Chapter 2: IP Addressing and Related Topics

TRUE/FALSE

1. IP addresses can be represented as domain names to make it possible for users to identify and access resources on a network.

   ANS: T PTS: 1 REF: 59

2. As a frame moves from interface to interface, the IP source and destination address information is preserved.

   ANS: T PTS: 1 REF: 59-60

3. Class D addresses always take the following binary form: bbbbbbbb.11111111.11111111.11111111.

   ANS: F PTS: 1 REF: 62

4. When a host uses a service that employs a multicast address, it registers itself to "listen" on that address, as well as on its own unique host address (and the broadcast address).

   ANS: T PTS: 1 REF: 62

5. Providing a narrower address space is the primary design goal for IPv6.

   ANS: F PTS: 1 REF: 77

MULTIPLE CHOICE

1. To be valid, any domain name must correspond to at least one unique ____.
   a. loopback address
   b. numeric IP address
   c. firewall
   d. IP gateway

   ANS: B PTS: 1 REF: 58

2. The ____ address is a six-byte numeric address, burned into firmware (on a chip) by network interface manufacturers.
   a. symbolic
   b. logical numeric
   c. reverse proxy
   d. physical numeric

   ANS: D PTS: 1 REF: 59

3. ____ is used to permit computers to translate numeric IP addresses to MAC layer addresses.
   a. ARP
   b. RARP
   c. Reverse proxying
   d. Subnet masking

   ANS: A PTS: 1 REF: 59

4. ____ is used to translate MAC layer addresses into numeric IP addresses.
   a. ARP
   b. RARP
   c. Reverse proxying
   d. Subnet masking

   ANS: B PTS: 1 REF: 59

5. The term ____ is used to describe the data frame crossing a router.
   a. firewall
   b. hop
   c. loopback
   d. dot squad

   ANS: B PTS: 1 REF: 60

6. ____ addresses are used for multicast communications, in which a single address may be associated with more than one network host machine.
   a. Class A
   b. Class B
   c. Class C
   d. Class D

   ANS: D PTS: 1 REF: 61

7. A ____ represents a network address that all hosts on a network must read.
   a. loopback
   b. hop
   c. broadcast address
   d. dot squad

   ANS: C PTS: 1 REF: 62

8. A ____ is a special bit pattern that "blocks off " the network portion of an IPv4 address with an all-ones pattern.
   a. reverse proxy
   b. summary address
   c. broadcast address
   d. subnet mask

   ANS: D PTS: 1 REF: 65

9. A(n) ____ is a device that interconnects multiple IP networks or subnets.
   a. subnet mask
   b. IP gateway
   c. layer-3 switch
   d. network address

   ANS: B PTS: 1 REF: 67

10. When a computer on one subnet wishes to communicate with a computer on another subnet, traffic must be forwarded from the sender to a nearby ____ to send the message on its way from one subnet to another.
    a. broadcast address
    b. IP gateway
    c. subnet mask
    d. proxy server

    ANS: B PTS: 1 REF: 67

11. The simplest form of subnet masking uses a technique called ____, in which each subnet includes the same number of stations and represents a simple division of the address space made available by subnetting into multiple equal segments.
    a. constant-length subnet masking
    b. firewall
    c. dot squad
    d. anycast

    ANS: A PTS: 1 REF: 67

12. One form of subnet masking uses a technique called ____ and permits a single address to be subdivided into multiple subnets, in which subnets need not all be the same size.
    a. IP gateway
    b. constant-length subnet masking
    c. variable-length subnet masking
    d. IP renumbering

    ANS: C PTS: 1 REF: 67

13. ____ gets its name from the notion that it ignores the traditional A, B, and C class designations for IP addresses and can therefore set the network-host ID boundary wherever it wants to, in a way that simplifies routing across the resulting IP address spaces.
    a. Route aggregation
    b. Address masquerading
    c. NAT
    d. Classless Inter-Domain Routing

    ANS: D PTS: 1 REF: 68

14. ____ allows IPv4 addresses from Class A, B, or C to be combined and treated as a larger address space, or subdivided arbitrarily, as needed.
    a. Supernetting
    b. Classless Inter-Domain Routing
    c. Subnet masking
    d. Address masquerading

    ANS: B PTS: 1 REF: 69

15. ____ may be performed by boundary devices that include proxy server capabilities to replace private IP addresses with one or more public IP addresses as outbound traffic exits the server, and to replace such public addresses with their proper private equivalents as incoming traffic passes through the server.
    a. IP renumbering
    b. Supernetting
    c. Address masquerading
    d. Subnetting

    ANS: C PTS: 1 REF: 70

16. One of the most important services that a ____ provides is to manage what source addresses appear in outbound packets that pass through it.
    a. loopback
    b. proxy server
    c. subnet mask
    d. layer-3 switch

    ANS: B PTS: 1 REF: 72

17. RFC ____ reserves three ranges of IP addresses for private use - a single Class A (10.0.0.0–10.255.255.255), 16 Class Bs (172.16.0.0–172.31.255.255), and 256 Class Cs (192.168.0.0–192.168.255.255).
    a. 1517
    b. 1518
    c. 1878
    d. 1918

    ANS: D PTS: 1 REF: 76

18. ____ lets networks use multiple private IPv4 addresses internally and maps them to one or more public IPv4 addresses externally.
    a. DNS
    b. IP gateway
    c. NAT
    d. VoIP

    ANS: C PTS: 1 REF: 76-77

19. Multicast addresses in IPv6 use a(n) ____ to define the portion of the Internet to which the multicast group pertains.
    a. scope identifier
    b. interface identifier
    c. loopback identifier
    d. aggregatable global unicast address

    ANS: A PTS: 1 REF: 80

20. Previously, IPv6 specified that interface identifiers followed the modified ____ format, which specifies a unique 64-bit interface identifier for each interface.
    a. RFC 4941
    c. EULA-64

b. EUI-64
d. IEEE 802.64v6

ANS: B PTS: 1 REF: 80

21. In IPv6, the ____ address is all zeroes and can be represented as two colon characters (::) in normal notation.
a. anycast
c. multicast
b. broadcast
d. unspecified

ANS: D PTS: 1 REF: 82

COMPLETION

1. The physical numeric address functions at a sublayer of the Data Link layer in the OSI network reference model, called the _____.

ANS:
Media Access Control layer
media access control layer
MAC layer

PTS: 1 REF: 59

2. _____ informs the network interface card to pass packets sent to that address to the IP stack so their contents can be read, and tells the IP gateway to forward such traffic onto the physical network, where the listening network interface resides.

ANS: Registration

PTS: 1 REF: 62-63

3. The activity of stealing (borrowing) bits from the host portion to further subdivide the network portion of an address is called _____.

ANS:
subnetting
subnetting a network address

PTS: 1 REF: 66

4. _____ combines contiguous network addresses by stealing bits from the network portion and using them to create a single, larger contiguous address space for host addresses.

ANS: Supernets

PTS: 1 REF: 67

5. In IPv6, _____ addresses are used to send an identical message to multiple hosts.

ANS: multicast

PTS: 1 REF: 83

MATCHING

Match each item with a statement below.

a. Solicited node address
b. Anycast address
c. Class E addresses
d. 255.0.0.0
e. 255.255.255.0
f. Secure end-to-end connection
g. ICANN
h. Application specific integrated circuits
i. Layer 3 switching

1. used by switches to make decisions
2. packets goes to the nearest single instance of this address
3. default mask for Class A networks
4. allows IP traffic to move in encrypted form between the sender and receiver without intermediate translation.
5. manages all IP-related addresses, protocol numbers, and well-known port addresses, and also assigns MAC layer addresses for use in network interfaces
6. default mask for Class C networks
7. special type of multicast address used to support Neighbor Solicitation (NS)
8. allows you to partition a large network into many smaller subnets, with almost no loss of performance
9. used for experimental purposes only

1. ANS: H PTS: 1 REF: 74
2. ANS: B PTS: 1 REF: 84
3. ANS: D PTS: 1 REF: 65
4. ANS: F PTS: 1 REF: 70-71
5. ANS: G PTS: 1 REF: 73
6. ANS: E PTS: 1 REF: 65
7. ANS: A PTS: 1 REF: 83
8. ANS: I PTS: 1 REF: 74
9. ANS: C PTS: 1 REF: 61

SHORT ANSWER

1. Briefly discuss IPs three-part addressing scheme.

   ANS:
   Symbolic: This consists of names that take a particular form, such as *www.support.dell.com*.
   Logical numeric: This consists of a set of four numbers, separated by periods, as in 172.16.1.10.Each of these four numbers must be smaller than 256 in decimal to be represented in eight binary digits, or bits.
   Physical numeric:This consists of a six-byte numeric address, burned into firmware (on a chip) by network interface manufacturers.

   PTS: 1 REF: 58-59

2. Why are concepts such as subnets and supernets important for TCP/IP networks?

   ANS:

The reason concepts like subnets and supernets are important for TCP/IP networks is that each of these ideas refers to a single “local neighborhood” on such a network, seen from a routing perspective. When network addresses are further subdivided beyond their defaults for whatever class to which an address belongs, such subnetting represents “stealing bits” (borrowing bits) from the host portion of the address and using those stolen (borrowed) bits to create multiple routing regions within the context of a single network address.

PTS: 1 REF: 66

3. Briefly describe how to calculate subnet masks.

ANS:
There are several varieties of subnet masks that you can design for a network, depending on how you want to implement an address segmentation scheme. The simplest form of subnet masking uses a technique called constant-length subnet masking (CLSM), in which each subnet includes the same number of stations and represents a simple division of the address space made available by subnetting into multiple equal segments.

Another form of subnet masking uses a technique called variable-length subnet masking (VLSM) and permits a single address to be subdivided into multiple subnets, in which subnets need not all be the same size.

PTS: 1 REF: 67

4. What are the limitations of creating a CIDR address?

ANS:
1. All the addresses in the CIDR address must be contiguous. Use of the standard network prefix notation for addresses,however, also makes it tidy and efficient to carve up any kind of address, as needed.

2. When address aggregation occurs, CIDR address blocks work best when they come in sets that are greater than 1 and equal to some lower-order bit pattern that corresponds to all 1s - namely in groups of 3, 7, 15, 31, and so on. That’s because this makes it possible to borrow the corresponding number of bits (two, three, four, five,and so on) from the network portion of the CIDR address block and use them to extend the host portion instead.

3. To use a CIDR address on any network, all routers in the routing domain must “understand” CIDR notation. This is typically not a problem for most routers that were built after September 1993, when RFCs 1517, 1518, and 1519 were approved, because most router vendors began to support CIDR addresses at that time.

PTS: 1 REF: 69

5. What are the disadvantages of using private IP addresses?

ANS:
The disadvantages are:

Such addresses may not be routed across the public Internet.

Some IP services require what's called a secure *end-to-end connection* - IP traffic must be able to move in encrypted form between the sender and receiver without intermediate translation. Thus, if either party to such a connection uses a public IP address, it's easiest to configure if both parties use a public IP address because the address for the "private end" of the connection cannot be routed directly across the Internet.

PTS: 1 REF: 70-71

6. Most organizations need public IP addresses only for two classes of equipment. Briefly describe each of these classes.

ANS:
Devices that permit organizations to attach networks to the Internet. These include the external interfaces on boundary devices of all kinds, such as routers, proxy servers, and firewalls, that help maintain the perimeter between the "outside" and "inside" on networks.

Servers that are designed to be accessible to the Internet. These include public Web servers, e-mail servers, FTP servers, news servers, and whatever other kind of TCP/IP Application layer services an organization may want to expose on the public Internet.

PTS: 1 REF: 71

7. List the constraints that determine the number and size of networks.

ANS:
These are:

Number of physical locations
Number of network devices at each location
Amount of broadcast traffic at each location
Availability of IP addresses
Delay caused by routing from one network to another

PTS: 1 REF: 73

8. Give two reasons why you should use binary boundaries.

ANS:
One reason is that, in the future, you may want to implement layer-3 switching to reduce the broadcast traffic, and if the devices fit in a binary boundary, you won't have to readdress them.

Another good reason to use binary boundaries is that one day you will want to classify your traffic to apply **Quality of Service** (**QoS**) or policies of some sort.

PTS: 1 REF: 75

9. What are some of the design goals for IPv6?

ANS:

Although providing a much larger address space is one of the primary design goals for IPv6, it is hardly the only reason for implementing IPv6, nor is this the only change made in the latest version of the IP protocol. IP has required a number of other important updates besides the lack of available unique addresses. IPv6 not only provides a vast abundance of IP addresses and better management of its address space, it eliminates the need for NAT and other technologies to be put in place to shore up the inadequate number of IPv4 addresses. IPv6 also makes it easier to administer and configure IP addresses.

Also, IPv6 has modernized routing support and natively allows for expansion along with the growing Internet.

Finally, IPv6 supports network security by using authentication and encryption extension headers, among other methods.

PTS: 1 REF: 77

10. How can you express native IPv6 addresses in URLs?

ANS:
RFC 2732 (originally proposed in 1999) describes a method to express IPv6 addresses in a form compatible with HTTP URLs. Because the colon character (:) is used by most browsers to set off a port number from an IPv4 address, native IPv6 addresses in their ordinary notation would cause problems. This RFC uses another pair of reserved characters, the square brackets ([and]), to enclose a literal IPv6 address. The RFC indicates that these square bracket characters are reserved in URLs exclusively for expressing IPv6 addresses. This RFC is now a standard, which means that this syntax represents the official format for expressing IPv6 addresses inside URLs.

Thus, an HTTP service available at port 70 of IPv6 address FEDC:BA98:7654:3210:FEDC:BA98:7654:3210 should be denoted as http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:70/ (in literal form).

PTS: 1 REF: 82