shows comparison.

Field	IPv4	IPv6
VER	Yes	Yes
HLEN	Yes	No
Service(or traffic class)	Yes	Yes
Flow Label	No	Yes
Total Length	Yes	No
Payload length	No	Yes
Identification	Yes	No
Flags	Yes	No
Flag offset	Yes	No
TTL(or Hop limit)	Yes	Yes
Protocol	Yes	No
Checksum	Yes	No
Source address	Yes	Yes
Destination address	Yes	Yes

27. Make a table to compare and contrast error-reporting messages in ICMPv6 with error-reporting messages in ICMPv4.

- The error-reporting messages in ICMPv4 and ICMPv6 are similar except that some messages have been totally deleted in version 6 or has been inserted in other categories.
- The following table shows a comparison.



Message	*v4*	*v6*	*Explanation*
Destination unreachable	√	√	
Source quench	√	■	Deleted from ICMPv6; rarely used
Time exceeded	√	√	
Parameter problem	√	√	
Redirection	√	■	Moved to neighbor-discovery category
Packet too big	■	√	Added in v6 to prevent big-packet size

28. Make a table to compare and contrast informational messages in ICMPv6 with informational messages in ICMPv4.

- The informational messages were known as query messages in the ICMPv4.
- The following table shows the comparison.

Message	***V4***	***V6***	***Explanation***
Echo request and Echo Reply	✓	✓	
Echo reply	✓	✓	
Timestamp request	✓	■	Not defined in the ICMPv6
Timestamp reply	✓	■	Not defined in the ICMPv6

29. Make a table to compare and contrast neighbor-discovery messages in ICMPv6 with the corresponding messages in version 4.

- The neighbor-discovery category is new in ICMPv6.
- In ICMPv4, one of these messages belonged to another category; the duties of others were covered by other protocols.
- The following table shows a comparison.

Message	*v4*	*v6*	*Explanation*
Router solicitation	■	√	Version 4 uses DHCP for this purpose
Router advertisement	■	√	Version 4 uses DHCP for this purpose
Neighbor solicitation	■	√	Version 4 uses ARP request packet
Neighbor advertisement	■	√	Version 4 uses ARP reply packet
Redirection	■	√	Included in error-reporting group in v4

30. Make a table to compare and contrast inverse neighbor-discovery messages in ICMPv6 with the corresponding messages in version 4.

- The inverse neighbor-discovery category is new in ICMPv6.
- The following table shows a comparison

Message	***V4***	***V6***	***Explanation***
Inverse-Neighbor-Solicitation Message	■	✓	Version 4 uses RARP request packet
Inverse-Neighbor-Advertisement Message	■	✓	Version 4 uses RARP reply packet

31. Make a table to compare and contrast group-membership messages in ICMPv6 with the corresponding messages in version 4.

- Group membership messages are new in Version 6. Version 4 is using IGMP protocol for this purpose.
- The following table shows a comparison.

Message	*v4*	*v6*	*Explanation*
Membership query	■	√	It was part of IGMP protocol in v4.
Membership report	■	√	It was part of IGMP protocol in v4.

32. Show the unabbreviated colon hex notation for the following IPv6 addresses:

a. **An address with 64 0s followed by 32 two-bit (01)s.**

0000:0000:0000:0000:5555:5555:5555:5555

b. **An address with 64 0s followed by 32 two-bit (10)s.**

0000:0000:0000:0000:AAAA: AAAA: AAAA: AAAA

c. An address with 64 two-bit (01)s.

5555:5555: 5555:5555: 5555:5555: 5555:5555

d. An address with 32 four-bit (0111)s.

7777: 7777: 7777: 7777: 7777: 7777: 7777:7777

33. Show abbreviations for the following addresses:

a. 0000:FFFF:FFFF:0000:0000:0000:0000:0000

0:FFFF:FFFF::

b. 1234:2346:3456:0000:0000:0000:0000:FFFF

1234:2346:3456::FFFF

c. 0000:0001:0000:0000:0000:FFFF:1200:1000

0:1::FFFF:1200:1000

d. 0000:0000:0000:0000:FFFF:FFFF:24.123.12.6

::FFFF:FFFF:24.123.12.6

34. Decompress the following addresses and show the complete unabbreviated IPv6 address:

a. ::2222

0000:0000:0000:0000:0000:0000:0000:2222

b. 1111::

1111:0000:0000:0000:0000:0000:0000:0000

c. B:A:CC::1234:A

000B:000A:00CC:0000:0000:0000:1234:000A

35. Show the original (unabbreviated) form of the following IPv6 addresses:

a. ::2

0000 :0000:0000:0000:0000:0000:0000:0002

b. 0:23::0

0000:0023:0000:0000:0000:0000:0000:0000

c. 0:A::3

0000:000A:0000:0000:0000:0000:0000:0003

36. What is the corresponding block or subblock associated with each of the following IPv6 addresses.

a. **FE80::12/10** – Link Local Addresses

b. **FD23::/7** – Unique local addresses

c. **32::/3** – Global unicast addresses

37. An organization is assigned the block 2000:1234:1423/48. What is the CIDR for the blocks in the first and second subnets in this organization?

- The first subnet block is 2000:1234:1423:0001/64.
- The second subnet block is 2000:1234:1423:0002/64.

38. Find the interface identifier if the physical address of the EUI is (F5-A9-23-AA-07-14-7A-23)$_{16}$ using the format we defined for Ethernet addresses.

- The interface identifier is F7A9:23AA:0714:7A23

39. Find the interface identifier if the Ethernet physical address is (F5-A9-23-12-7A-B2)$_{16}$ using the format we defined for Ethernet addresses.

- Change the seventh bit from 0 to 1(F5 to F7) and insert four extra hexadecimal digits (FF-FE) after the sixth digits.
- The interface identifier is F7A9:23FF:FE12:7AB2

40. An organization is assigned the block 2000:1110:1287/48. What is the IPv6 address of an interface in the third subnet if the IEEE physical address of the computer is (F5-A9-23-14-7A-D2)$_{16}$.

- The IPv6 address of an interface is 2000:1110:1287:0002:F7A9:23FF:FE14:7AD2

41. Using the CIDR notation, show the IPv6 address compatible to the IPv4 address 129.6.12.34.

- **:: 129.6.12.34/128**

42. Using the CIDR notation, show the IPv6 address mapped to the IPv4 address 129.6.12.34.

- ::FFFF:129.6.12.34/128

43. Using the CIDR notation, show the IPv6 loopback address.

- ::1/128

44. Using the CIDR notation, show the link local address in which the node identifier is 0::123/48.

- FE80::123/48

45. Using the CIDR notation, show the site local address in which the node identifier is 0::123/48.

- FC00::123/48