



Exam : 1D0-460

Title : CIW Internetworking Professional

Ver : 11.27.08

QUESTION 1:

Which extension header uses a variable-length Initialization vector (IV)?

- A. Authentication.
- B. Fragment.
- C. Encrypted security payload.
- D. Routing.

Answer: C

Explanation: Payload Data is a variable-length field containing data described by the Next Header field. The Payload Data field is mandatory and is an integral number of bytes in length. If the algorithm used to encrypt the payload requires cryptographic synchronization data, e.g., an Initialization Vector (IV), then this data MAY be carried explicitly in the Payload field. Any encryption algorithm that requires such explicit, per-packet synchronization data MUST indicate the length, any structure for such data, and the location of this data as part of an RFC specifying how the algorithm is used with ESP. If such synchronization data is implicit, the algorithm for deriving the data MUST be part of the RFC. (Reference RFC 2406)

Incorrect Answers:

A, B, D: These extension headers do not have the Initialization Vector.

QUESTION 2:

Which header field was created for packets that require special heading by IPv6 routers?

- A. The flow label field.
- B. The next header field.
- C. The protocol field.
- D. The payload length field.

Answer: A

Explanation:

A: The flow label field is used by the sender to label packets that require special processing at the router.

Incorrect Answers:

B: The next header field is used for identifying Ipv6 header extensions.

C: The protocol field was renamed to the next header field. The protocol field does not exist in Ipv6.

D: The payload length contains the size of the packet, excluding the size of the header.

QUESTION 3:

In IPv6, what does the Site-Level Aggregator identify?

- A. Individual locations.
- B. Backbone providers.
- C. Server location
- D. ISPs.

Answer: D

Explanation: An ISP can be identified by either a Site-Level Aggregator (SLA ID) or a Next-Level Aggregator (NLA ID). In the NLA, which is a Network Service Provider or ISP (Tier 2), so an ISP can fall if they support downstream service providers. An ISP can be a Site-Level Aggregator if it has downstream customers which are not service providers. The difference between a SLA and NLA depends on whether the address space is delegated.

Incorrect Answers:

- A: The are identified by the Interface ID.
- B: Internet Backbone Providers are identified by the Top Level Aggregator (TLA ID), and is considered Tier 1.
- C: The are identified by the Interface ID.

QUESTION 4:

Within the Encrypted Security payload (ESP) extension header, which of the following identifies the encryption association?

- A. Security Parameters Index (SPI)
- B. Payload Type.
- C. Padding.
- D. Sequence Number.

Answer: A

Explanation: By combining the SPI with the destination address and the Security Protocol (ESP) identifies the security association of the packet. The SPI is an unsigned 32-bit integer.

Incorrect Answers:

- B: The ESP header does not have a field called the payload type. There is payload data and payload length, for the length of the payload. The type of payload is actually stored in the next header field.
 - C: Padding are the characters added after the data payload. The number of padding characters is determined by a pad length. Padding is used to control the size and alignment of the message. The Pad Length indicates the number of 8-bit passing bytes to be added after the data. The padding ensures the message ends on a 64-bit boundary.
 - D: The sequence number is used for anti-replay.
-

QUESTION 5:

Why were checksums eliminated from IPv6?

- A. To introduce alternative error checking.
- B. To accommodate different topologies.
- C. To increase packet processing speed.
- D. To increase MTU discovery over networks.

Answer: C

Explanation: Checksums were eliminated to reduce overhead and speed packet processing. Calculation of the checksum was a mathematical operation that took time, and by eliminating it eliminated that overhead.

Incorrect Answers:

- A: The purpose was not to offer alternative checking, it was to get rid of the checking because checksums and CRC checks occurred in other places.
- B: The topology was not affected by the checksum, so having it would not affect any new or different topologies.
- D: The objective was to speed up all processing, and not directed at any one particular function.

QUESTION 6:

Which of the following choices lists the recommended sequence of IPv6 extension headers?

- A. Destination options, authentication, Hop-by-Hop, routing.
- B. Hop-by-hop, routing, destination options, authentication.
- C. Destination options, routing, hop-by-hop, authentication.
- D. Hop-by-hop, destination options, routing, authentication.

Answer: D

QUESTION 7:

What is the address prefix in binary for multicast addresses?

- A. 1111 1110 11
- B. 1111 1111
- C. 0000 010
- D. 1111 1110 10

Answer: B

Explanation: This question is confusing, since coding for Ipv4 is different than Ipv6. Lucily both encodings are not listed as possible answers. Hopefully the question on the exam will be worded more clearly.

An IPv6 multicast address is an identifier for a group of nodes. A node may belong to any number of multicast groups. Multicast addresses have the following format:

| 8 | 4 | 4 | 112 bits |

+-----+-----+-----+-----+

|11111111|flgs|scop| group ID |

+-----+-----+-----+-----+

11111111 at the start of the address identifies the address as being a multicast address.

+--+--+--+

flgs is a set of 4 flags: |0|0|0|T|

+--+--+--+

The high-order 3 flags are reserved, and must be initialized to 0.

T = 0 indicates a permanently-assigned ("well-known") multicast address, assigned by the global internet numbering authority.

T = 1 indicates a non-permanently-assigned ("transient") multicast address.

scop is a 4-bit multicast scope value used to limit the scope of the multicast group. The values are:

0 reserved

1 node-local scope

2 link-local scope

3 (unassigned)

4 (unassigned)

5 site-local scope

6 (unassigned)

7 (unassigned)

8 organization-local scope

9 (unassigned)

A (unassigned)

B (unassigned)

C (unassigned)

D (unassigned)

E global scope

F reserved

group ID identifies the multicast group, either permanent or transient, within the given scope.

Incorrect Answers:

A, C, D: These bit configurations do not fit the prefix of multicast address.

QUESTION 8:

Why was the IPv6 Time To Live (TTL) field changed to the Hop Limit field in IPv6?

A. TTL is measured in milliseconds, whereas most routers route packets in nanoseconds.

B. TTL is measured in milliseconds, whereas most routers route packets in seconds.

C. TTL is measured in milliseconds, whereas most routers route packets in hops.

D. TTL is measured in seconds, whereas most routers route packets in milliseconds.

Answer: D

Explanation:

The hop limit field now holds the number of hops, and no longer holds a time value. The problem is that the routers and the network have become too fast (yes, this is a good thing!). The router can route a packet through the network from end to end in less than a second. Having a TTL that can only be represented in seconds was no longer compatible with the capabilities of the network.

Incorrect Answers:

A, B, C: TTL was measured in seconds, so these options are incorrect.

QUESTION 9:

A SNMP Protocol Data Unit (PDU) type 3 is which type of command?

- A. GetResponse.
- B. GetRequest.
- C. GetNextRequest.
- D. SetRequest.

Answer: D

Explanation: Remember this table for Protocol Data Units (PDU) For SNMP:

Command	PDU Type
GetRequest	0
GetNextRequest	1
GetResponse	2
SetRequest	3
Trap	4

You will get questions on the exam that could ask you any of the 5 PDU types, you should remember them all. The exam will ask you for one PDU type, and usually list 4 of the 5 types from the table above.

Incorrect Answers:

A, B, C. See table.

QUESTION 10:

Within the Encrypted Security Payload (ESP) extension header, which of the following

ensures that messages end on a 64-bit boundary?

- A. Sequence Number.
- B. Payload Type.
- C. Padding.
- D. Security Parameters Index (SPI).

Answer: C

Explanation: Padding is used to control the size and alignment of the message. The Pad Length indicates the number of 8-bit padding bytes to be added after the data.

Incorrect Answers:

- A: The sequence number is a 32-bit unsigned number used to provide anti-replay abilities.
- B: The ESP header does not have a field called the payload type. There is payload data and payload length, for the length of the payload. The type of payload is actually stored in the next header field.
- D: By combining the SPI with the destination address and the Security Protocol (ESP) identifies the security association of the packet. The SPI is an unsigned 32-bit integer.

QUESTION 11:

Simple network management protocol (SNMP) uses which type of encryption when it sends a SetRequest command?

- A. 128-bit
- B. 32-bit
- C. Cleartext
- D. 64-bit

Answer: C

Explanation: SNMP is totally cleartext. There is no encryption or other protection provided on the payload.

Incorrect Answers:

- A, B, D: SNMP does not use or provide facilities for encryption.

QUESTION 12:

In IPv6, what is the new name for the point-to point address introduced in IPv4?

- A. Unicast
- B. Anycast
- C. Vericast
- D. Multicast

Answer: A

Explanation:

A: Unicast refers to a single point-to-point address.

Incorrect Answers:

B: Anycast is a group address, where one member of the group processes the message. It is still a point to many addressing scheme since the message is addressed to a group.

C: Vericast is not a term used in Ipv6, and is probably a detractor thrown in to confuse you.

D: Multicast is a group address, where everyone in the group processes the message. It is a point to many addressing scheme.

QUESTION 13:

In IPv6, which configuration scheme requires an address server to allocate an IP address to a client from a pool of addresses?

A. Stateless autoconfiguration.

B. Stateless configuration.

C. Stateful autoconfiguration.

D. Stateful configuration.

Answer: C

Explanation: Stateful autoconfiguration requires a server. If it is stateful, state is accomplished from the server, if it is stateless, then client generates its own IP address.

Incorrect Answers:

A: Stateless autoconfiguration does not require a server.

B, D: Stateless and Stateful refer to autoconfiguration, not configuration.

QUESTION 14:

Which Internet control message protocol (ICMPv6) message type would you receive if you do not have the permission to remotely access a remote computer?

A. Packet Too Big.

B. Time Exceeded.

C. Redirect.

D. Destination Unreachable.

Answer: D

Explanation: A Destination Unreachable message SHOULD be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion. (An ICMPv6 message MUST NOT be generated if a packet is dropped due to congestion.)

If the reason for the failure to deliver is lack of a matching entry in the forwarding node's routing table, the Code field is set to 0 (NOTE: this error can occur only in nodes that do not hold a

"default route" in their routing tables).

If the reason for the failure to deliver is administrative prohibition, e.g., a "firewall filter", the Code field is set to 1.

If there is any other reason for the failure to deliver, e.g., inability to resolve the IPv6 destination address into a corresponding link address, or a link-specific problem of some sort, then the Code field is set to 3.

A destination node **SHOULD** send a Destination Unreachable message with Code 4 in response to a packet for which the transport protocol (e.g., UDP) has no listener, if that transport protocol has no alternative means to inform the sender. (Reference: RFC 2463)

Incorrect Answers:

A: A Packet Too Big **MUST** be sent by a router in response to a packet that it cannot forward because the packet is larger than the MTU of the outgoing link. The information in this message is used as part of the Path MTU Discovery process [PMTU].

Sending a Packet Too Big Message makes an exception to one of the rules of when to send an ICMPv6 error message, in that unlike other messages, it is sent in response to a packet received with an IPv6 multicast destination address, or a link-layer multicast or link-layer broadcast address. (Reference: RFC 2463)

B: If a router receives a packet with a Hop Limit of zero, or a router decrements a packet's Hop Limit to zero, it **MUST** discard the packet and send an ICMPv6 Time Exceeded message with Code 0 to the source of the packet. This indicates either a routing loop or too small an initial Hop Limit value. (Reference: RFC 2463)

C: Neighbor Discovery defines five different ICMP packet types: A pair of Router Solicitation and Router Advertisement messages, a pair of Neighbor Solicitation and Neighbor Advertisements messages, and a Redirect Message. The Redirect is used by routers to inform hosts of a better first hop for a destination.)Reference: RFC 2461)

QUESTION 15:

Which IPv6 field was revised and renamed the Next header field in IPv6?

- A. The Option Field.
- B. The type of service field.
- C. The protocol field.
- D. The hop limit field.

Answer: C

Explanation: The protocol field was renamed to Next Header.

Incorrect Answers:

A: The option field was removed and not carried over to Ipv6.

B: The type of service field was removed and not carried over to Ipv6.

D: The TTL fields was renamed to Hop Limit, Hop Limit is an Ipv6 field.

QUESTION 16:

What is the difference between Anycast and multicast?

- A. Multicast is used to reference a group, whereas Anycast is not.
- B. Anycast communicates only with the closest member in a group, whereas multicast communicates to the entire group.
- C. Multicast delivers only to the first in the group, whereas Anycast delivers the group as a whole.
- D. Multicast is used to reference a group, whereas Anycast is used to reference a Single entity.

Answer: B

Explanation: Multicast identifies a group of hosts. All hosts will process the message. Anycast also identifies a group of hosts. Only one member will process the message. It is usually the closest member of the group.

Incorrect Answers:

- A: Both Anycast and Multicast reference a group.
- C: The message is delivered to the entire group in both cases. But in Anycast, only one member processes the message.
- D: Both Anycast and Multicast reference a group.

QUESTION 17:

Which feature of Internet Group Management Protocol (IGMP) in IPv6 was excluded from Internet control message protocol (ICMP) in IPv6?

- A. Group membership query.
- B. Information request/information reply.
- C. Router solicitation/router advertisement.
- D. Group membership report/reduction.

Answer: B

Explanation: Information Request and Information Reply was excluded and not made part of ICMPv6.

Incorrect Answers:

- A: Group Membership Query is now part of ICMPv6
- C: Router Solicitation and Router Advertisement are included in ICMPv6.
- D: Group Membership Report and Group Membership reduction are now part of ICMPv6.

QUESTION 18:

Which extension header is identified by value 0 in the next header field?

- A. Routing extension header.
- B. Destination options extension header.
- C. Hop-by-hop extension header.
- D. Fragment extension header.

Answer: C

Explanation: The following table should be memorized, these are the code mappings.

Next Header Field	Function
0	Hop by hop options header
43	Routing Header
44	Fragment Header
60	Destination Options Header
52	ESP Header
59	No Next Header

Incorrect Answers:

A, B, D: The proper codes for these headers can be searched in the given table above.

QUESTION 19:

Which part of an IPv6 packet is similar to IPv4 option field?

- A. The data header.
- B. The extension header.
- C. The next header.
- D. The transmission header.

Answer: B

Explanation: Ipv6 can specify options after the main header by using extension headers.

Incorrect Answers:

- A: There is a packet header, and headers for the extensions. There is no data header.
- C: The Next Header identifies the type of Header Extension that comes next, but it does not provide actual information on the options themselves.
- D: There is a packet header, and headers for the extensions. There is no transmission header.

QUESTION 20:

IPv6 implements security at the Internet layer with an encrypted security payload (ESP) extension header. What is this security concept called?

- A. Authentication.
- B. Initialization.
- C. Padding.
- D. Confidentiality.

Answer: D

Explanation: The ESP is used for encryption services. When the packet is encrypted, only those who have the correct keys can decrypt the data and read it. If you don't have the keys, you can't read the data. The data is protected from unauthorized entities from reading the data, so the data's confidentiality is maintained.

Incorrect Answers:

- A: Authentication of the packet is accomplished by the authentication extension header, which would be designated by the Next Header Field by a code 51.
- B: This is not termed initialization.
- C: This is not termed padding.

QUESTION 21:

What is the major difference between Simple network management protocol (SNMP) and remote network monitoring (RMON)?

- A. SNMP has stronger security than RMON.
- B. SNMP can slow down network traffic.
- C. SNMP is a set of MIB definitions whereas RMON is not.
- D. RMON can slow down network traffic.

Answer: B

Explanation: SNMP can be used to poll the management information base (MIBs) of various SNMP agents. Gathering of data can take a toll on the network depending on the number of agents polled and the polling interval. As either number increases, the network traffic also increases. For example, if there are 100 managed SNMP devices, and the information needs to be updated every second, there will be 100 devices polled each second. This is very granular (fine) but takes a toll on the network. As SNMP traffic increases on the network, other traffic slows down as bandwidth is degraded.

Now compared to the RMON, RMON is like a packet sniffer or protocol analyzer. RMON monitors the interface and collects information from the network data stream and stores it within the RMON MIB. RMON is not generating network traffic to collect its data. It is possible to add SNMP commands to RMON to collect certain information, but that would be a SNMP process, and not a RMON collection process.

Incorrect Answers:

- A: SNMP barely has any security, as long as the community name is kept a secret, and then the community name is passed in the clear so that anyone capturing packets can find out anyway.
- C: SNMP and RMON use the Management Information Base. RMON has a MIB specific to it,

and saves collected data in that MIB. SNMP can then be used to collect that information at a later time.

D: See the explanation above. Normally RMON does not generate network traffic, it just sits there and listens to the existing traffic as it passes by.

QUESTION 22:

Address 0.0.0.0.0.0.1 in IPv6 serves the same function at which address in IPv4 address scheme?

- A. 10.10.10.1
- B. 172.20.40.71
- C. 127.129.11.12
- D. 255.255.255.255

Answer: C

Explanation: The address is the loopback address, which should map to 127.0.0.1. The closest address in the list is 127.129.11.12, since this address is off the 127 network, which is reserved for loopback addresses.

Incorrect Answers:

A: This is a regular IP address, within the Private IP Address space. 10.0.0.0-10.255.25.255 is a reserved range as Private IP Addressing.

B: This is a regular class B address.

D: This is a broadcast address, and not a loopback address.

QUESTION 23:

Which IP address range is reserved by the ICANN for private networks?

- A. 0.0.0.0 and 255.255.255.255
- B. 127.0.0.0 through 127.31.255.255
- C. 172.16.0.0 through 172.31.255.255
- D. 196.0.0.0 through 196.255.255.255

Answer: C

Explanation: The address ranges that are reserved by ICANN for private networks are:

10.0.0.0-10.255.255.255

172.16.0.0-172.31.255.255

192.168.0.0-192.168.255.255

Notice that each range falls within a different class of IP addresses.

Incorrect Answers:

A: This is the entire IP address space, and not just for private networks.

B: IP Addresses beginning with 127 are loopback addresses, and reserved for loopback

functions.

D: This is not the private address for the Class C range.

QUESTION 24:

Which Internet control message protocol (ICMPv6) message type would you receive if your message exceeded the size limit on a network segment?

- A. Parameter problem.
- B. Destination unreachable.
- C. Redirect.
- D. Packet Too Big.

Answer: D

Explanation: A Packet Too Big MUST be sent by a router in response to a packet that it cannot forward because the packet is larger than the MTU of the outgoing link. The information in this message is used as part of the Path MTU Discovery process [PMTU]. Sending a Packet Too Big Message makes an exception to one of the rules of when to send an ICMPv6 error message, in that unlike other messages, it is sent in response to a packet received with an IPv6 multicast destination address, or a link-layer multicast or link-layer broadcast address. (Reference: RFC 2463)

Incorrect Answers:

A: If an IPv6 node processing a packet finds a problem with a field in the IPv6 header or extension headers such that it cannot complete processing the packet, it MUST discard the packet and SHOULD send an ICMPv6 Parameter Problem message to the packet's source, indicating the type and location of the problem. (Reference: RFC 2463)

B: A Destination Unreachable message SHOULD be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion. (An ICMPv6 message MUST NOT be generated if a packet is dropped due to congestion.)

If the reason for the failure to deliver is lack of a matching entry in the forwarding node's routing table, the Code field is set to 0 (NOTE: this error can occur only in nodes that do not hold a "default route" in their routing tables).

If the reason for the failure to deliver is administrative prohibition, e.g., a "firewall filter", the Code field is set to 1.

If there is any other reason for the failure to deliver, e.g., inability to resolve the IPv6 destination address into a corresponding link address, or a link-specific problem of some sort, then the Code field is set to 3.

A destination node SHOULD send a Destination Unreachable message with Code 4 in response to a packet for which the transport protocol (e.g., UDP) has no listener, if that transport protocol has no alternative means to inform the sender. (Reference: RFC 2463)

C: If an IPv6 node processing a packet finds a problem with a field in the IPv6 header or extension headers such that it cannot complete processing the packet, it MUST discard the packet and SHOULD send an ICMPv6 Parameter Problem message to the packet's source, indicating the type and location of the problem. (Reference: RFC 2463)

Neighbor Discovery defines five different ICMP packet types: A pair of Router Solicitation and Router Advertisement messages, a pair of Neighbor Solicitation and Neighbor Advertisements messages, and a Redirect Message. The Redirect is used by routers to inform hosts of a better first hop for a destination.)Reference: RFC 2461)

QUESTION 25:

Multicasting in IPv6 uses three management message that are similar to Ipv4 equivalents. What does the group membership query message in IPv6 do?

- A. It is sent to routers to terminate membership in a group.
- B. It is sent by stations to determine which local routers are members of a particular group.
- C. It is sent by stations by indicate membership in a particular group.
- D. It is sent by router to determine which local stations are members of a particular group.

Answer: D

Explanation: The routers send the query to determine which local stations are participating in the group.

Incorrect Answers:

- A: A group membership report can be used to TERMINATE membership in a group.
- B: Stations either indicate membership in a group or terminate membership. Stations do not query routers for membership.
- C: A group membership report is used to indicate that a member is still a member of the group, and is sent in response to the group membership query.

QUESTION 26:

Using the IEEE-EUI-64 conversion process, how do you convert the 48-bit host address (MAC address) to an IPv6 64-bit address?

- A. Add FF: EE between the third and fourth bytes.
- B. Add FE: EE between the third and fourth bytes.
- C. Add EF: FE between the third and fourth bytes.
- D. Add FF: FE between the third and fourth bytes.

Answer: D

Explanation: Example: A2-67-97-6B-FE-34 = A2-67-97-FF-FE-6B-FE-34

Incorrect Answers:

- A, B, C: You need to add the values FF:FE, and even though the position is correct, the code to be added is incorrect.

QUESTION 27:

Which Internet control message protocol (ICMPv6) message type would you receive if the

Hop limit field reached zero?

- A. Time exceeded.
- B. Destination unreachable.
- C. Parameter problem.
- D. Redirect.

Answer: B

Explanation: If a router receives a packet with a Hop Limit of zero, or a router decrements a packet's Hop Limit to zero, it MUST discard the packet and send an ICMPv6 Time Exceeded message with Code 0 to the source of the packet. This indicates either a routing loop or too small an initial Hop Limit value. (Reference: RFC 2463)

Incorrect Answers:

B: A Destination Unreachable message SHOULD be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion. (An ICMPv6 message MUST NOT be generated if a packet is dropped due to congestion.)

If the reason for the failure to deliver is lack of a matching entry in the forwarding node's routing table, the Code field is set to 0 (NOTE: this error can occur only in nodes that do not hold a "default route" in their routing tables).

If the reason for the failure to deliver is administrative prohibition, e.g., a "firewall filter", the Code field is set to 1.

If there is any other reason for the failure to deliver, e.g., inability to resolve the IPv6 destination address into a corresponding link address, or a link-specific problem of some sort, then the Code field is set to 3.

A destination node SHOULD send a Destination Unreachable message with Code 4 in response to a packet for which the transport protocol (e.g., UDP) has no listener, if that transport protocol has no alternative means to inform the sender. (Reference: RFC 2463)

C: If an IPv6 node processing a packet finds a problem with a field in the IPv6 header or extension headers such that it cannot complete processing the packet, it MUST discard the packet and SHOULD send an ICMPv6 Parameter Problem message to the packet's source, indicating the type and location of the problem. (Reference: RFC 2463)

D: Neighbor Discovery defines five different ICMP packet types: A pair of Router Solicitation and Router Advertisement messages, a pair of Neighbor Solicitation and Neighbor Advertisements messages, and a Redirect Message. The Redirect is used by routers to inform hosts of a better first hop for a destination.)Reference: RFC 2461)

QUESTION 28:

Which feature of Internet Group Management Protocol (IGMP) in IPv4 was excluded from Internet Control Message Protocol (ICMP) in IPv6?

- A. Subnet mask request/subnet mask reply.
- B. Group membership report/reduction.
- C. Router solicitation/router advertisement.

D. Neighbor solicitation/neighbor advertisement.

Answer: A

Explanation: Subnet Mask Request and Subnet Mask Reply were not carried over to Ipv6.

Incorrect Answers:

B, C, D: These functions are currently part of ICMPv6.

QUESTION 29:

An SNMP protocol Data unit (PDU) type 2 is which type of command?

- A. GetResponse.
- B. GetRequest.
- C. GetNextRequest.
- D. SetRequest.

Answer: A

Explanation: Remember this table for Protocol Data Units (PDU) For SNMP:

Command	PDU Type
GetRequest	0
GetNextRequest	1
GetResponse	2
SetRequest	3
Trap	4

You will get questions on the exam that could ask you any of the 5 PDU types, you should remember them all. The exam will ask you for one PDU type, and usually list 4 of the 5 types from the table above.

Incorrect Answers:

B, C, D: See table.

QUESTION 30:

How do flags and scopes fields work with multicasting?

- A. A scope is used for transient addresses, and flags are used to distinguish between local and

global groups.

B. Flags are used with the prefix, and a scope is added to the group identifier.

C. Flags are used for transient addressed, and a scope is used to distinguish between local and global groups.

D. Flags and scope fields work only with anycasting.

Answer: C

Explanation: The flags field is 4 bits in length, and the first three bits are reserved and not yet assigned. The fourth bit is the T bit, (RFC 2460) and used to determine if whether the multicast address is permanent (well-known) or temporary (transient). Scoping is used to control the destination groups to receive the message.

The following is the coding of the scope field in the multicast header, as per RFC 2373, the scope is a 4-bit value, and the values are (in Hex):

0 reserved

1 node-local scope

2 link-local scope

3 (unassigned)

4 (unassigned)

5 site-local scope

6 (unassigned)

7 (unassigned)

8 organization-local scope

9 (unassigned)

A (unassigned)

B (unassigned)

C (unassigned)

D (unassigned)

E global scope

F reserved

Incorrect Answers:

A, B, C: These statements are incorrect.

QUESTION 31:

Which type of DNS server has no authority of its own, but processes queries by asking other services for information?

A. Root

B. Primary

C. Caching

D. Forwarding

Answer: C

Explanation: A caching server has no static database. When a request is received, the

caching DNS server queries other DNS servers to resolve any request that can't be resolved in its own cache. When a caching DNS server is started, its cache is empty.

Incorrect Answers:

A, B, D: These types of servers have their own authority (designated by SOA records) and zones. The zones are static databases which those servers startup with.

QUESTION 32:

Which protocol was created as an alternative to RARP?

- A. Address resolution protocol (ARP).
- B. Interior gateway routing protocol (IGRP).
- C. Classless interdomain routing (CIDR).
- D. BOOTstrap protocol (BOOTP).

Answer: D

Explanation: BOOTP is used by diskless workstations to obtain an IP address. The BOOTP enabled workstation broadcasts a packet with its MAC address in it, requesting an IP address. Essentially, RARP also does this, RARP requests an IP address based on a given MAC address.

The question is oddly worded. Since ARP and RARP were based on the BOOTP protocol. This implies that BOOTP was here first, and RARP was the alternative.

Incorrect Answers:

- A: ARP is the complement of RARP, where an IP address is given and we are looking for a hardware address.
- B: IGRP is a routing protocol, and is only used by routers to update their routing tables.
- C: CIDR is a method of combining adjacent networks into one larger network. It is not involved in MAC to IP address resolution.

QUESTION 33:

The Internet was created in 1968. What was its original name?

- A. ARPANET
- B. CompuServe
- C. WorldNet
- D. Defense Net

Answer: A

Explanation: The name of the original network that is called the Internet today was Arpanet. It is an acronym for Advanced Research Project Agency Network, created in 1968 by the Department Of Defense (DOD).

Incorrect Answers:

- B: CompuServe was a private network and BBS system, provided by a private vendor, and

serving only the users who signed up and paid monthly fees.

C: Worldnet was a private network and BBS system, provided by a private vendor, and serving only the users who signed up and paid monthly fees.

D: Even though the Internet, and its predecessor originated from the Department Of Defense (DOD), defense net was not the name of the network.

Note: Companies like CompuServe, WorldNet, and Prodigy are older private networks that now provide ISP services for their users. This allows an entry point into the Internet from those private networks. However, for the original Internet, which was only used by the Military, Education Institutions, and Contractors, was the former Arpanet network.

QUESTION 34:

Which of the following IP addresses is reserved as the Loopback address?

- A. 127.0.0.0
- B. 127.0.0.1
- C. 255.255.255.0
- D. 255.255.255.255

Answer: B

Explanation: The 127 range is reserved for loopback addresses. The common loopback address for the TCP/IP stack is: 127.0.0.1

Incorrect Answers:

A, C, D: These are essential different forms of all ones or all zeros broadcast addresses. These are not loopback addresses.

QUESTION 35:

Which of the following choices correctly names the four layers of Internet architecture model?

- A. Transport, network, data link, and Internet.
- B. Transport, data link, physical, and network access.
- C. Application, presentation, presentation, data link, and physical.
- D. Application, transport, Internet, and network access.

Answer: D

Explanation: These are the four layers. The OSI Session, Application, and Presentation layers map to the Application Layer, the OSI Transport Layer to the Transport Layer, Network Layer to the Internet Layer, and the Physical and Data Link Layers to the Network Access Layer.

Incorrect Answers:

A: There are no network or data link layers. The network layer is called Internet Layer.

B: There is no data link or physical layers, they are combined into network access.

C: There are no presentation (combined into the application layer) or data link and physical (combined into the network access layer).

QUESTION 36:

Which of the following is a nearly universal method of name resolution on the Internet?

- A. ARP
- B. UDP
- C. POP
- D. DNS

Answer: D

Explanation: DNS (Domain Name Server) is a server implementation of the static HOSTS file implementation. Originally, to set a IP address to Host Name mapping, the HOSTS file was used, which was a flat text file. Implementation of DNS provided a central server method of performing the functions of the HOSTS file with minimal maintenance and high performance.

Incorrect Answers:

A: ARP (Address Resolution Protocol) is used to determine the hardware address of a node for specific IP address. A packet with the IP address is sent and the appropriate client should return an ARP Reply with the MAC address that goes with the requested IP address. This is MAC address resolution, not name resolution.

B: UDP (User Datagram Protocol) is a transport layer protocol, which is used for connectionless data transfer.

C: POP (Post Office Protocol) is a Application Level protocol used by client to retrieve e-mail off e-mail server.

QUESTION 37:

Routing occur in which layer of Internet architecture model?

- A. Transport
- B. Internet
- C. Network access
- D. Physical

Answer: B

Explanation: The Internet Layer in the Internet Model maps to the Network Layer in the OSI model. Functionality remains the same, so routing is done at this level.

Incorrect Answers:

A: The transport layer works with host-to-host issues, and routing functions do not occur at this level.

C: The Network Access layer maps to the Physical and Data Link layers of the OSI model.

Routing is not performed here.

D: There is no physical layer in the Internet Architecture model. The physical and data link layers of the OSI model map to the network access layer. Routing does not occur here.

QUESTION 38:

Ivan is planning his company network. He is going to use at least 400 subnets, with up to 1000 hosts on each subnet. Which class of addresses should he use?

- A. Class A.
- B. Class B.
- C. Class C.
- D. Class D.

Answer: A

Explanation: One must be careful, the wrong way to do this is to take 400 times 1000 (which gives 400,000) and see how many bits 400,000 can fit in - even if it leads to the correct answer, it won't always.

The first step is to add 2 to each number, because there are two reserved host and network addresses. Remember, the formula is: $2^n - 2$.

The next step is to round each number up to the next straight power of 2. For the networks we get 512 ($400 + 2$ raised up) and 1024 ($1000 + 2$ raised up).

Next, find the number of subnet mask bits required to represent each: 512 will require 9 network bits, and 1024 will require 10 bits, for a total of 19 bits ($9 + 10$).

A Class A address gives us 8 bits of Networking, and 24 bits in Host addressing. We can carve out our new network by using 19 of the 24 bits for the host.

Incorrect Answers:

B: A Class B address gives 16 bits of networking and 16 bits of host. We can't fit 19 bits into a 16 bit number, and we can't touch any of the first 16 bits, which is the assigned network address.

C: A Class C address gives 24-bits of networking and 8-bits of host. We can't fit 19 bits into a 8-bit number, and we can't touch any of the first 24-bits, which is the assigned network address.

D: A Class D address is a Multicast address range, and can't be used for network/host addressing.

QUESTION 39:

Rachel is managing a network that has two groups of client machines separated by a router. The machines on the same segment as the DHCP server are correctly configured, whereas the machines on the other sides of the router are not. Rachel also has a domain name server on the network. What should Rachel do to her network to ensure that all client machines are correctly configured?

- A. Add a DNS server to the same segment that has the DHCP server.
- B. Add a DNS server to the segment that does not have the DHCP server.
- C. Add a DHCP relay agent to the same segment that has the DHCP server.

D. Add a DHCP relay agent to the segment that does not have the DHCP server.

Answer: D

Explanation:

DHCP uses broadcasts for all four phases (DORA) of its process. This requires broadcasts to get from the client to the DHCP server, and from the DHCP server to the client. The problem is that between these two subnets is a router that does not pass broadcasts. Now there is an exception, and that is when the router is equipped with the BOOTP RFC, which allows the packets to pass. (DHCP is based on BOOTP). However, not all routers have this modification, or have this modification turned on. Unless specified in the question, the RFC is assumed not present or enabled. That leaves the use of a relay agent. The DHCP relay agent intercepts the broadcasts, and then communicates directly with the DHCP server to pass the requests back and forth. In order for the relay agent to hear the broadcasts, it must be on the orphaned segment, the segment that does not have a DHCP server. If the relay agent is placed on the segment with the DHCP relay server, then it will not hear the broadcasts from the other segment, because if it did, then we never needed the relay agent in the first place.

Incorrect Answers:

A, B: DNS services are not used by DHCP. DHCP does all its work via broadcasts, and does not use or refer to DNS or WINS.

C: The problem is that the machines that are separated by the router are not receiving a configuration. Since the client is broadcasting the discovery packet, and the router is not passing broadcasts, the relay agent on the other side of the router will not get the discovery packet. The agent is in fact on the wrong side of the router.

QUESTION 40:

Which choice shows the correct sequence of maturity-level states for a protocol?

- A. Proposed, draft, experimental, standard.
- B. Standard, experimental, proposed, draft.
- C. Experimental, proposed, draft, standard.
- D. Draft, experimental, proposed, standard.

Answer: D

Explanation: The protocol is first drafted, which is a document laying out the framework of the protocol. It then goes through an experimental stage where it is tried out and implemented in a test or limited environment. If the results are promising, the protocol can go through a proposed stage where it is being proposed as a standard. The standard is the final stage where the protocol is officially accepted. Remember that we start with Draft, and end with Standard.

Incorrect Answers:

A, B, C: These are not in the correct order.

QUESTION 41:

What is a typical length of IPv6 header?

- A. 48bits.
- B. 320 bits.
- C. 160 bits.
- D. 1024 bits.

Answer: B

Explanation: The header of an Ipv6 header is fixed at 40 octets, which is $8 \times 40 = 320$ bits in size.

Incorrect Answers:

A: 48 Bits is too small for an Ipv6 header, especially when you consider that the header has to hold a source and destination address of 128 bits each.

C: 160 Bits is the size of an Ipv4 header, which is 20 octets ($20 \times 8 = 160$). Also, the Ipv6 header has to hold both a source and destination address for the packet, at 128 bits each, which is 256 bits just in addressing alone.

D: The header is not 1024 bits.

QUESTION 42:

Which range of port numbers is called the 'well-known' port numbers?

- A. 1 to 1023
- B. 1024 to 16385
- C. 1024 to 2048
- D. 1024 to 65535

Answer: A

Explanation: The ports in the range 1-1023 are known as the well-known port numbers. These ports are used by the server part of a connection.

Incorrect Answers:

B, C, D:

The ports above 1023 are not called well known ports. These ports are used for client ports or for alternate server ports when the defaults are not used. The ports in the range of 1024-65535 (all the ports above 1023) are known as Ephemeral ports. Ports in the range of 1024-49151 are called registered ports, and ports 49152-65535 are dynamic or private ports.

QUESTION 43:

Assuming the n = number of host bits, which of the following choices shows the correct formula for finding maximum number of hosts per subnet?

- A. $2n+2$
- B. $2n$
- C. $2n-2$
- D. $n+2$

Answer: C

Explanation: What the question is asking refers to the subnet mask. When it says number of host bits, it refers to the number of bits in the subnet mask that represents the host. So, if I have a Class C address, which gives me 24 bits for the network and 8 bits for the host, the question asks how many hosts does the 8 bits give me. Well, two to the eighth power is 256. However, there are two special situations where I can't use addresses in the range. There are two special bit configurations for broadcasts, the all zeros and the all ones broadcasts. This means that in the range of possible 256 addresses. I can't use Zero or 255. So, I have to subtract 2, and that leaves me with 254 possible host addresses.

Incorrect Answers:

- A: This would be two many addresses, since I can never go over $2n$, and even that is too many.
- B: This is not enough, because there are two reserved addresses that cannot be used.
- D: This is not correct, and actually doesn't even come close.

QUESTION 44:

Which TCP/IP suite protocol is used to troubleshoot and manage networks?

- A. DHCP
- B. SNMP
- C. IGMP
- D. RIP

Answer: B

Explanation: System Network Management Protocol is a management protocol, used to manage, control, monitor, and troubleshoot networks.

Incorrect Answers:

- A: DHCP is used to assign IP addresses to hosts, and can also assign TCP/IP parameters for various TCP/IP entries.
- C: IGMP is Internet Group Message Protocol.
- D: RIP is a routing protocol used by routers to update their routing tables,

QUESTION 45:

Which of the following choices lists the events that establish a TCP connection in the correct sequence?

- A. Passive open, SYN, ACK
- B. Active open, active close, passive open

- C. Passive open, active open, ACK
- D. Active open, passive open, ACK

Answer: D.

Explanation: Actually the sequence is Active Open, Passive Open, Ack, Ack.

Incorrect Answers:

A, B, C: These are either the wrong order or wrong options, and do not represent any valid TCP sequence.

QUESTION 46:

Which protocol is used to determine a hardware address from a given IP address?

- A. Address resolution protocol (ARP).
- B. Reverse address resolution protocol (RARP).
- C. Carrier sense multiple access with collision detection (CSMA/CD).
- D. Domain name system (DNS).

Answer: A

Explanation:

ARP is used to determine the MAC address of the destination node of an IP packet. The ARP message is sent bearing the IP address. The node with that IP address adds its MAC address to the message and returns an ARP response.

Incorrect Answers:

B: RARP is the opposite. You give it the hardware address (MAC address) and it returns the IP address.

C: CSMA/CD is the physical medium access method used by hardware protocols such as Ethernet. It is not directly involved with addressing.

D: A DNS server performs IP to NAME mappings. Neither is a hardware address.

QUESTION 47:

Which layer of the OSI model provides flow control?

- A. Presentation.
- B. Transport.
- C. Network.
- D. Data link.

Answer: B

Explanation: The transport layer, layer 4, provides end-to-end flow control.

Incorrect Answers:

A: The Presentation layer (layer 6) deals with data preparation, which includes code conversion

and encryption. Flow control is handled by the lower layers.

C: The network layer (Layer 3) is responsible for IP Addressing of the host and routing decisions. It is not concerned with flow control.

D: The data link layer also does some flow control, as it manages node-to-node frame transfer. However, having to pick between the two, I have selected Transport.

QUESTION 48:

Which of the following provides a means for diskless workstations to determine IP addresses and other network parameters?

- A. Address resolution protocol (ARP).
- B. BOOTstrap protocol (BOOTP).
- C. Domain name system (DNS).
- D. Machine access control (MAC).

Answer: B

Explanation: BOOTP is the protocol used here. DHCP, which also does the same function is an enhancement that is based on the BOOTP protocol.

Incorrect Answers:

A: ARP is used to find a MAC (Hardware) address for a given IP address. The IP addresses are already assigned. Here, for a diskless workstation, we are asking for a NEW IP address to be given to the workstation.

C: DNS provides IP Address to Name mappings. It does not assign an IP address to a node.

D: MAC is the hardware address of the network interface card (NIC). This is burnt into the NIC, although it can be overridden. MAC runs at Layer 2, and when we discuss IP addresses, we are talking a Layer 3 address. MAC does not assign an IP address.

QUESTION 49:

Edwin works for an ISP where he must implement a DNS server. Which type of DNS server must be installed?

- A. Root.
- B. Master.
- C. Primary.
- D. Forwarding.

Answer: B

Explanation: An ISP will usually provide services for its customers that include email accounts, as well as running a website for the ISP itself. This needs to be a Primary or Master server, as both operate the same way.

Incorrect Answers:

A: An ISP would not install a root server, A root server is a special DNS server which is

maintained by special Internet registry agencies.

C: A primary server is usually implemented at a company or organization.

D: The ISP will need to maintain its own zone, so either a Primary or Master server function is required.

QUESTION 50:

Which series of standards specifies local area network (LAN) and metropolitan area network (MAN) technologies?

- A. IEEE 802
- B. IEEE 208
- C. RFC 1661
- D. MTU 1004

Answer: A

Explanation: The IEEE 802 standards are used for LAN technology. For example, 802.1 is used in bridging, 802.2 is used as a data link protocol, 802.3 is Ethernet, 802.5 is Token Ring and FDDI, 802.11 is wireless.

Incorrect Answers:

B: IEEE 208 is not the standards. In the IEEE the standards are not sequentially numbered, the 802 and 208 would be dates that the standards committee was either created or first met.

C: RFC (Request for Comments) are involved with standards for TCP/IP protocols and applications.

D: There is formal standards body called MTU.

QUESTION 51:

Which technique is used by Ethernet to prevent collisions?

- A. Packet switching.
- B. CSMA/CD
- C. UDP
- D. NetBEUI

Answer: B

Explanation: Carrier Sense Multiple Access / Collision Detection (CSMA/CD) is the physical medium signaling protocol used by Ethernet. It helps prevent collisions by detecting traffic on the medium BEFORE attempting to transmit.

Incorrect Answers:

A: Packet switching occurs at a higher layer/level. It is not involved with the physical layer, so it is not involved with working with the medium. A sample of Packet Switching is frame relay which runs at layer 2.

C: UDP is a transport layer (Layer 4) protocol, and many layers above the physical layer where

medium sensing occurs.

D: NetBEUI is a data link (Layer 2) protocol which uses 802.2, and is above the workings of physical medium sensing, where collisions would occur.

QUESTION 52:

Sahan wants to clear TCP/IP network information from her Windows NT workstation. Which command should she use?

- A. Ipconfig /release
- B. Ipconfig /renew
- C. Ipconfig /clear
- D. Ipconfig /reset

Answer: A

Explanation: The /release parameter will release the current IP address and cancel the lease. This command can only be issued if the IP address and configuration was initially provided via a DHCP server.

Incorrect Answers:

B: The /renew is used to renew the current lease of the IP address. The /renew causes interaction with the DHCP server to extend the current lease. It does not clear the information, the information will remain.

C, D: /clear and /reset are not valid parameters of the ipconfig command. If they are used, they will cause an error. Actually, since they are invalid, the ipconfig command will display the help screen to show you what is valid, as well as the correct usage.

QUESTION 53:

In Windows NT, which command displays the IP network adapter information?

- A. Ping /r
- B. Ipconfig /all
- C. tracert
- D. ifconfig

Answer: B

Explanation: The ipconfig command will provide IP information for a machine. It will list all adapters, with the domain name, IP address, subnet mask, and default gateway. By adding the /all parameter, for each interface we will get the NIC type/brand, the physical address (The MA address), and the remainder of the IP stack data, including the primary and secondary DNS servers, WINS Servers, and DHCP client information.

Incorrect Answers:

A: A ping /r command is used by the ping command to record the route for count hops. It does not provide adapter information for any machine, including the source and target nodes.

C: Tracert is the traceroute command, and is used to record the hops along the path between the source machine and the target machine. Like ping, the tracert command uses ICMP echo/reply commands, and does not collect or obtain adapter information for any machine or device, including the source and target machines.

D: Ifconfig is not supported on the Windows NT Platform.

QUESTION 54:

How is a request for comments (RFC) indexed after it has been standardized?

- A. X.500
- B. Frequently Asked Questions (FAQ).
- C. Standard (STD).
- D. IEEE 802

Answer: C

Explanation: After a RFC has been accepted as a standard, it is indexed as a Standard (STD).

Incorrect Answers:

A: X.500 is a protocol, and not a method of organizing documents.

B: FAQ is not the proper term for this definition.

D: IEEE 802 is a set of standards for LAN and MANs. It is at a lower level (Physical & Datalink) in the OSI stack. RFC's refer to the Internet, which is defined at layers 3 and above.

QUESTION 55:

Which network-layer protocol is responsible for addressing hosts?

- A. SPX
- B. TCP
- C. IP
- D. HTTP

Answer: C

Explanation: IP is a network layer protocol (Layer 3). It is responsible for addressing hosts and routing.

Incorrect Answers:

A: SPX (Sequenced Packet exchange Protocol) is a transport layer protocol (Layer 4).

B: TCP is a transport layer protocol (Layer 4).

D: HTTP is an application, and runs at the application layer (layer 7) level.

QUESTION 56:

Which of the following is the mathematical calculation that is used to verify the validity of

a packet?

- A. Cyclical redundancy check (CRC).
- B. Open system interconnection (OSI).
- C. Data link control. (DLC).
- D. Transmission Control Protocol (TCP).

Answer: A

Explanation: The CRC is an algorithm used to calculate the validity of a packet. It is a checksum used to determine if there are bit errors on the packet or frame.

Incorrect Answers:

B: OSI is not a mathematical calculation.

C: DLC is a Data Link protocol, it is not a mathematical calculation.

D: TCP is a transport protocol, it is not a mathematical calculation.

QUESTION 57:

How many bits are used to form an IPv6 address?

- A. 16bits
- B. 32bits
- C. 256bits
- D. 128bits

Answer: D

Explanation: Ipv6 uses a 128 bit address.

Incorrect Answers:

A, C: Ipv6 uses a 128 bit address.

B: Ipv6 uses a 128 bit address. Ipv4 uses the 32 bit address, and there are mapping techniques to map the 32 bit IPv4 address onto a 128 bit Ipv6 address.

QUESTION 58:

Which of the following choices lists the correct sequence for the events of the DHCP initialization process?

- A. Discover, offer, request, acknowledge.
- B. Request, discover, offer, acknowledge.
- C. Offer, acknowledge, request, discover.
- D. Discover, request, offer, acknowledge.

Answer: A

Explanation: Think DOR

A. The first packet that goes out is a discovery packet which has the responsibility to seeking out and discovering a DHCP server. It is the request saying that: "hey - I need an IP address". The DHCP server, or servers if there are more than one, may offer an IP address to the client. The client, will receive the offer, and if there are more than one DHCP server, the client will receive multiple offers. The client must now choose from the available offers (usually takes the first offer to make it simple) and now makes the formal request, saying: "May I have this IP address". Finally, the DHCP server should acknowledge and say: 'Yes'. Note that it is possible that the DHCP server timed out and gave the address away to someone else, so the acknowledgement is important.

Incorrect Answers:

B, C, D: These sequences are not the correct order.

QUESTION 59:

Lars just cleared the TCP/IP network information from his Windows NT 4.0 workstation. Which command should he use to receive new configuration?

- A. Ipconfig /release
- B. Ipconfig /renew
- C. Ipconfig /clear
- D. Ipconfig /reset

Answer: B

Explanation: To have a new configuration assigned immediately, a renew is issued.

Incorrect Answers:

A: This is the actual command that was used to do the clear of the information. Now, after releasing the current configuration, the adapter will eventually go out and get a new configuration. There are some differences between Windows NT and Windows 2000, for example Windows 2000 - if it doesn't get a DHCP response, will generate an APIPA, which is a special private IP address. However, the thing to note here is that after a release the system MAY eventually receive a new configuration, where using the renew parameter will request the information be assigned immediately.

C, D: There are no such parameters for the ipconfig command.

QUESTION 60:

What is the default class A subnet mask?

- A. 255.0.0.0
- B. 255.255.0.0
- C. 255.255.255.0
- D. 255.255.255.255

Answer: A

Explanation:

A. 255.0.0.0 is a Class A default subnet mask.

Incorrect Answers:

B: 255.255.0.0 is a Class B default subnet mask.

C: 25.255.255.0 is a Class C default subnet mask.

D: 255.255.255.255 is not really a subnet mask, a subnet mask separates a network from a host.

In this case just the full address is used.

QUESTION 61:

Which extension header is identified by value 44 in the Next Header field?

A. Fragment extension header

B. Routing extension header

C. Hop-by-bop extension header

D. Destination options extensions header

Answer: A

Explanation: The following table should be memorized, these are the code mappings.

Next Header Field	Function
0	Hop by hop options header
43	Routing Header
44	Fragment Header
60	Destination Options Header
52	ESP Header
59	No Next Header

Incorrect Answers:

B, C, D: The proper codes for these headers can be searched in the given table above.

QUESTION 62:

Which IPv6 header field was created to identify and distinguish between packets of

different priorities?

- A. The flow label field
- B. The class field
- C. The payload length field
- D. The protocol field

Answer: B

Explanation: Traffic class replaced the TOS (Type of Service) field, and was implemented to handle different data packet priorities, such as real time data.

Incorrect Answers:

- A: Used by the sender to label packets that require special handling by IPv6 routers
- C: The payload length field is used to hold the length of the packet, which does not include the size of the header.
- D: The protocol field was renamed to Next Header. The protocol field does not exist in IPv6.

QUESTION 63:

To send SNMP traps after the service is started, what must you add for them to work?

- A. A management information base
- B. A password
- C. A new user
- D. An IP address

Answer: D

Explanation: A trap requires an IP address. This IP address is the destination IP address of the management station which is monitoring that device or system. The SNMP agent isn't just going to broadcast the trap, it needs a explicit destination to send it.

Incorrect Answers:

- A: SNMP uses a management information base (MIB), but the trap does have to rely on that database being present.
- B, C: SNMP works on community names. A community name is the 2nd piece of information required to set up a trap. (The first being the IP address). SNMP does not use userids or passwords, so these items have no meaning.

QUESTION 64:

In IPv6, which configuration scheme allows a client to automatically configure its own IP address with or without IPv6 routers?

- A. Stateful autoconfiguration
- B. Stateless autoconfiguration
- C. Stateful configuration

D. Stateless configuration

Answer: B

Explanation: Stateless autoconfiguration allow the client to autoconfigure and generate its own IP address. A server for providing this address is not required.

Incorrect Answers:

A: Statful autoconfiguration requires a server to provide the IP address, similar to DHCP in Ipv4.

C, D: Stateful and Stateless refer to the autoconfiguration process.

QUESTION 65:

Which type of Protocol Data Unit does SNMP send when an event occurs?

- A. SetRequest
- B. GetNextRequest
- C. GetRequest
- D. Trap

Answer: A

Explanation: Remember this table for Protocol Data Units (PDU) For SNMP:

Command	PDU Type
GetRequest	0
GetNextRequest	1
GetResponse	2
SetRequest	3
Trap	4

You will get questions on the exam that could ask you any of the 5 PDU types, you should remember them all. The exam will ask you for one PDU type, and usually list 4 of the 5 types from the table above.

The trap command is issued by an agent running on a monitored device, and is returned to the management station(s).

Incorrect Answers:

A: SetRequest is sent from the management station to the monitored device, and is used to change MIB parameters on the monitored device.

B: GetNextRequest is sent from the management station to the monitored device, and is used after either a GetRequest or another GetNextRequest to get the next MIB block. This command is used for sequential stepping through the MIB database.

C: GetRequest is sent from the management station to the monitored device, and is used to read values from the MIB database on the monitored device.

QUESTION 66:

An SNMP protocol data unit type 0 is which type of command?

- A. GetRequest
- B. GetResponse
- C. SetRequest
- D. GetNextRequest

Answer: A

Explanation: Remember this table for Protocol Data Units (PDU) For SNMP:

Command	PDU Type
GetRequest	0
GetNextRequest	1
GetResponse	2
SetRequest	3
Trap	4

You will get questions on the exam that could ask you any of the 5 PDU types, you should remember them all. The exam will ask you for one PDU type, and usually list 4 of the 5 types from the table above.

Incorrect Answers:

B, C, D: See table.

QUESTION 67:

Within the Encrypted Security Payload extension header, which of the following uniquely identifies each packet?

- A. Padding

- B. Sequence number
- C. Security parameters index
- D. Payload type

Answer: B

Explanation: The sequence number is a 32-bit unsigned number used to provide anti-replay abilities. It uniquely identifies the message within the data stream.

Incorrect Answers:

A: Padding is used to control the size and alignment of the message. The Pad Length indicates the number of 8-bit padding bytes to be added after the data.

B: By combining the SPI with the destination address and the Security Protocol (ESP) identifies the security association of the packet. The SPI is an unsigned 32-bit integer.

D: The ESP header does not have a field called the payload type. There is payload data and payload length, for the length of the payload. The type of payload is actually stored in the next header field.

QUESTION 68:

Which feature of Internet Group Management Protocol in IPv4 was excluded from Internet control message protocol in IPv6?

- A. Source Quench
- B. Router Advertisement
- C. Group Membership Report
- D. Neighbor Solicitation

Answer: A

Explanation: Source Quench was omitted.

Incorrect Answers:

B, C, D: These features are currently part of ICMPv6.

QUESTION 69:

Which extension header is identified by value 60 in the Next Header field?

- A. Fragment extension header
- B. Hop-by-hop extension header
- C. Routing extension header
- D. Destination options extension header

Answer: D

Explanation:

The following table should be memorized, these are the code mappings.

Next Header Field	Function
0	Hop by hop options header
43	Routing Header
44	Fragment Header
60	Destination Options Header
52	ESP Header
59	No Next Header

Incorrect Answers:

A, B, C: The proper codes for these headers can be searched in the given table above.

QUESTION 70:

Simple Network Management Protocol uses which protocol to make requests and responses?

- A. TCP
- B. IPX
- C. UDP
- D. SPX

Answer: C

Explanation: SNMP uses UDP port 161 for requests and responses, and UDP port 162 for Traps.

Incorrect Answers:

A: TCP is not used with SNMP. SNMP is connection-less.

B, D: IPX and SPX are non-IP protocols. SNMP is based on IP and only communicates with IP devices.

QUESTION 71:

Within the Encrypted Security Payload extension header, which of the following uses 32-bit word variables from a random number generator to ensure that hackers cannot predict the first message words?

- A. Security parameters index

- B. Payload type
- C. Sequence number
- D. Initialization vector

Answer: D

Explanation: First, information about the IV:

Payload Data is a variable-length field containing data described by the Next Header field. The Payload Data field is mandatory and is an integral number of bytes in length. If the algorithm used to encrypt the payload requires cryptographic synchronization data, e.g., an Initialization Vector (IV), then this data MAY be carried explicitly in the Payload field. Any encryption algorithm that requires such explicit, per-packet synchronization data MUST indicate the length, any structure for such data, and the location of this data as part of an RFC specifying how the algorithm is used with ESP. If such synchronization data is implicit, the algorithm for deriving the data MUST be part of the RFC. (Reference RFC 2406)

The random number generator is used in the IV to provide the cryptographic synchronization data.

Incorrect Answers:

A: The SPI is an arbitrary 32-bit value that, in combination with the destination IP address and security protocol (ESP), uniquely identifies the Security Association for this datagram. The set of SPI values in the range 1 through 255 are reserved by the Internet Assigned Numbers Authority (IANA) for future use; a reserved SPI value will not normally be assigned by IANA unless the use of the assigned SPI value is specified in an RFC. It is ordinarily selected by the destination system upon establishment of an SA (see the Security Architecture document for more details). The SPI field is mandatory.

The SPI value of zero (0) is reserved for local, implementation-specific use and MUST NOT be sent on the wire. For example, a key management implementation MAY use the zero SPI value to mean "No Security Association Exists" during the period when the Ipsec implementation has requested that its key management entity establish a new SA, but the SA has not yet been established.

B: The payload type is specified in the Next Header Field. The Next Header is an 8-bit field that identifies the type of data contained in the Payload Data field, e.g., an extension header in IPv6 or an upper layer protocol identifier. The value of this field is chosen from the set of IP Protocol Numbers defined in the most recent "Assigned Numbers" [STD-2] RFC from the Internet Assigned Numbers Authority (IANA). The Next Header field is mandatory. (Reference RFC 2406)

C: The sender's counter is initialized to 0 when an SA is established. The sender increments the Sequence Number for this SA and inserts the new value into the Sequence Number field. Thus the first packet sent using a given SA will have a Sequence Number of 1.

If anti-replay is enabled (the default), the sender checks to ensure that the counter has not cycled before inserting the new value in the Sequence Number field. In other words, the sender MUST NOT send a packet on an SA if doing so would cause the Sequence Number to cycle. An attempt to transmit a packet that would result in Sequence Number overflow is an auditable event. (Note that this approach to Sequence Number management does not require use of modular arithmetic.) (Reference RFC 2406)

QUESTION 72:

How many bits are used to form an IPv4 address?

- A. 16 bits
- B. 32 bits
- C. 48 bits
- D. 64 bits

Answer: B

Explanation: A IPv4 address is 32 bits, an IPv6 address is 128 bits.

Incorrect Answers:

A, D: These addresses sizes are not used in any IP version.

C: This address size is not used in any IP version. However, note that the hardware address, the MAC address, is 48 bits long, it is 6 octets.

QUESTION 73:

Which Boolean operator is used with the subnet mask to determine the network portion of an Internet address?

- A. AND
- B. OR
- C. NOT
- D. NOR

Answer: A

Explanation: A Boolean AND operation generates a truth table such that if both bits are a one, then result is one, otherwise the result is zero. When applying the subnet mask, the network portion is represented by 1 bits and the host is represented by 0 bits. After ANDing the subnet mask with the IP address, all that will be left is the network portion.

Incorrect Answers:

B: A Boolean OR option generates a truth table such that if both bits are zero, the result is zero, otherwise the result will be one. Merging the subnet mask with the IP address will not yield the network ID, the IP address will almost look more like the subnet mask itself.

C: A Boolean NOT operation flips the bit, if it is a zero, it becomes a one, and if a one it becomes a zero. This will yield a totally corrupted IP address, and will not yield the network ID, nor anything of use.

D: A Boolean NOR operation is a NOT OR operation that does the OR and the NOT, and will also produce garbage for an IP address.

QUESTION 74:

Birgitta is the system administrator for a network with 100 client machines. She wants to

avoid manually maintaining all of the TCP/IP configurations. Which type of server could she add to her network to automatically manage the IP addresses?

- A. DNS server
- B. SNMP server
- C. DHCP server
- D. SGMP server

Answer: C

Explanation: The DHCP server will assign IP addresses, and will do so with a leasing facility. With leasing, IP addresses can be returned when they are no longer needed or used by the client. The IP addresses are managed, since the server can be administered, and show which IP addresses are assigned, and to which hosts.

Also, for the management of TCP/IP configurations, DHCP has the scope options facility. With this feature, other TCP/IP parameters on the client can be dynamically changed, such as the default gateway, assigning name servers (DNS, WINS), and assigning the DNS domain which the client will belong.

Incorrect Answers:

A: A DNS server provides IP address to NAME mappings. It does not affect any other TCP/IP configuration parameters.

B: The SNMP server is used to manage a network. It would not be able to even contact a client (or be contacted by a client) until that client received a valid IP address.

D: This is not a commonly known server, and definitely not listed within the general know list of TCP/IP servers.

QUESTION 75:

What is another name for Classless Interdomain Routing (CIDR)?

- A. Subnetting
- B. Supernetting
- C. IP forwarding
- D. Multicasting

Answer: B

Explanation: CIDR is a form of supernetting. It is essentially subnetting in reverse. In supernetting, or CIDR, we combine subnets to make a larger network. Remember in subnetting, we take a network and slice it up into subnet pieces. In Supernetting, we take pieces and splice them together to make a larger address space. Now supernetting does require that certain rules be followed, since you can't just take any pieces and splice them. The subnets being combined must be contiguous, the number of subnets being combined a power of two, and the first subnet should start at that power of two. What is done in the CIDR/Supernetting is to drop back on the 1 bits in the subnet mask. (Remember, in subnetting, we added 1 bits to the subnet mask).

Incorrect Answers:

A: AS explained in the answer, subnetting is essentially the opposite to supernetting, and supernetting is the process for CIDR.

C: IP Forwarding is the process where the routing function passes an IP packet to the next hop. IP addressing has to be considered during this process, but this is not an alternative name for CIDR.

D: Multicasting is a form of broadcasting where a specified group will receive the packets. In reality, broadcasting is a special form of multicasting where in broadcasting - everyone gets the packet. In either case, these are not related to CIDR.

QUESTION 76:

Which type of DNS server identifies the top-level domains on the Internet?

- A. Root
- B. Master
- C. Primary
- D. Caching

Answer: A

Explanation:

The highest level domain servers on the internet are the root servers. These are the servers service the domain . (Period, pronounced DOT). Off of this domain are your first level domains, such as COM, ORG, EDU, MIL, etc.

Incorrect Answers:

B: A Master DNS server maintains the DNS database for its appropriate zone. It is also the authority for the zone.

C: A primary DNS server is a DNS server that you would install locally at a company to service that company.

D: A caching DNS server has no authority nor database. It builds it cache of information based on information it receives calling other DNS servers while satisfying requests.

QUESTION 77:

How many bits are in the network portion of a Class B subnet mask?

- A. 8 bits
- B. 16 bits
- C. 32 bits
- D. 4 bits

Answer: B

Explanation: A Class B subnet mask is 16 bits network, 16 bits host

Incorrect Answers:

- A: A Class A subnet mask is 8 bits network, 24 bits host.
C: A subnet mask does not have a 32 bit network, that would be the entire mas.
D: At least 8 bits are used for the network, the first 4 bits represent the class type.
-

QUESTION 78:

Which URL leads to a reference site for researching Requests for Comments (RFCs)?

- A. <http://www.rfc-list.org/>
B. <http://www.rfc-editor.org/>
C. <http://www.rfc-home.org/>
D. <http://www.standards.org/>

Answer: B

Explanation:

Rfc-editor is the location. Since it is a not for profit organization, it uses the .ORG suffix.

Incorrect Answers:

A, C, D: These are not the correct URLs.

QUESTION 79:

Which OSI model layer represents the cable, wire or network media connecting two or more computers?

- A. Application
B. Session
C. Transport
D. Physical

Answer: D

Explanation: When you get down to the wire and cable, you are at the lowest layer, which is the Physical layer (Layer 1). This is the level that manufacturers must, at a minimum, provide device drivers. This level includes cable, wire, fiber, as well as microwave and satellite connections. Also running at this level are non-intelligent hubs, and repeaters.

Incorrect Answers:

A: The Application layer (Layer 7) is the highest layer in the OSI model, and is the farthest away from the network medium. The Application layer only talks with the presentation layer (Layer 6), the layer below it.

B: The Session Layer (Layer 5) is a very high layer in the OSI model, and is far away from the network medium. The Session layer only communicates with either the presentation layer (Layer 6) above, or the transport layer (Layer 4) below.

C: The Transport layer (Layer 4) is a high layer in the OSI model, and far away from the network medium. The transport layer only communicates with either the Session layer (layer 5) above or the Network layer (Layer 3) below.

QUESTION 80:

Which of the following is a routable protocol?

- A. NetBEUI
- B. DLC
- C. IPX/SPX
- D. PDC

Answer: C

Explanation: IPX/SPX is a routable protocol. By being routable, the header information of the packets and the addressing structure of the network provides the ability of correctly routing the packet from one network to another.

Incorrect Answers:

A, B: NetBEUI and DLC both run as IEEE 802.2 protocols, and are routable. These are essentially broadcast protocols that do not have any form of a network address.

D: PDC is not a network protocol.

QUESTION 81:

Which protocol is used to determine an IP address from a given hardware address?

- A. Address resolution protocol (ARP).
- B. Reverse address resolution protocol (RARP).
- C. Carrier sense multiple access with collision detection (CSMA/CD).
- D. Domain name system (DNS).

Answer: B

Explanation: RARP is used to find the IP address when the hardware (MAC) address is known.

Incorrect Answers:

B: ARP is the opposite. You give it the IP address and it returns the hardware (MAC) address.

C: CSMA/CD is the physical medium access method used by hardware protocols such as Ethernet. It is not directly involved with addressing.

D: A DNS server performs IP to NAME mappings. Neither is a hardware address.

QUESTION 82:

Which of the following is the name for a document that contains detailed information about standardized Internet protocols and those in various stages of development?

- A. Host file
- B. Frequently Asked Questions (FAQ)

- C. Standard (STD)
- D. Request for Comments (RFC)

Answer: D

Explanation: The request for comments is a series of technical reports about the Internet. There you will find discussions of different aspects of computing, including new and revised protocols, standards, procedures, and programs. Defined documents of the Internet protocol suite (standards) by the IETF (Internet Engineering Task Force). See: <http://www.rfc-editor.org>

Incorrect Answers:

- A: Host File I not the proper term for this.
- B: Frequently asked Questions is not the proper term for this.
- C: Standard is not the proper term for this. The Standard (STD) is the term used for RFC's that have become a standard, and does not include the RFC's that are proposed or still in development.

QUESTION 83:

Which of the following choices lists the two protocols that are used in the Internet architecture transport layer?

- A. ARP and RARP
- B. TCP and IP
- C. TCP and UDP
- D. DLC and NetBEUI

Answer: C

Explanation: TCP (Transmission Communications Protocol) and UDP (User Datagram Protocol) are transport layer protocols (Layer 4).

Incorrect Answers:

- A: ARP (Address Resolution Protocol) and RARP (Reverse Address Resolution Protocol) are used to map an IP address to a MAC address. These protocols run on the IP layer, which is the Network Layer, Layer 3.
- B: TCP (Transmission Communications Protocol) is a transport layer Layer 4) protocol, but IP is not. IP is a network layer (Layer 3) protocol.
- D: DLC (Data Link Control) and NetBEUI are data link layer (layer 2) protocols.

QUESTION 84:

Why was the Header Length field omitted from IPv6?

- A. IPv6 made it an option
- B. The IPv6 header is fixed as 40 Bytes
- C. IPv6 renamed it the Payload Length field

D. The IPv6 header is fixed as 20 bytes with options

Answer: B

Explanation: The IPv6 header is fixed at 40 bytes, also called 40 octets (8 bit units). Some questions will ask this in bits, which would be $(40 \times 8 = 160)$ 160 Bits.

Incorrect Answers:

A, C: The header does not specify or control the size of the header, the header is of fixed length.

D: The IPv6 header is fixed length, at 40 bytes. It is the IP4 header that is fixed as 20 bytes with options.

QUESTION 85:

Which protocol provides an encapsulation method for sending IP packets over a serial link?

- A. Point-to-Point Protocol (PPP)
- B. Transmission Control Protocol (TCP)
- C. Post Office Protocol (POP)
- D. User Datagram Protocol (UDP)

Answer: A

Explanation: There are two common protocols used to encapsulate IP packets across a serial link: SLIP (Serial Line Interface Protocol) and PPP. SLIP is rarely used anymore, PPP is commonly used today. SLIP & PPP runs at the physical layer (Layer 1). This allows PPP (because of the control information that PPP has that SLIP does not) to also transport non-IP traffic such as IPX and NetBUEI.

Incorrect Answers:

B: TCP is a transport layer protocol (Layer 4). TCP can be passed through a PPP link.

C: POP is used to receive mail from a mail server. POP is an application level protocol (Layer 7), and can be passed through a PPP connection.

D: UDP is a transport layer protocol (Layer 4). UDP can be passed through a PPP link.

QUESTION 86:

What is the default algorithm for IPv6 Authentication extension headers?

- A. Message Digest 3
- B. Message Digest 5
- C. Message Digest 6
- D. Message Digest 4

Answer: B

Explanation: Authentication is accomplished via Message Digest 5, abbreviated as MD5.

Incorrect Answers:

A, C, D: The answer is MD5, so these other answers are incorrect.

QUESTION 87:

Reiko works for an ISP where she must implement a DNS server that will host multiple company domains. Which type of DNS server must she install?

- A. Root.
- B. Caching
- C. Primary.
- D. Forwarding.

Answer: C

Explanation: When a domain is hosted, it is registered with a domain registry, and is added to the root servers. When a user wants to access the domain, the root server forwards the request to the DNS server that has been registered. If these are independent domains that are not subbed off the ISP's domain root, then these references should point directly to the DNS servers on the company's intranet.

Some companies are small, and do not run their own DNS servers. So what they will do is have the ISP run the DNS servers, and this is the process of hosting a DNS server for someone else. The DNS server receiving the requests, at the company's intranet, will normally be a primary zone DNS server,

Incorrect Answers:

A: AN ISP does not create a ROOT server. This is reserved by the various Internet Registry entities, responsible for updating and maintaining the root DNS servers. In North America, this would be InterNIC.

B: A caching server has no information in it. It builds information by requesting the required information, as requests are made, from other DNS servers. At least a primary DNS server with the information must be present, and at this point of entry, we need a primary zone DNS server.

D: The request received by the root is already forwarded. The type of server needed to host the DNS at this point need to be a primary zone DNS server.

QUESTION 88:

What is the predecessor to the Domain Name System (DNS)?

- A. Simple Network Management Protocol (SNMP)
- B. Hosts file
- C. NetBIOS
- D. Dynamic Host Configuration Protocol (DHCP)

Answer: B

Explanation: The HOSTS file was a hardcoded text file containing the IP to Name

mappings. When there were many hosts, this file became large, and grew to the point where it could not be managed. The hard part was that after the file was changed, getting all the machines to obtain the copy of the new file. The file grew so large, that it was unmanageable. Think of it this way: There are millions of domains out there, and probably over a hundred million nodes to be mapped, image a test file with a hundred million entries in it. Just scanning the file is prohibitive.

Although not mentioned in this problem, let me add this: There is also another file called LMHOSTS, which is similar to the HOSTS file. However, the LMHOSTS file is for NetBIOS mappings. HOSTS was replaced by DNS, LMHOSTS was replaced by WINS.

Incorrect Answers:

A: SNMP is an application protocol used to manage networks. It is not related to the DNS service.

C: NetBIOS is a layer 2 protocol that rides on the 802.2 specification. It does not interface with DNS, where DNS works on IP, a network layer protocol. DNS is an application, its traffic runs on port 53, all of it UDP traffic, except zone transfers which are TCP.

D: DHCP is a protocol that is used to assign IP addresses. As part of an option, the DHCP protocol can assign DNS server addresses, but that is as close as DHCP comes to DNS. DHCP does not provide IP to Name mappings.

QUESTION 89:

Which transport-layer protocol provides reliable delivery of data?

- A. IPX
- B. TCP
- C. IP
- D. HTTP

Answer: B

Explanation: TCP (Transmission Control Protocol) is a transport layer (Layer 4) protocol. It is connection oriented, and thus provides reliable delivery of data.

Incorrect Answers:

A: IPX is a network layer protocol (Layer 3) and does not provide reliable delivery of data. Reliable delivery is the responsibility of upper layer protocols. The network layer is only responsible for routing of the data, and is not concerned with actual delivery of that data, which at this level we call packets. The network layer runs essentially connection-less protocols.

C: IP is a network layer protocol (Layer 3) and does not provide reliable delivery of data. Reliable delivery is the responsibility of upper layer protocols. The network layer is only responsible for routing of the data, and is not concerned with actual delivery of that data, which at this level we call packets. The network layer runs essentially connection-less protocols.

D: HTTP is an application, which would run at the application layer (Layer 7), so it is not a transport layer protocol. HTTP relies on TCP, so there is reliable delivery of data. Do not get confused because HTTP is reliable and is a protocol, HTTP runs at layer 7 and the question asks for a layer 4 protocol.

QUESTION 90:

What is a typical length of Ipv4 header?

- A. 48bits.
- B. 120 bits.
- C. 160 bits.
- D. 1024 bits.

Answer: C

Explanation: The standard header for an IP Version 4 packet is 20 Octets (20 x 8 = 160 bits). The Ipv4 packet header has 12 require fields and one optional field.

Incorrect Answers:

A, B, D: The answer is 160 bits or 20 bytes. These other answers are incorrect.

QUESTION 91:

Reiko wants to use Dynamic Host configuration protocol (DHCP) to automatically configure the 100 client machines on her network. Ten of these machines are running Linux, and she wants them to have static IP addresses. The other 90 machines are Windows workstations, which do not need static IP addresses. Which is the best strategy for Reiko to configure the DHCP server?

- A. Use manual allocation for all machines
- B. Use dynamic allocation for all machines
- C. Use manual allocation for the Linux machines, and use dynamic allocation for the Windows machines
- D. Use manual allocation for the Linux machines, and use manual allocation for the Windows machines

Answer: C

Explanation: Since the Linux machines require static addresses, those machines must be configured with an IP address. If DHCP is to still be involved in the process for Linux, then those static addresses must be assigned to each machine using a reservation. Usually, a manual allocation will mean going to the Linux machine and hardcoding the IP address. For the Windows clients, all that needs to be done is make them DHCP clients. If the Linux machines are not set up as reservations, then the DHCP scope will not have (or exclude) the addresses used in the Linux machines.

Incorrect Answers:

A: The use of manual allocation for all machines would mean that DHCP is not required at all. This essentially means static IP addresses for all nodes. In order to support that environment under DHCP, every node would require a reservation, which is excessive work. The benefits of using DHCP in this environment would be small.

B: The only way to use dynamic allocation on all machines is to use reservations for the Linux

addresses. However, this would be assumed and reading too much into the question. Without reservations, you can't have static IP addresses in the scope range.

D: If manual allocation is used on the Windows machines, then a DHCP server is not required, and you lose the benefits of having DHCP on the network.

QUESTION 92:

Another term for Classless Interdomain Routing (CIDR) is;

- A. Subnetting
- B. Supernetting
- C. IP forwarding
- D. Multicasting

Answer: B

Explanation: CIDR is a form of supernetting. It is essentially subnetting in reverse. In supernetting, or CIDR, we combine subnets to make a larger network. Remember in subnetting, we take a network and slice it up into subnet pieces. In Supernetting, we take pieces and splice them together to make a larger address space. Now supernetting does require that certain rules be followed, since you can't just take any pieces and splice them. The subnets being combined must be contiguous, the number of subnets being combined a power of two, and the first subnet should start at that power of two. What is done in the CIDR/Supernetting is to drop back on the 1 bits in the subnet mask. (Remember, in subnetting, we added 1 bits to the subnet mask).

Incorrect Answers:

A: As explained in the answer, subnetting is essentially the opposite to supernetting, and supernetting is the process for CIDR.

C: IP Forwarding is the process where the routing function passes an IP packet to the next hop. IP addressing has to be considered during this process, but this is not an alternative name for CIDR.

D: Multicasting is a form of broadcasting where a specified group will receive the packets. In reality, broadcasting is a special form of multicasting where in broadcasting - everyone gets the packet. In either case, these are not related to CIDR.

QUESTION 93:

What is the term for the router on a local network that routes packets to remote destination networks?

- A. Proxy server
- B. Default gateway
- C. Domain controller
- D. Forwarding server

Answer: B

Explanation: The default gateway is the router address used to forward packets to another subnet, i.e. remote destination network. When a packet has to be shipped, the subnet mask is used to remove the host bits of the destination address, and if the resulting network of the destination does not match the current network, the packet is shipped to the default gateway.

Incorrect Answers:

A: A proxy server is used to connect two networks, usually (but not required) one of the networks is the Internet. The proxy server reissues all the IP requests on behalf of the clients it is servicing. The proxy server is not a router, although some of its functions appear as routing functions.

C: A domain controller is a server that services the logon requests of clients. Although routing services can be run on a domain controller so that the domain controller can perform routing, this is not the main function of a device called a domain controller. This is a routing function.

D: A forwarding server refers to a type of DNS server, which does not involve routing functions.

QUESTION 94:

Reiko's workstation cannot connect to the network. She checks the network configuration and finds the IP address is set to 127.45.23.6. Why is this a problem?

- A. This address is reserved by the ICANN for private networks
- B. This address is reserved for directed broadcasts
- C. This address is reserved as the Loopback address
- D. This address does not conform to the IPv4 standard

Answer: C

Explanation: IP addresses that begin with 127 (have the first octet as 127) are reserved for the loopback addresses.

Incorrect Answers:

A: The address ranges that are reserved by ICANN for private networks are:

10.0.0.0-10.255.255.255

172.16.0.0-172.31.255.255

192.168.0.0-192.168.255.255

B: Usually we would need to see the subnet mask to determine if this is a broadcast address. We can easily see without the subnet mask that it can't be. The last nibble (half of a octet) would be 0b'0110'. A directed broadcast, as an all ones broadcast, would have the host as all ones. Since the last bit of the address is a zero, this could not be an all ones broadcast.

D: The address does conform to IPv4 standards. However, if the address was not the loopback address, then we would need to see the subnet mask to see if the address was valid as a node address.

QUESTION 95:

Which field is common to all extension headers in IPv6?

- A. The protocol field
- B. The Next Header field
- C. The Type of service field
- D. The Hop Limit field

Answer: B

Explanation: The following table should be memorized, these are the code mappings.

Next Header Field	Function
0	Hop by hop options header
43	Routing Header
44	Fragment Header
60	Destination Options Header
52	ESP Header
59	No Next Header

As you can see, these codes are specified in the Next Header Field.

Incorrect Answers:

- A: The protocol field was renamed to the Next Header field. It does not exist as a field in Ipv6.
- C: The type of service field, which was a field in Ipv4, was removed and does not exist in Ipv6.
- D: The hop limit field was formerly known as the TTL field. Although this field does exist in Ipv6, it is not common to the extension headers.

QUESTION 96:

Which Internet Control Message Protocol (ICMPv6) message type would you receive if you incurred an IP header error?

- A. Destination Unreachable
- B. Redirect
- C. Parameter problem
- D. Time exceeded

Answer: C

Explanation: If an IPv6 node processing a packet finds a problem with a field in the IPv6

header or extension headers such that it cannot complete processing the packet, it MUST discard the packet and SHOULD send an ICMPv6 Parameter Problem message to the packet's source, indicating the type and location of the problem. (Reference: RFC 2463)

Incorrect Answers:

A: A Destination Unreachable message SHOULD be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion. (An ICMPv6 message MUST NOT be generated if a packet is dropped due to congestion.)

If the reason for the failure to deliver is lack of a matching entry in the forwarding node's routing table, the Code field is set to 0 (NOTE: this error can occur only in nodes that do not hold a "default route" in their routing tables).

If the reason for the failure to deliver is administrative prohibition, e.g., a "firewall filter", the Code field is set to 1.

If there is any other reason for the failure to deliver, e.g., inability to resolve the IPv6 destination address into a corresponding link address, or a link-specific problem of some sort, then the Code field is set to 3.

A destination node SHOULD send a Destination Unreachable message with Code 4 in response to a packet for which the transport protocol (e.g., UDP) has no listener, if that transport protocol has no alternative means to inform the sender. (Reference: RFC 2463)

B: Neighbor Discovery defines five different ICMP packet types: A pair of Router Solicitation and Router Advertisement messages, a pair of Neighbor Solicitation and Neighbor Advertisements messages, and a Redirect Message. The Redirect is used by routers to inform hosts of a better first hop for a destination. (Reference: RFC 2461)

D: If a router receives a packet with a Hop Limit of zero, or a router decrements a packet's Hop Limit to zero, it MUST discard the packet and send an ICMPv6 Time Exceeded message with Code 0 to the source of the packet. This indicates either a routing loop or too small an initial Hop Limit value. (Reference: RFC 2463)

QUESTION 97:

Given the IPv4 address 205.196.145.11, what is the converted IPv6 address?

- A. ::205.196.145.11
- B. 205.196.145::11
- C. 205::196.145.11
- D. 205.196.145.11::

Answer: A

Explanation: The dotted decimal representation of the Ipv6 address, which is a 128 bit address, is 8 sixteen bit integers, separated by a colon. The Ipv4 address is 4 eight bit integers separated by colons. The Ipv4 IP address is superimposed right justified over the Ipv6 address, and preceded by two consecutive colons.

Incorrect Answers:

B, C, D: although the notation of :: is used in the representation, the :: comes first, and these answers have the :: in the wrong position.

QUESTION 98:

Which extension header is identified by value 43 in the Next Header field?

- A. Hop-by-hop extension header
- B. Destination options extensions header
- C. Fragment extension header
- D. Routing extension header

Answer: D

Explanation: The following table should be memorized, these are the code mappings.

Next Header Field	Function
0	Hop by hop options header
43	Routing Header
44	Fragment Header
60	Destination Options Header
52	ESP Header
59	No Next Header

Incorrect Answers:

A, B, C: The proper codes for these headers can be searched in the given table above.

QUESTION 99:

Why was border gateway protocol (BGPv4) not updated for use in IPv6?

- A. It can already handle 128-bit addresses.
- B. It is a multiple-address routing protocol.
- C. It builds upon the hierarchical routing concept.
- D. It is optimized to work specifically with 32-bit addresses.

Answer: D

QUESTION 100:

What technology eliminates the concept of class A, B, and C networks?

- A. CIDR
- B. VAT
- C. NAT
- D. CIAT
- E. CSMA

Answer: A

Basically, CIDR eliminates the concept of class A, B, and C networks and replaces this with a generalized "IP prefix". CIDR can be used to perform route aggregation in which a single route can cover the address space of several "old-style" network numbers and thus replace a lot of old routes. This lessens the local administrative burden of updating external routing, saves routing table space in all backbone routers and reduces route flapping (rapid changes in routes), and thus CPU load, in all backbone routers. CIDR will also allow delegation of pieces of what used to be called "network numbers" to customers, and therefore make it possible to utilize the available address space more efficiently.

QUESTION 101:

Classless IP routing replaces a classfull address with:

- A. a generalized "IP prefix"
- B. a generalized "IP suffix"
- C. a specialized "IP prefix"
- D. a specialized "IP suffix"

Answer: A

Basically, CIDR eliminates the concept of class A, B, and C networks and replaces this with a generalized "IP prefix". CIDR can be used to perform route aggregation in which a single route can cover the address space of several "old-style" network numbers and thus replace a lot of old routes. This lessens the local administrative burden of updating external routing, saves routing table space in all backbone routers and reduces route flapping (rapid changes in routes), and thus CPU load, in all backbone routers. CIDR will also allow delegation of pieces of what used to be called "network numbers" to customers, and therefore make it possible to utilize the available address space more efficiently.

QUESTION 102:

Under CIDR, what is used to merge many networks into a logical domain?

- A. FSN
- B. CSN
- C. DSN
- D. ASN

Answer: D

ASN stands for Autonomous System Number and acts to merge many networks into a logical domain.

QUESTION 103:

CIDR saves spaces on which of the following?

- A. routing tables
- B. routing racks
- C. address space
- D. domain names

Answer: A

The routing tables in the Internet have been growing as fast as the Internet and the router technology specifically and computer technology in general has not been able to keep pace. In December 1990 there were 2190 routes and 2 years later there were over 8500 routes. In July 1995 there are now over 29,000 routes, which require approximately 10 MB in a router with a single peer. Routers at interconnection points (or multi-homed hosts doing full routing with many peers) receive these routes from several peers, and need several dozen megabytes of RAM (and the appropriate CPU horsepower) to handle this. A list of those routers that can handle this appears at the end of this question. Routers with 64MB of memory have the capacity for approximately 60,000 routes after which some routes will just have to be left out of the global routing tables, and the more likely ones to be left out are routes covering small pieces of address space.
Without the CIDRization work that has gone on for the past 2 years the routing tables would be in excess of 65,000 routes. By CIDRizing you help the Internet reduce the routing overload as well as increasing the likelihood that in the future your routes will be carried by all ISPs.

QUESTION 104:

Rules for subnetting TCP/IP networks can be found in which of the following RFCs (Choose two)?

- A. RFC 950
- B. RFC 1812
- C. RFC 952
- D. RFC 1814
- E. RFC 950

Answer: A,B

There are two sets of rules for subnetting TCP/IP networks. The original set of rules can be found in RFC 950, and the new set of rules can be found in RFC 1812.

QUESTION 105:

By using a subnet mask of 255.255.255.192, you can split the network into how many portions?

- A. three
- B. four
- C. five
- D. six
- E. eight

Answer: B

By using a subnet mask of 255.255.255.192, you can split the network into four portions, each with 64 hosts (62 usable.) Subnetwork one includes the addresses .1 through .62, subnetwork two includes the addresses .65 through .126, subnetwork three includes .129 through .190, and subnetwork four includes the hosts .193 through .254. On a true class "C" network, subnetwork four is not valid.

QUESTION 106:

By using a subnet mask of 255.255.255.192, you can split the network into portions with how many usable hosts on each portion?

- A. 32
- B. 52
- C. 62
- D. 64
- E. 80

Answer: C

By using a subnet mask of 255.255.255.192, you can split the network into four portions, each with 64 hosts (62 usable.) Subnetwork one includes the addresses .1 through .62, subnetwork two includes the addresses .65 through .126, subnetwork three includes .129 through .190, and subnetwork four includes the hosts .193 through .254. On a true class "C" network, subnetwork four is not valid.

QUESTION 107:

By using a subnet mask of 255.255.255.128, you can split that network into two halves, with the second half containing the host addresses from:

- A. 129 to .254
- B. 128 to .254
- C. 129 to .255
- D. 128 to .255

Answer: A

By using a subnet mask of 255.255.255.128, you can split that network into two halves, the first

half containing the host addresses .1 through .126, the second half containing the host addresses .129 through .254. Note that on a true class "C" network, you can't use the top subnet, since the bit in the subnet portion (one bit on a class "C") would be one (refer to ground rule "D".)

QUESTION 108:

The first routing decision made on an IP packet is made by which of the following?

- A. the user
- B. the gateway
- C. the workstation sending it
- D. the workstation receiving it

Answer: C

The primary use of the subnet mask (from our perspective at the Near Side of the 'Net) is for workstations to determine whether or not the server or workstation they're trying to talk to (the "destination IP address") is on the same subnet as itself; if the destination IP address is on your subnet, you'll send the IP packet directly to the other computer via the Ethernet or Token Ring (or whatever) network you're on, without bothering the router... at all! The first routing decision made on an IP packet is made by the workstation sending it; it decides whether or not to send the packet to a router.

QUESTION 109:

Subnet masks are often abbreviated using:

- A. a forward slash "/" and the number of "one" bits
- B. a backward slash "\" and the number of "one" bits
- C. a colon ":" and the number of "one" bits
- D. a semi-colon ";" and the number of "one" bits

Answer: A

Subnet masks are often abbreviated using a forward slash "/" and the number of "one" bits in the mask. For example, a network 192.168.1.0 with a subnet mask of 255.255.255.0 can be expressed as 192.168.1.0/24 (since 255.255.255.0 is 24 binary ones followed by eight binary zeros.) Therefore, a /25 subnet is a subnet with a mask of 255.255.255.128, and a /26 subnet has a mask of 255.255.255.192, etc.

QUESTION 110:

How many bits are used to form an IPv6 address?

- A. 16
- B. 32
- C. 256
- D. 128

Answer: D

QUESTION 111:

A SNMP Protocol Data Unit (PDU) type 1 is which type of command?

- A. GetResponse.
- B. GetRequest.
- C. GetNextRequest.
- D. SetRequest.

Answer: C

Explanation: Remember this table for Protocol Data Units (PDU) For SNMP:

Command	PDU Type
GetRequest	0
GetNextRequest	1
GetResponse	2
SetRequest	3
Trap	4

You will get questions on the exam that could ask you any of the 5 PDU types, you should remember them all.