Network pro

You have implemented a network where hosts are assigned specific roles, such as for file sharing and printing. Other hosts access those resources but do not host services of their own.

What type of network do you have?

Client/server

Peer-to-peer

Intranet

Extranet

Client/server

Explanation

In a client/server network, hosts have specific roles. For example, some hosts are assigned server roles which allows them to provide network resources to other hosts. Other hosts are assigned client roles which allows them to consume network resources.

In a peer-to-peer network, each host can provide network resources to other hosts or access
resources located on other hosts, and each host is in charge of controlling access to those
resources.

An intranet is a private network that uses Internet technologies. Services on an intranet are only available to hosts that are connected to the private

network. An extranet is a private network that uses Internet technologies, but whose resources are made available to external (but trusted) users. For example, you might create a Web site on a private network that only users from a partner company can access.

You have implemented a network where each device provides shared files with all other devices on the network.

What type of network do you have?

Multiple access

Peer-to-peer

Polling

Client/server

Peer-to-peer

Explanation
In a peer-to-peer network, each host can provide network resources to other hosts or access resources located on other hosts, and each host is in charge of controlling access to those resources.

In a client/server network, hosts have specific roles. For example, some hosts are assigned server roles which allows them to provide network resources to other hosts. Other hosts are assigned client roles which allows them to consume network resources.

Polling is a media access method where a single device grants permission to other devices to access the network. Multiple access describes a media access method where each device determines when the medium is free.

You have a network that uses a logical bus topology. How do messages travel through the network?

Messages are broadcast to all devices connected to the network.

Messages travel from one device to the next until they reached the destination device.

Messages are sent to a central device which then forwards the message to the destination device.

Messages are sent directly to the correct destination device.

Messages are broadcast to all devices connected to the network.

Explanation
Messages sent using a physical bus topology are broadcast to all devices in the network. The device in the middle of the star (typically a hub), receives the message and forwards it on to all other devices.

In which of the following topologies does each device on the network act as a repeater, sending the signal to the next device?

Bus

Tree

Star

Ring

Ring

Explanation

In ring topologies, each device on the network acts as a repeater to send the signal to the next device.

Which of the following topologies connects each device to a neighboring device?

Bus

Tree

Ring

Star

Ring

Explanation

In ring topologies, each device is connected to a neighboring device, until a ring is formed.

You have a network that uses a logical ring topology. How do messages travel through the network?

Messages are sent directly to the destination device only.

Messages are sent to a central device which then forwards the message to the destination device.

Messages travel from one device to the next until they reached the destination device.

Messages are sent to all devices connected to the network.

Messages travel from one device to the next until they reached the destination device.

Explanation

In a logical ring topology, messages travel to each device in turn. If the message is not intended for that device, the message is forwarded to the next device on the network.

You have a small network that uses a hub to connect multiple devices. What physical topology is used?

Mesh

Ring

Star

Bus

Star

Explanation

A hub creates a network with a physical star topology. The physical star

topology uses a logical bus topology, where messages are sent to all devices connected to the hub. A mesh topology is a series of point-to-point links between devices. A ring topology uses a central device called an MSAU.

You have been asked to implement a network infrastructure that will accommodate failed connections. Which of the following network topologies provides redundancy for a failed link?

Star

Mesh

Bus

Ring

Mesh

Explanation
In a mesh topology, each network device is interconnected to all other network nodes. This creates multiple data paths and in the event of a failed link, the data has an alternate route to arrive at its destination.
The star topology connects network devices to the network with a single patch cable and the failure of a patch cable will make the connected device unavailable. The bus topology has a single point of failure, if there is a break in the network media, the network will be unavailable. A single break in a physical ring topology will disable the network.

You have implemented an adhoc wireless network that doesn't employ a wireless access point. Every wireless network card can communicate directly

with any other wireless network card on the network. What type of physical network topology has been implemented in this type of network?

Mesh

Ring

Star

Tree

Bus

Mesh

Explanation
This type of network uses a physical mesh topology. The key characteristics of a mesh topology
are:
• There's no central connecting point.
• Any host can communicate directly with any other host on the network.

A mesh network, such as this one, is usually impractical on a wired network. Each host would have to have a separate, dedicated network interface and cable for each host on the network. However, a mesh topology can be implemented with relative ease on a wireless network due to the lack of wires.

You want to implement a fault tolerant topology as you interconnect routers on your wide area network. Which of the following would meet your needs?

Bus

Ring

Mesh

Star

Mesh

Explanation

A mesh topology has multiple connections at each node, increasing connectivity fault tolerance. None of the other topologies have native fault tolerance built in.

Which of the following topologies connects all devices to a trunk cable?

Tree

Bus

Star

Ring

Bus

Explanation

The bus topology connects all devices to a trunk cable.

What device is used to create a physical star topology?

Switch

Firewall

Bridge

Router

Switch

Explanation

A physical star topology uses a switch or a hub. Routers are used to connect multiple subnets together. A firewall is a router that performs filtering on packets or other information contained in network communications.

Which of the following topologies connects each network device to a central hub?

Star

Mesh

Bus

Ring

Star

Explanation

Star topologies connect each device on the network to a central hub.

Which of the following protocols stores email on the mail server and gives users a choice to download mail or keep it on the server? (Select 2)

POP3

SMTP

NTP

IMAP4

IMAP4 & POP3

Explanation

IMAP4 allows a mail server to hold messages for a client. POP3 is a simpler protocol than IMAP4 that downloads email messages and deletes them from the server by default, but most newer POP3 clients provide an option to leave mail on the server after download. SMTP allows
a user to send email to a server. The NTP protocol synchronizes the clocks of all computers on a network.

Which protocol is used on the World Wide Web to transmit Web pages to Web browsers?

SMTP

HTML

HTTP

NNTP

HTTP

Explanation

HTTP or HyperText Transfer Protocol is used by Web servers and browsers to transmit Web pages on the Internet. This is often confused with HTML or HyperText Markup Language which is the markup language used to create Web content.

You want to transfer a file from a UNIX server to a Windows 2000 computer. Which of the following utilities could you use to do this? Select all that apply.

Netstat

TFTP

FTP

Tracert

Telnet

NBTSTAT

FTP & TFTP

Explanation

UNIX computers use TCP/IP, as do Windows 2000 computers. Therefore, the TCP/IP utilities FTP and TFTP will both allow you to transfer files.

Which of the following TCP/IP protocols do email clients use to download messages from a remote mail server?

SNMP

POP3

SPC

FTP

SMTP

POP3

Explanation

The POP3 protocol is part of the TCP/IP protocol suite and used to retrieve email from a remote server to a local client over a TCP/IP connection. SNMP is a protocol used to monitor network traffic. SMTP is a TCP/IP protocol used to send email. FTP is used to transfer files.

You want to allow your users to download files from a server running the TCP/IP protocol. You want to require user authentication to gain access to specific directories on the server. Which TCP/IP protocol should you implement to provide this capability?

HTML

FTP

IP

HTTP

TFTP

TCP

FTP

Explanation

You should implement the File Transfer Protocol (FTP). It enables file transfers and supports user authentication. The Trivial File Transfer Protocol (TFTP) enables file transfer, but does not support user authentication.

Which of the following protocols allows hosts to exchange messages to indicate problems with packet delivery?

IP

TCP

ARP

DHCP

IGMP

ICMP

ICMP

Explanation

The Internet Control Message Protocol (ICMP) allows hosts to exchange messages to indicate the status of a packet as it travels through the network.

Your company has just acquired another company in the same city. You are given the task of integrating the two email systems so that messages can be

exchanged between the email servers. However, each network uses an email package from a different vendor. Which TCP/IP protocol will enable messages to be exchanged between systems?

IMAP4

SMTP

ICMP

POP3

FTP

SMTP

Explanation
The Simple Mail Transfer Protocol (SMTP) specifies how messages are exchanged between email servers. POP3 and IMAP4 are used by email clients to download email messages from email servers. FTP is a file transfer protocol. ICMP is used in ping and traceroute for communicating network communication information.

You have a large TCP/IP network and want to keep hosts' real time clock synchronized. What protocol should you use?

SMTP

NNTP

SAP

NTP

SNMP

NTP

Explanation

The network time protocol (NTP) lets you keep clocks synchronized.

What protocol sends email to a mail server?

SNMP

POP3

SMTP

FTP

TFTP

SMTP

Explanation

SMTP sends email to a mail server.

You are asked to recommend an email retrieval protocol for a company's sales team. The sales team needs to access email from various locations and possibly different computers. The sales team does not want to worry about transferring email messages or files back and forth
between these computers. Which email protocol was designed for this purpose?

IMAP

SMTP

MFTP

POP4

POP3

IMAP

Explanation

The Internet Message Access Protocol (IMAP) is an email retrieval protocol designed to enable users to access their email from various locations without the need to transfer messages or files back and forth between computers. Messages remain on the remote mail server and are not automatically downloaded to a client system. POP3 is an email retrieval protocol that downloads and then deletes messages from a mail server. POP3 is well suited for reading email offline; however, you need to go online when you want to receive and send new messages. Once your new messages have been downloaded to your computer you can log off to read them. This option is often used when email is received over a dialup connection.

Which OSI model layer is responsible for guaranteeing reliable message delivery?

Transport

Application

Data Link

Session

Transport

Explanation

The Transport layer is responsible for connection services that provide reliable message delivery through error detection and correction mechanisms. Specifically, the TCP protocol provides these services. The Application layer integrates network functionality into the host operating system, and enables network services. The Session layer's primary function is managing the sessions in which data is transferred. The Data Link layer defines the rules and procedures for hosts as they access the Physical layer.

You are an application developer and are writing a program to exchange video files through a TCP/IP network. You need to select a transport protocol that will guarantee delivery. Which TCP/IP protocol would you implement that provides this capability?

RIP

TCP

IP

FTP

UDP

TFTP

TCP

Explanation

Write the application to use the Transmission Control Protocol (TCP). TCP guarantees delivery through error checking and acknowledgments.

Which three of the following functions are performed by the OSI Transport layer?

Reliable message delivery

Format packets for delivery through the media

Data segmentation and reassembly

End-to-end flow control

Path identification and selection

Control media access, logical topology, and device identification

Consistent data formatting between dissimilar systems

Reliable message delivery, Data segmentation and reassembly, & End-to-end flow control

Explanation

The Transport layer is responsible for taking upperlayer data, breaking it into segments, and providing for reliable communications through end-to-end flow control and error correction and detection. Transmitting messages through the media is performed at the Physical layer. Media access, logical

topology, and device identification occurs at the Data Link layer. Path identification and selection is a function of the Network layer. Data formatting is performed at the Presentation layer.

In the OSI model, what is the primary function of the Network layer?

Transmits data frames

Ensures that packets are delivered with no loss or duplication

Routes messages between networks

Allows applications to establish, use, and end a connection

Routes messages between networks

Explanation
The Network layer is responsible for routing messages between networks.

Which of the following functions are performed at the Physical layer of the OSI model?

Data translation

Movement of data across network cables

Conversation identification

Enablement of network services

Provision of an environment in which to run network applications

Movement of data across network cables

Explanation

The Physical layer is concerned with how to transmit data and how to connect network hosts.

In the OSI model, which of the following functions are performed at the Application layer? (Select all that apply.)

Data translation

Enabling communication between network clients and services

Conversation identification

Integration of network functionality into the host operating system

Enabling communication between network clients and services

Integration of network functionality into the host operating system

Explanation

The Application layer enables network services, and integrates network functionality into the
host operating system. Applications actually run above the OSI Application layer.
Conversation identification is accomplished at the Session layer through connection or
transaction ID numbers. Data translation is performed at the Presentation layer.

Which two of the following are included as part of Data Link layer specifications?

Composition of electrical signals as they pass through the transmission medium.

Controlling how messages are propagated through the network.

Synchronizing individual bits as they are transmitted through the network.

Identifying physical network devices.

Controlling how messages are propagated through the network.

Identifying physical network devices.

Explanation
The Data Link layer controls identifying devices on a network as well as how messages travel through the network (the logical topology).
The other functions listed here are performed by the Physical layer.

Which of the following tasks is associated with the Session layer?

Connection establishment

Acknowledgement coordination

Transmission synchronization

Host ID number assignment

Connection establishment

Explanation

Connection establishment is controlled through Session layer protocols.

What is the basic purpose of the OSI Physical layer?

Defines basic physical structures, such as disks.

Coordinates rules for managing network servers.

Coordinates rules for routing packets.

Coordinates rules for transmitting bits.

Coordinates rules for transmitting bits.

Explanation

The OSI Physical layer coordinates rules for transmitting bits.

Which of the following are functions of the MAC sublayer? (Select two.)

Mapping hardware addresses to linklayer addresses

Defining a unique hardware address for each device on the network

Creating routing tables based on MAC addresses

Letting devices on the network have access to the LAN

Defining a unique hardware address for each device on the network

Letting devices on the network have access to the LAN

Explanation

The MAC sublayer defines a unique MAC or datalink address for each device on the network. This address is usually assigned by the manufacturer. The MAC sublayer also provides devices with access to the network media.

The Data Link Layer of the OSI model is comprised of two sublayers. What are they? (Select two.)

LLC

DLC

LAT

MAC

SAN

Explanation

The Data Link layer is split into the following sublayers:

• Logical Link Control (LLC) Sublayer Provides the operating system link to the device driver.

• Media Access Control (MAC) Sublayer Translates generic network requests into device specific terms.

In the OSI model, which of the following functions are performed at the Presentation layer? (Select two.)

Maintain separate client connections

Handle general network access, flow control, and error recovery

Encrypt and compress data

Transmit data frames

Specify data format (such as file formats)

Provide network services

Encrypt and compress data

Specify data format (such as file formats)

Explanation

The Presentation layer encrypts data, changes and converts character sets, and compresses data. File formats (such as . jpg, . wmv, and . wav) are part of the Presentation layer. The Application layer provides network services. The Session layer maintains separate client connections through session IDs, and maintains those sessions. Flow control and error detection are provided at both the Transport layer and the Data Link layer. Transmitting frames happens at the Physical layer.

Which of the following protocols includes extensive error checking to ensure that a transmission is sent and received without mistakes?

TCP

UDP

UDB

UCP

TCP

Explanation

The TCP protocol includes error checking.

The UDP transport protocol provides which of the following features? (Select all that apply.)

Guaranteed delivery

Low overhead

Sequence numbers and acknowledgements

Connectionless datagram services

Low overhead

Connectionless datagram services

Explanation

UDP is a connectionless protocol used by applications that need low overhead and do not

require guaranteed delivery.

You are adding new wires in your building for some new offices. The building has a false ceiling that holds the lights. You would like to run your Ethernet cables in this area. Which type of cable must you use?

Plenum

PVC

Fiber optic

Cat 5e or Cat 6e

STP

Plenum

Explanation

Plenum cable is fire resistant and nontoxic; it must be used when wiring above ceiling tiles. PVC cable cannot be used to wire above ceilings because it is toxic when burned. Cat 5e cables provide better EMI protection than Cat 5 cables, and Cat 6e cables are an improvement over Cat 6 specifications, but neither are a requirement for using in a ceiling area. If the area has a lot of EMI, you might consider using STP or fiber optic cables, but this would not be a requirement just because wires were in a ceiling area. Typically, you can avoid EMI sources by rerouting cables.

In which of the following situations might you use an RJ11 connector?

You want to connect the 10BaseT network card in your computer to a switch.

You want to connect your computer to the Internet with a dialup connection.

You want to upgrade your 10BaseT network to 100BaseT.

You want to test a network cable to see if there is a break in the line.

You want to connect your computer to the Internet with a dialup connection.

Explanation

RJ11 connectors are typically used for telephones and modems.

You are installing networking wiring for a new Ethernet network at your company's main office building. The project specifications call for Category 5 UTP network cabling and RJ45 wall jacks. Near the end of the project, you run out of wire before the last few runs are complete.
You have a spool of Category 3 network cable in storage. Upon investigation, it appears very similar to Category 5 wiring. Should you substitute Category 3 cabling for Category 5 cabling to finish the project?

No, the sheath surrounding Category 5 cable is much thicker; creating an extra layer of shielding to reduce crosstalk and support higher data rates.

Yes, you can substitute Category 5 wiring with Category 3 wiring, as they are electrically identical.

No, Category 5 cabling has more twists per inch than Category 3 cabling to reduce crosstalk and support higher data rates.

No, Category 3 cabling doesn't support RJ45 connectors.

No, Category 5 cabling uses a thicker copper wire than Category 3 cable; enabling higher data transmission rates.

No, Category 5 cabling has more twists per inch than Category 3 cabling to reduce crosstalk and support higher data rates.

Explanation

While Category 3 and Category 5 cabling may appear similar physically, they

are electrically

different. Category 5 cabling is twisted much tighter than Category 3 cabling. This reduces

When would you typically use an RJ11 connector?

When using single mode fiber optic cables.

When connecting a phone to a phone line.

When using multimode fiber optic cables.

When using RG6 cables.

When using Cat 3 cables.

When using Cat 5 or higher cables.

When connecting a phone to a phone line.

Explanation

An RJ11 connector is used for connecting analog telephones to the telephone jacks. Cat 3, Cat 5, and higher twisted pair cables use RJ45 connectors. Coaxial cables use Ftype or BNC connectors. Fiber optic cables use a variety of connectors (RC, RT, LC, MTRJ).

Which of the following applications is more likely to justify the investment in Category 6 cable?

Instant Messaging

Printing

Email

Streaming video

Streaming video

Explanation

Category 6 cable is specified to extend the available bandwidth from 100 MHz to 200 MHz. This serves as the basis for greater capacity, throughput and reliability. Producing high quality streaming multimedia usually requires consistent highspeed network bandwidth.

Email and messaging are typically low bandwidth applications consisting of small, brief transmissions. Printing typically consists of greater amounts of data being transferred, however printing is highly amenable to delays and buffering and usually will not suffer any noticeable

effects with decreased bandwidth.

Which of the following cable types often includes a solid plastic core?

Cat 3

Cat 6

Cat 5e

Cat 5

Cat 6

Explanation

Cat 6 cables include a solid plastic core that keeps the twisted pairs separated and prevents the cable from being bent too tightly.

You have just signed up for a broadband home Internet service that uses coaxial cable. Which connector type will you most likely use?

RJ45

SC

Ftype

BNC

ST

RJ11

F-type

Explanation

Use an F-type connector for broadband cable connections that use coaxial cable. Use a BNC connector for 10Base2 Ethernet networks. Use an RJ11 connector for modem connections to a phone line. Use an RJ45 connector for an Ethernet network that uses twisted pair cable. Use ST and SC connectors for fiberoptic cables.

You have a small home network connected to the Internet using an RG6 cable. You need to move the router connecting the network to the Internet, but can't find any RG6 cable. Which cable types could you use instead?

RG8 or RG58

RG58 or RG59

RG8, RG58, or RG59

RG8

RG59

RG58

RG59

Explanation

RG6 has an impedance rating of 75 ohms. When using coaxial cables, it is important to use cables with the same impedance rating. Only RG59 is rated for 75 ohms. RG8 and RG58 are rated for 50 ohms.

F-type connectors are typically used with cables using which of the following standards? (Select two.)

RG58

Cat 6e

Cat 5e

RG6

Cat 5

RG59

RG6 & RG59

Explanation

F-type connectors are used with coaxial cable, and are typically used for cable TV and satellite installations using RG6 or RG59 cables. RG58 cables typically use BNC connectors and cables are used for 10Base2 Ethernet. Cat 5, 5e, and 6e cables use RJ45 connectors.

Which of the following cable classifications are typically used for cable and satellite networking with coaxial cables? (Select two.)

RG6

RG8

RG58

RG59

RG6 & RG59

Explanation

Both RG6 and RG59

can be used for cable and satellite networking applications, although RG6 has less signal loss than RG59, and is a better choice for networking applications, especially where longer distances (over a few feet) are involved. Both RG6 and RG59 have an impedance rating of 75 ohms.

RG8 and RG58 have an impedance rating of 50 ohms and were used with 10 Mbps Ethernet.

Of the following cables, which offer the best protection against EMI?

Cat 5e

Cat 5

Cat 6e

RG6

RG6

Explanation

Coaxial cable offers better protection against EMI than twisted pair cables. Coaxial cable has a mesh conductor which provides a ground and protects against EMI. In general, the higher the twisted pair cable standard, the better protection against some forms of EMI (typically crosstalk). For twisted pair, use shielded twisted pair instead of unshielded twisted pair. Use fiber optic for the best protection against EMI.

Which of the following are characteristics of coaxial network cable? (Choose three.)

It uses two concentric conductors made from plastic or glass which conduct light signals.

It has a conductor made from copper in the center of the cable.

It is composed of four pairs of 22-gauge copper wire.

The conductors within the cable are twisted around each other to eliminate crosstalk.

It uses two concentric metallic conductors.

The ends of the cable must be terminated.

It uses RJ45 connectors

It has a conductor made from copper in the center of the cable.
It uses two concentric metallic conductors.
The ends of the cable must be terminated.

Explanation
Coaxial cable is composed of a central copper conductor surrounded by an insulator which is then surrounded by a second metallic mesh conductor. The name coaxial is derived from the fact that both of these conductors share a common axis. When using coaxial cable, both ends of the cable must be terminated.

Which of the following are characteristics of an LC fiber optic connector? (Choose two.)

They use a stainless steel housing.

They are threaded.

They can be used with either fiber optic or copper cabling.

They use a one-piece bayonet connecting system.

They use a housing and latch system similar to an RJ45 UTP connector.

They are half the size of standard connectors.

They use a housing and latch system similar to an RJ45 UTP connector.

They are half the size of standard connectors.

Explanation
LC fiber optic connectors are small; about half the size of other fiber optic connectors. Their appearance is similar to a typical RJ45 connector used with UTP wiring. Like an RJ45 connector, it uses a small latch to lock the connector in a jack.

Of the following cables, which offer the best protection against EMI?

Cat 5e

Cat 5

RG6

Single mode fiber optic

Single mode fiber optic

Explanation Fiber optic cables offer the best protection against electromagnetic interference (EMI).

Which of the following forms of optical fiber would usually be used to connect two buildings across campus from each other, which are several kilometers apart?

Fibre Channel mode

Multimode

Single mode

Dual mode

Single mode

Explanation

In this scenario, use single mode fiber optic cables. Fiber optic is graded as single mode or multimode. Single mode consists of a single very thin core which produces fewer reflections. This provides greater effective bandwidth over greater distances. Multimode is less costly than single mode fiber. Multimode transmits multiple light rays concurrently. Multimode is used to transmit over shorter distances as the rays tend to disperse as the transmission distance increases. Fibre channel is a network topology used in storage area networks.

Which of the following are characteristics of an MT-RJ fiber optic connector? (Select two.)

They are used with multifiber fiber optic ribbon cables.

They use a nickel-plated housing.

They can be used with multimode fiber optic cables.

They use a keyed bayonet.

They must never be used with singlemode fiber-optic cables.

They use metal guide pins to ensure accurate alignment.

They can be used with multimode fiber optic cables.

They use metal guide pins to ensure accurate alignment.

Explanation

MTRJ connectors can be used with either multimode or single-mode fiber optic cabling. The connector is made from plastic and uses metal guide pins to ensure it is properly aligned in the jack.

Which of the following is true about single mode fiber optic network cabling?

It's less expensive than multimode fiber optic cabling.

The central core is smaller than that of multimode fiber optic cabling.

The central core is composed of braided plastic or glass fibers.

It doesn't support segment lengths as long as that supported by multimode fiber optic cabling.

It transmits multiple rays of light concurrently.

The central core is smaller than that of multimode fiber optic cabling.

Explanation

Single mode fiber optic cabling transmits a single ray (or mode) of light through glass or plastic fiber. It supports longer transmission distances than multimode fiber optic cable and is also more expensive. It also has a central

core that is much smaller than that of multimode fiber
optic cabling.

Which of the following are advantages of using fiber optic cabling for a network, as opposed to other types of cabling? (Select two.)

Immunity to electromagnetic interference

Lower installation cost

Greater cable distances without a repeater

Faster installation

Immunity to electromagnetic interference

Greater cable distances without a repeater

Explanation
Compared to other types of cabling, fiber optic cabling allows greater cable distances without a
repeater and is immune to electromagnetic interference. However, installation costs more and
takes longer.

Which of the following connectors is used with fiber optic cables and connects using a twisting motion?

F-type

SC

BNC

LC

ST

ST

Explanation

The ST connector is used with fiber optic cable and uses a twist-type connector. Tip: To remember the difference between ST and SC connectors, associate the T in ST with " twist". SC and LC connectors are used with fiber optic cables but plug in instead of twist. F-type
and BNC connectors use a twist to connect, but are used with coaxial cables.

Which of the following connectors are used with fiber optic cables and include both cables in a single connector? (Select two.)

SC

BNC

ST

MTRJ

LC

MTRJ

LC

Explanation

Both the LC and MTRJ connectors have both fiber optic cables in a single connector. ST and SC connectors hold a single strand of fiber optic cable. A cable using either connector has two connectors on each end. A BNC connector is used with coaxial cable.

Which of the following connectors usually require polishing as part of the assembly process? (Select two.)

BNC

SC

ST

IDC

AUI

SC & ST

Explanation

The fiber optic cable assembly process is more complex than other assemblies. It is necessary to polish the exposed fiber tip to ensure that light is passed on from one cable to the next with no dispersion.

Which of the following terms identifies the wiring closet in the basement or a ground floor that typically includes the demarcation point?

Smart jack

IDF

110 block

Horizontal cross connect

MDF

MDF

Explanation

The main distribution frame (MDF) is the main wiring point for a building. The MDF is typically located on the bottom floor or basement. The LEC typically installs the demarc to the MDF. An intermediate distribution frame (IDF) is a smaller wiring distribution point within a building. IDFs are typically located on each floor directly above the MDF, although additional IDFs can be added on each floor as necessary.

A horizontal cross connect connects wiring closets on the same floor. A smart jack is a special loopback plug installed at the demarcation point for a WAN service. Technicians at the central office can send diagnostic commands to the smart plug to test connectivity between the central office and the demarc. Use 66 and 110 blocks to connect individual wires within a wiring closet.

Which of the following methods would you use to create a crossover cable?

Use the T568B standard.

Use the T568A standard on one connector, and the BLOG convention on the other connector.

Use the T568A standard on one connector, and the T568B standard on the other connector.

Use the T568B standard on one connector, and the BLOG convention on the other connector.

Use the T568A standard.

Use the T568A standard on one connector, and the T568B standard on the other connector.

Explanation
The easiest way to create a crossover cable is to arrange the wires in the first connector using the T568A standard and arrange the wires in the second connector using the T568B standard. A crossover cable connects the transmit pins on one connector to the receive pins on the other connector (pin 1 to pin 3 and pin 2 to pin 6).

When using 110 blocks for connecting Cat5 and higher data cables, which recommendation should you follow?

Keep wire pairs twisted up to within one-half of an inch of the connector.

Use C5 connectors.

Connect wires using the T568B standard.

Connect wires using the T568A standard.

Keep wire pairs twisted up to within one-half of an inch of the connector.

Explanation

When using for Cat5 (or higher) wiring, be sure to preserve the twists in each wire pair to within one-half of an inch of the connecting block.

Use C4 connectors to connect four pairs of wires. When connecting data wires on a 110 block, you typically connect wires in the following order:

• White wire with a blue stripe, followed by the solid blue wire.

• White wire with an orange stripe, followed by the solid orange wire.

• White wire with a green stripe, followed by the solid green wire.

• White wire with a brown stripe, followed by the solid brown wire.

T568A and T568B are used to connect wires within an RJ45 connector when making drop cables.

You are building network cables and attaching RJ45 connectors to each end. Which tool do you need for this task?

Vampire taps

Crimping tool

Punch down tool

Needle nose pliers

Crimping tool

Explanation

You should use a crimping tool designed for RJ45 connectors to attach connectors to UTP cable.

You have a network that occupies both floors of a building. The WAN service provider has installed the line for the WAN service into the building in a wiring closet on the main floor. You have a second wiring closet on the second floor directly above the wiring closet that holds
the demarc. Which of the following terms describes the closet on the second floor?

Vertical cross connect

Demarc extension

MDF

IDF

Horizontal cross connect

IDF

Explanation
An intermediate distribution frame (IDF) is a smaller wiring distribution point within a building. IDFs are typically located on each floor directly above the MDF, although additional IDFs can be added on each floor as necessary. The main distribution frame (MDF) is the main wiring point for a building. The MDF is typically located on the bottom floor or basement. The LEC typically installs the demarc to the MDF. A vertical cross connect connects the MDF on the main floor to IDFs on upper floors. Cabling runs vertically (up and down) between the MDF and the IDFs. A horizontal cross connect connects IDFs on the same floor. Cabling runs horizontally (sideways) between the IDFs. A

demarc extension extends the demarcation point from its original location to another location within the building.

What tool should you use to extend network services beyond the demarc?

Media certifier

Tone generator

Crimper

Punchdown tool

Punchdown tool

Explanation
A demarc is the location where the local network ends and the telephone company's network begins. This location is usually at a punch down block in a wiring closet. You use a punchdown tool to attach wires to the punch down block.

Which of the following describes the point where the service provider's responsibility ends and the customer's responsibility begins for installing and maintaining wiring and equipment?

Smart jack

Punchdown block

IDF

Demarc

Vertical cross connect

Demarc

Explanation

When you contract with a local exchange carrier (LEC) for data or telephone services, they install a physical cable and a termination jack onto your premises. The demarcation point (demarc) is the line that marks the boundary between the telco equipment and the private network or telephone system. Typically, the LEC is responsible for all equipment on one side of the demarc, and the customer is responsible for all equipment on the other side of the demarc. A smart jack is a special loopback plug installed at the demarcation point for a WAN service. Technicians at the central office can send diagnostic commands to the smart plug to test connectivity between the central office and the demarc. A punchdown block is a block used to connect individual copper wires together. While the demarc might terminate in a punchdown block, punchdown blocks are used within other locations at the customer site. An intermediate distribution frame (IDF) is a smaller wiring distribution point within a building. IDFs are typically located on each floor directly above the main distribution frame (MDF), although additional IDFs can be added on each floor as necessary. A vertical cross connect connects the IDF to the MDF on a different floor.

You are preparing to attach wires in a 110 block. You want to connect the wires and trim off the excess at the same time. Which of the following should you do? (Select two.)

Use a butt set with clips.

Use a punchdown tool with a notched blade.

Point the cut side of the tool towards the connected end of the wire.

Use a punchdown tool with a straight blade.

Use a butt set with a jack.

Point the cut side of the tool towards the wire end.

Use a punchdown tool with a notched blade.

Point the cut side of the tool towards the wire end.

Explanation

Use a punchdown tool to connect wires to a 110 or 66 block. When using a punchdown tool, choose the right blade for the job:

• Use a notched blade for a 110 block.

• Use a straight blade for a 66 block.

• For both blade types, you can use the end without a cutting blade if you want to punch down without cutting the wire. When using the cutting blade, point the cut side of the punchdown tool towards the wire end that you want to trim.

You are making Ethernet drop cables using Cat5e cable and RJ45 connectors. You need to remove the plastic coating over the cable to expose the individual wires. Which tool should you use?

Snips

Punchdown tool

Butt set

Cable stripper

Cable stripper

Explanation

Use a cable stripper to remove the plastic covering for a cable. Note: When making drop cables or using punchdown blocks, do not remove the plastic covering for individual wires. Use snips to cut cables. Use a punchdown tool to push wires into 66 or 110 blocks and cut wires at the same time. Use a butt set to connect to phone lines to monitor, make, or answer phone calls.

You have a network that occupies the top floor of a three story building. The WAN service provider has installed the line for the WAN service into the building in a wiring closet on the main floor. What would you use to relocate the WAN line into a wiring closet on your floor?

Horizontal cross connect

Demarc extension

66 block

Smart jack

110 block

Demarc extension

Explanation

A demarc extension extends the demarcation point from its original location to another location within the building. The demarc extension typically consists of a single wire bundle that attaches to the existing demarc and supplies a termination point to a different location. You might need a demarc extension if your network occupies an upper floor of a building. The LEC will typically install the demarc into the MDF on the bottom floor, and you will need to install an extension to place the demarc into the IDF on your floor. A horizontal cross connect connects IDFs on the same floor. Cabling runs horizontally (sideways) between the IDFs. A smart jack is a special loopback plug installed at the demarcation point for a WAN service. Technicians at the central office can send diagnostic commands to the smart plug to test connectivity between the central office and the demarc. Use 66 and 110 blocks to connect individual wires within a wiring closet. These blocks can be used to connect devices to the WAN service wiring, but are not typically used for installing a demarc extension.

You have a network that occupies all three floors of a building. The WAN service provider has installed the line for the WAN service into the building in a wiring closet on the main floor. You have a wiring closet on the two remaining floors directly above the wiring closet on the main floor. What would you use to connect the wiring closets together?

Demarc extension

Horizontal cross connect

Vertical cross connect

Smart jack

Vertical cross connect

Explanation

A vertical cross connect connects the main distribution frame (MDF) on the main floor to intermediate distribution frames (IDFs) on upper floors. Cabling runs vertically (up and down) between the MDF and the IDFs. A horizontal cross connect connects IDFs on the same floor. Cabling runs horizontally (sideways) between the IDFs. A smart jack is a special loopback plug installed at the demarcation point for a WAN service. Technicians at the central office can send diagnostic commands to the smart plug to test connectivity between the central office and the demarc. A demarc extension extends the demarcation point from its original location to another location within the building. The demarc extension typically consists of a single wire bundle that attaches to the existing demarc and supplies a termination point to a different location. You might need a demarc extension if your network occupies an upper floor of a building. The LEC will typically install the demarc into the MDF on the bottom floor, and you will need to install an extension to place the demarc into the IDF on your floor.

Which pins in an RJ45 connector are used to transmit data when used on a 100BaseT Ethernet network? (Choose two.)

Pin 1

Pin 2

Pin 3

Pin 4

Pin 5

Pin 6

Pin 7

Pin 8

Pin 1 & Pin 2

Explanation

On a 100BaseT network cable, the RJ45 pinouts are as follows:

• Pin 1: Tx+

• Pin 2: Tx-

•Pin 3: Rx+

• Pin 4: Unused

• Pin 5: Unused

• Pin 6: Rx-

•Pin 7: Unused

• Pin 8: Unused

You want to use the T568A standard for adding connectors to your Cat5 cable. Starting with pin 1, which order should you use for the wires within the connector?

White/orange, orange, white/green, blue, white/blue, green, white/brown, brown

White/green, green, white/orange, blue, white/blue, orange, white/brown, brown

White/orange, orange, white/green, green, white/blue, blue, white/brown, brown

White/blue, blue, white/orange, orange, white/green, green, white/brown, brown

White/green, green, white/orange, blue, white/blue, orange, white/brown, brown

Explanation

The T568A standard uses the following order of wires in the connector: White/green, green, white/orange, blue, white/blue, orange, white/brown, brown. The T568B standard switches the orange and green wires (along with their corresponding white wires). Use the order Blue-Orange-Green-Brown (BLOG), with the white wire first, for connecting wires on a 110 punchdown block.

Which of the following uses metal clips placed over plastic slots for connecting individual copper wires?

25 pair

66 block

100 pair

110 block

110 block

Explanation

A 110 block is a punchdown block that uses metal clips fitted over plastic pins. When connecting wires using a 110 block, place the wires in the plastic slots, attach the metal clip, then punch down the connecting cable on the top of the clip. A 66 block uses metal pins for connecting wires. Wires are placed in the pins, and pins within a row are electrically connected. 25 pair and 100 pair are cable bundles that include multiple pairs of copper wires (either 25 pairs of wires or 100 pairs of wires).

You are connecting Cat5e cables to a 110 block. In what order should you connect the wires to follow standard wiring conventions?

White/orange, orange, white/green, blue, white/blue, green, white/brown, brown

White/green, green, white/orange, blue, white/blue, orange, white/brown, brown

White/blue, blue, white/orange, orange, white/green, green, white/brown, brown

White/brown, brown, white/blue, blue, white/orange, orange, white/green, green

White/blue, blue, white/orange, orange, white/green, green, white/brown, brown

Explanation

When connecting data wires on a 110 block, you typically connect wires in

the following order:

• White wire with a blue stripe, followed by the solid blue wire.

• White wire with an orange stripe, followed by the solid orange wire.

• White wire with a green stripe, followed by the solid green wire.

• White wire with a brown stripe, followed by the solid brown wire.

Tip: Use BLOG (blue-orange-green) to remember the wire order, and remember to start with the white striped wire first.

When adding RJ45 connectors to a drop cable, use one of the following orders, based on the standard you want to follow:

• T568A- To use this standard, arrange the wires from pins 1 to 8 in each connector in the following order: GW, G, OW, B, BW, O, BrW, Br.

• T568B- To use this standard, arrange the wires from pins 1 to 8 in each connector in the following order: OW, O, GW, B, BW, G, BrW, Br.

You are working with 25 pair wires and 66 blocks. You have pushed the wires onto the 66 block, but now need to cut off the excess end of each wire. Which tool should you use?

Snips

Butt set

Cable stripper

Punchdown tool

Punchdown tool

Explanation

Use a punchdown tool to push wires into 66 or 110 blocks and cut wires at the same time. The punchdown tool has a blade on one side the cuts off the excess wires. Use snips to cut cables or wires. However, a punchdown tool would be easier to use for this task than wire snips. Use a cable stripper to remove the plastic covering for a cable. Note: When making drop cables or using punchdown blocks, do not remove the plastic covering for individual wires. Use a butt set to connect to phone lines to monitor, make, or answer phone calls.

Which of the following is used to terminate individual wires from a 25 pair or 100 pair cable using female RJ45 ports?

66 block

110 block

Patch panel

Horizontal cross connect

Patch panel

Explanation

A patch panel is a device that typically connects individual stranded wires into female RJ45 connectors. For example, you might connect 4 pairs of wires from a punchdown block to a port on the patch panel. On the patch panel, you then connect drop cables (cables with RJ45
connectors) to the patch panel on one end and a computer on the other end.

Use 66 and 110 blocks to connect individual wires within a wiring closet. These punchdown blocks connect the individual wires together, but do not terminate in RJ45 connectors. A horizontal cross connect connects IDFs on the same floor.

You want to use the T568B standard for adding connectors to your Cat5 cable. Starting with pin 1, which order should you use for the wires within the connector?

White/blue, blue, white/orange, orange, white/green, green, white/brown, brown

White/orange, orange, white/green, blue, white/blue, green, white/brown, brown

White/orange, orange, white/green, green, white/blue, blue, white/brown, brown

White/green, green, white/orange, blue, white/blue, orange, white/brown, brown

White/orange, orange, white/green, blue, white/blue, green, white/brown, brown

Explanation

The T568B standard uses the following order of wires in the connector: White/orange, orange, white/green, blue, white/blue, green, white/brown, brown.

The T568A standard switches the green and orange wires (along with their corresponding white wires). Use the order Blue-Orange-Green-Brown (BLOG), with the white wire first, for connecting wires on a 110 punchdown block.

You have a network that occupies all three floors of a building. The WAN service provider has installed the line for the WAN service into the building in a wiring closet on the main floor. You have a second wiring closet on the main floor. You need to connect the two wiring closets.
Which of the following are typically used to connect the two wiring closets? (Select two.)

Demarc extension

25 pair

Horizontal cross connect

Smart jack

Vertical cross connect

25 pair

Horizontal cross connect

Explanation
A horizontal cross connect connects wiring closets on the same floor. 25 pair or 100 pair wiring punched down into 66 or 110 blocks are often used to connect the wiring closets together. A vertical cross connect connects the

IDF to the MDF on a different floor. The demarcation point (demarc) is the line that marks the boundary between the telco equipment and the private network or telephone system. A demarc extension extends the demarcation point from its original location to another location within the building. A smart jack is a special loopback plug installed at the demarcation point for a WAN service. Technicians at the central office can send diagnostic commands to the smart plug to test connectivity between the central office and the demarc.

A host wants to send a message to another host with the IP address 115. 99. 80. 157. IP does not know the hardware address of the destination device. Which protocol can be used to discover the MAC address?

DNS

IGMP

BOOTP

DHCP

ARP

ICMP

ARP

Explanation

Hosts use the Address Resolution Protocol (ARP) to discover the hardware address of a host.

Which of the following is a valid MAC address?

95ABC2F4. ABC5. 569D. 43BF

AB. 07. CF. 62. 16. BD

FABC. 875E. 9BG6

145. 65. 254. 10

AB. 07. CF. 62. 16. BD

Explanation

MAC addresses are comprised of 12 hexadecimal digits (ranging from 09 and AF). They are typically represented as a three sets of four hexadecimal digits or six sets of two hexadecimal digits separated with periods. Regardless of the grouping and separator values, look for 12 hex digits for a valid MAC address.

What device sends signals from a computer onto a network?

Router

Transceiver

Cable

Gateway

Transceiver

Explanation

A transceiver (short for transmitter/receiver) sends signals to and receives signals from the network. It translates the parallel data stream of the computer to the serial data stream of the network and vice versa. Most transceivers are now built into network interface cards (NICs).

Which of the following is true about the MAC address? (Select two.)

It is typically represented by octets of decimal numbers between 0255.

It is a 32-bit address.

It is a 64-bit address.

It is a 48-bit address.

It is typically represented by hexadecimal numbers.

It is a 48-bit address.

It is typically represented by hexadecimal numbers.

Explanation

The MAC address identifies the physical address of the network adapter. The MAC address is a 12-digit (48-bit) hexadecimal number (each number ranges from 09 or AF). The address is often written as 00B0D006BCAC or 00B0. D006. BCAC, although dashes, periods, and
colons can be used to divide the MAC address parts. An IPv4 address is 32bits and uses octets of decimal numbers between 0255. An IPv6 address is a 64-bit address that uses 32 hexadecimal numbers.

Which network component connects a device with the transmission media and allows it to send and receive messages?

Client

Network interface card

Peripheral

Protocol

Server

Network interface card

Explanation
The network interface card (NIC) allows a device to send and receive messages over the transmission media.

Which of the following is a valid MAC address?

73-99-12-61-15

192. 168. 12. 15

34-9A-86-1G-B3-24

C0-34-FF-15-01-8E

255. 255. 255. 0

83-5A-5B-0B-31-55-F1

C0-34-FF-15-01-8E

Explanation

A MAC or hardware address is a unique identifier hard coded on every network adapter card. A valid MAC address has a total of 12 hexadecimal numbers. Hexadecimal numbers contain the numbers 0 to 9 and the letters A to F. Valid values in a MAC address range anywhere from 00 to FF. Note that one of the answers would be a valid MAC address except it uses a G value, which is beyond the range of a hexadecimal number.

At which OSI model layer does a media converter operate?

Layer 1

Layer 2

Layer 3

Layer 4

Layer 1

Explanation

A media converter operates at the OSI model layer 1 (Physical layer). The media converter translates frames into bits and transmits them on the transmission medium. At layer 2, the MAC address is added to make the data into a frame. At layer 3, the IP address is added to the packet. A media converter does not alter or use the MAC address or the IP address.

You have a server that has a 100BaseFX network interface card that you need to connect to a switch. The switch only has 100BaseTX switch ports. Which device should you use?

Gateway

Bridge

Media converter

Hub

Repeater

Media converter

Explanation
Use a media converter to convert from one media type to another media type within the same architecture. Use a bridge to connect two devices that use different network architectures, for example to connect a wired network to wireless clients. A hub or a repeater connect devices using the same media type.

What type of module might a switch use to allow it to modify the media type supported by a switch port? (Select two.)

MPLS

GBIC

OCx

SFP

GBIC & SFP

Explanation
Older network adapters used an external transceiver that matched the media type. While nearly all current network adapters come with a built in transceiver type, new devices, such as switches and routers, use transceiver modules that allow you to modify the media type of a
port by changing the transceiver. Transceiver modules include the following:

• A GBIC (gigabit interface converter) is a larger sized transceiver that fits in a port slot and is used for Gigabit media including copper and fiber optic.
• An SFP (small formfactor pluggable) is similar to a GBIC but with a smaller size. An SFP is sometimes called a miniGBIC.
• An XFP transceiver is similar in size to an SFP but is used for 10 Gigabit networking.

Which of the following statements accurately describes how a modem works? (Select two.)

It modulates digital data from the PC into analog data and transmits it on a telephone network.

It communicates over a telephone network using digital signals.

It transmits digital signals over ordinary telephone copper wiring at a rate up to 128 Kbps.

It demodulates analog data from a telephone network into digital PC data.

It demodulates analog PC data into digital data that can be transmitted through a telephone network.

It modulates digital data from a telephone network into analog data that a PC can use.

It modulates digital data from the PC into analog data and transmits it on a telephone network.

It demodulates analog data from a telephone network into digital PC data.

Explanation
Modem is shorthand for modulator/demodulator. Its job is to convert (or modulate) digital data from a PC into analog telephone signals and transmit them through a telephone network. It also receives analog data from the telephone network and converts (or demodulates) it into
digital PC data.

Which three of the following devices operate at the Data Link layer of the OSI model?

Routers

Bridges

Switches

Repeaters

Network interface cards (NICs)

Hubs

Bridges, Switches & NICs

Explanation

Network interface cards (NICs), bridges, and switches all operate at the OSI Data Link layer. They use the physical device address (MAC address) to identify packets. Hubs and repeaters operate at the Physical layer they simply repeat packets without regard to addresses. Routers function at the Network layer they examine the logical device and network address to perform routing tasks.

Which of the following hardware devices regenerates a signal out all connected ports without examining the frame or packet contents? (Select two.)

Bridge

Hub

Repeater

Switch

Gateway

Router

Hub & Repeater

Explanation

A hub and a repeater send received signals out all other ports. These devices do not examine the frame or the packet contents. A switch or a bridge use the MAC address in a frame for forwarding decisions. A router uses the IP address in a packet for forwarding decisions.

Which of the following best describes how a switch functions?

It connects multiple segments of different architectures. It translates frames, and forwards them to the appropriate segment.

It connects multiple segments of different architectures. It translates frames, and broadcasts them to all of its ports.

It connects multiple cable segments (or devices), and forwards frames to the appropriate segment.

It connects multiple cable segments (or devices), and broadcasts frames to all of its ports.

It connects multiple cable segments (or devices), and forwards frames to the appropriate segment.

Explanation

Switches have multiple ports and can connect multiple segments or devices. The switch forwards frames to the appropriate port. They function similarly to a hub, except instead of sending packets to all ports, switches send packets only to the destination computer's port.

A switch is associated with which OSI model layer?

Transport

Network

Data Link

Physical

Data Link

Explanation

Switches are associated with the Data Link layer of the OSI model. Switches examine the device address in the packet and forward messages directly to that device.

How do switches and bridges learn where devices are located on a network?

When a frame enters a port, the destination IP address is copied from the frame header.

When a frame enters a port, the source IP address is copied from the frame header.

When a frame enters a port, the source MAC address is copied from the frame header.

When a frame enters a port, the destination MAC address is copied from frame header.

When a frame enters a port, the source MAC address is copied from the frame header.

Explanation

Bridges and switches learn addresses by copying the MAC address of the source device and placing it into the MAC address table. The port number which the frame entered is also recorded in the table and associated with the source MAC address. The switch or the bridge cannot record the destination MAC address because it does not know the port that is used to reach the destination device. Bridges and switches operate at Layer 2 and do not use IP addresses (which exist at Layer 3).

An access point that conforms to the IEEE 802. 11b standard acts most closely to what other networking device?

Router

Gateway

Hub

Terminal

Patch bay

Hub

Explanation

An access point functions like a hub by connecting multiple wireless hosts to a wired Ethernet network.

At which layer of the OSI model do hubs operate?

Data Link

Internet

Physical

Layer 3

Physical

Explanation

Hubs operate at layer 1, or the Physical layer of the OSI model.

Your company purchases a new bridge, which filters packets based on the MAC address of the destination computer. On which layer of the OSI model is this device functioning?

Data Link

Transport

Presentation

Session

Data Link

Explanation

The bridge is operating at the Data Link layer.

Which of the following devices operate at OSI model layer 2? (Select two.)

Network interface card

Firewall

Switch

Hub

Repeater

Router

Switch & Network interface card

Explanation

A network interface card and a switch operate at layer 2 (Data Link) of the OSI model. Layer 2 includes protocols that define the MAC address. The MAC address is burned into the network interface card, and a switch uses the MAC address to make forwarding decisions. A hub or a repeater operate at layer 1; they regenerate a signal without looking at layer 2 or layer 3 information. A router operates at layer 3, using the IP address to make forwarding decisions. A firewall operates at layer 3 or higher, using packet or data contents for making
filtering decisions.

An 8-port switch receives a frame on port number 1. The frame is addressed to an unknown device. What will the switch do?

Send the frame out the destination port.

Drop the frame.

Send the frame out ports 2-8.

Send the frame out all 8 ports.

Send the frame out ports 2-8.

Explanation

Because the switch does not know the port that is used to reach the destination device, it will send the frame out all ports except for the port on which the frame was received. After the switch learns the port that is used to reach the destination device, it will send the frame out
only that port.

Which of the following devices is used on a LAN and offers guaranteed bandwidth to each port?

Router

Bridge

Switch

Switch

Explanation

A switch offers guaranteed bandwidth to each port.

Which of the following is the best device to deploy to protect your private network from a public untrusted network?

Firewall

Gateway

Hub

Router

Firewall

Explanation

A firewall is the best device to deploy to protect your private network from a public untrusted network. Firewalls are used to control traffic entering and leaving your trusted network environment. Firewalls can manage traffic based on source or destination IP address, port
number, service protocol, application or service type, user account, and even traffic content. Routers offer some packet based access control, but not as extensive as that of a full-fledged firewall. Hubs and gateways are not sufficient for managing the interface between a trusted and an untrusted network.

You are the network administrator for a small organization. Recently, you contracted with an ISP to connect your organization's network to the Internet to provide users with Internet access. Since doing so, it has come to your attention that an intruder has invaded your network
from the Internet on three separate occasions. What type of network hardware should you implement to prevent this from happening again?

Proxy server

Switch

Hub

Firewall

CSU/DSU

Router

Firewall

Explanation

The role of a firewall is to provide a barrier between an organization's network and a public network, such as the Internet. Its job is to prevent unauthorized access into the organization's private network. To do this, the firewall examines incoming packets and determines whether they should be allowed to enter based on a set of rules defined by the network administrator.

At what OSI layer does a router operate to forward network messages?

Network

Session

Physical

Data Link

Transport

Network

Explanation

A router uses the logical network address specified at the Network layer to

forward messages to the appropriate LAN segment. A bridge, on the other hand, uses the MAC address and works at the Data Link layer.

Which of the following hardware devices links multiple networks and directs traffic between networks?

Repeater

Router

Bridge

Hub

Router

Explanation
A router is a device that links multiple networks and directs traffic between networks. Each network linked by routers has its own unique identifier called the " network number" or" network address."

At which of the following OSI layers does a router operate?

Layer 1

Layer 2

Layer 3

Layer 4

Layer 3

Explanation

A router operates at layer 3, or the Network layer.

You are the administrator of your company's network. You want to prevent unauthorized access to your intranet from the Internet. Which of the following should you implement?

Proxy server

Packet Internet Groper

ICS

Firewall

Firewall

Explanation

A firewall allows you to filter unwanted traffic from the Internet to your network. Packet Internet Groper is better known by its acronym, PING, a TCP/IP command. A proxy server caches web pages. ICS allows you to connect a small network to the Internet through a single connection.

Which two of the following tasks do routers perform?

Control access to the transmission media

Identify devices through hardware addresses

Maintain information about paths through an internetwork

Multiplex signals onto the same transmission media

Route data based on logical network addresses

Route data based on hardware device addresses

Maintain information about paths through an internetwork

Route data based on logical network addresses

Explanation

Routers build and maintain tables of routes through an internetwork, and deliver data between networks based on logical network addresses.

A network is connected following the IEEE 802. 3 specifications. Which of the following best describes when a device can transmit messages?

The device is notified of its turn to send messages.

The device requests permission from a controlling device.

The device with the token can use the transmission media.

The device transmits whenever it is ready.

The device listens to determine if the transmission media is free.

The device listens to determine if the transmission media is free.

Explanation

The IEEE 802. 3 committee describes the CSMA/CD media access method.

Devices listen to the network to determine if the transmission media is free before transmitting.

Which of the following connectors is used with Ethernet 10BaseT networks?

RJ11

RJ45

15-pin

D-shell

BNC

RJ45

Explanation

RJ45 connectors are used with Ethernet 10-BaseT networks.

The media access control method of all Ethernet networks is _____.

CSMA/CD

CSMA/CA

Polling

Token passing

CSMA/CD

Explanation

Carrier sense multiple access with collision detection (CSMA/CD) is the media access control method of all Ethernet networks.

Which of the following physical topologies are used with Ethernet networks? (Select two.)

Mesh

Star

Bus

Ring

Bus & Star

Explanation

Ethernet networks use either a physical bus or physical star topology. Hubs can also be cascaded to form a tree topology.

Which of the following use the CSMA/CD access method? Select all that apply.

Token Ring

1000BaseT

10BaseT

FDDI

1000BaseT

10BaseT

Explanation

CSMA/CD stands for Carrier Sense Multiple Access / Collision Detection. It defines the steps network devices take when two devices attempt to use a data channel simultaneously. Ethernet networks use CSMA/CD, including 10BaseT, 10Base2 and 1000BaseT.

You would like to implement 10 Gbps Ethernet over a distance of at least 10 kilometers. Which of the following would meet the requirement for this implementation? (Select three.)

10GBaseER standards

10GBaseLR standards

Multimode fiber

Single mode fiber

10GBaseSR standards

Single mode fiber

10GBaseER standards

10GBaseLR standards

Explanation

For 10 Gbps Ethernet at distances of 10 kilometers or more, use singlemode

fiber optic cable. 10GBaseLR (up to 10 km) and 10GBaseER (up to 40 km) both support 10 Gbps single mode fiber. Multimode fiber is cheaper but has a shorter maximum distance than single mode fiber.
10GBaseSR uses multimode fiber at distances up to 300 meters.

With an Ethernet 10BaseT network, the maximum cable length between a computer and the hub is:

100 meters

100 feet

500 feet

185 meters

100 meters

Explanation
With an Ethernet 10BaseT network, the maximum cable length between a computer and the
hub is 100 meters.

Which of the following Ethernet standards uses fiber optic cabling? (Select two.)

1000BaseCX

100BaseT4

100BaseFX

100BaseTX

1000BaseLX

100BaseFX

1000BaseLX

Explanation

100BaseFX and 1000BaseLX are Ethernet standards that use fiberoptic. Following the Ethernet naming conventions:

• F designates fiberoptic cables. Ethernet standards with the F designation are 10BaseFL and 100BaseFX.

• L designates " long" distances and requires fiberoptic to support the distance. Ethernet standards with the L designation are 10BaseFL, 1000BaseLX, and 10GBaseLR.

• S designates " short" distances that use fiberoptic cables. Ethernet standards with the S designation are 1000BaseSX and 10GBaseSR.

• T designates twisted pair cables. Ethernet standards with the T designation are 10BaseT, 100BaseTX, 100BaseT4, and 1000BaseT.

• C designates copper cables. The 1000BaseCX standard is for fast Ethernet at short distances within wiring closets.

You are planning a network for an educational campus. Due to the size of the buildings and the distance between them, you have elected to use 10BaseFL hubs, cabling, and network interface cards. What is the maximum length for the network cable between a workstation and a hub?

550 meters

1000 meters

220 meters

100 meters

412 meters

2000 meters

2000 meters

Explanation

The maximum length for a 10BaseFL network segment is 2000 meters (2 km). Because a 10baseFL network uses a physical star topology, a segment is defined as one of the arms of the star, (between the hub and a host). That means the fiberoptic cable between the hub and a workstation can be up to 2000 meters long. 100BaseFX supports up to 412 meters. 1000BaseSX and 1000BaseLX support up to 550 meters. 100 meters is the maximum twisted pair cable length.

Which of the following standards is used by SONET?

10GBaseER

1000BaseSX

1000BaseLX

1000BaseCX

10GBaseLW

10GBaseLW

Explanation

10GBase standards ending in W are used for SONET implementations. These include 10GBaseSW (short), 10GBaseLW (long), and 10GBaseEW (extended). 10GBaseER is for extended fiber optic but not used with SONET. 1000Base standards are not used for SONET. 1000BaseCX is a copper cable specification.

What type of cabling is used with 100BaseTX Fast Ethernet networks?

Type 1A STP or Category 5 UTP

Type 5 STP or Category 1 UTP

Category 3 UTP, Category 4 UTP, or Category 5 UTP

None of the above

Type 1A STP or Category 5 UTP

Explanation

Either Type 1A STP or category 5 UTP can be used with 100BaseTX Fast Ethernet networks.

Your network follows the 100BaseFX specifications for Fast Ethernet, and uses halfduplex cable. What is the maximum cable segment length allowed?

100 meters

412 meters

550 meters

1, 000 meters

2, 000 meters

412 meters

Explanation

For 100BaseFX, halfduplex, multimode cable has a maximum segment length of 412 meters. 1000BaseSX and 1000BaseLX support multimode cable up to 550 meters. 10BaseFL supports fiber optic cable between 1, 000 and 2, 000 meters.

You have been tasked with designing a highspeed Ethernet network. Your client's building already has 150ohm shielded twisted pair (STP) wiring installed. Due to budget constraints, they have asked you to reuse the existing wiring instead of installing new fiberoptic cabling. Which Ethernet standard could you implement in this situation?

1000BaseZX

10BaseFL

1000BaseLX

1000BaseCX

1000BaseT

1000BaseSX

1000BaseCX

Explanation

The 1000BaseCX standard specifies 150ohm STP cabling. The maximum cable length is 25 meters. The 10BaseFL, 1000BaseSX, 1000BaseLX, and 1000BaseZX standards employ fiberoptic cabling. 1000BaseT uses Category 5 UTP instead of STP cabling.

What topology is used with 100BaseTX Fast Ethernet networks? (Select two.)

Physical star/logical bus

Physical star/logical ring

Physical star/logical star

Physical ring/logical star

Physical star/logical bus

Physical star/logical star

Explanation

100BaseTX Fast Ethernet networks use a physical star/logical bus topology when a hub is used or a physical star/logical star when a switch is used.

You are working on upgrading the network in an older building. Over the years, the building has had several types of networking cable installed. The network must support 1000 Mbps Ethernet. You would like to minimize the cost of the upgrade by replacing cables only if

necessary. Which types of cable must be replaced to support the required network speed? (Select two.)

Cat 3

Cat 4

Cat 5

Cat 5e

Cat 6

Cat 6e

Cat 3 & Cat 4

Explanation
1000 Mbps Ethernet (Gigabit Ethernet) requires at least Cat 5 cables. While Cat 5 supports 1000 Mbps, it can have poor performance during high-data transfers. Whenever possible, it is best to use a higher grade cable (Cat 5e or Cat 6) if you want 1000 Mbps data transmission.
Cat 3 only supports 10 Mbps Ethernet. Cat 5e or Cat 6 is required for 10 Gbps Ethernet.

Ethernet 100BaseFX networks use what type of cabling?

Unshielded twisted pair

Fiber optic

Shielded twisted pair

Coaxial

Fiber optic

Explanation

Ethernet 100BaseFX networks use fiber optic cabling.

Which Gigabit Ethernet standard can support long network segments up to a maximum of 5 km when used with fiberoptic cable?

1000BaseSX

1000BaseLX

1000BaseT

1000BaseCX

1000BaseLX

Explanation

1000BaseLX supports segment lengths of up to 5 km when used with fiber-optic cable. This maximum segment length is cut to 550 m when fiber-optic cable is used and it operates in half-duplex. 1000BaseSX supports segment lengths of only 550 meters. 1000BaseCX uses copper wire and supports segment lengths of only 25 meters. 1000BaseT uses twisted pair cables.

Which Gigabit Ethernet standard uses fiberoptic cabling and supports network segments up to a maximum of 550 meters long?

1000BaseT

1000BaseZX

1000BaseCX

1000BaseSX

1000BaseSX

Explanation

The 1000BaseSX standard uses fiberoptic cable with a maximum segment length of 550 meters. However, to implement segments this long, you must use 50 micron, 500MHz/km fiber optic cable. Other types of cable will shorten the maximum segment length. 1000BaseFX also supports lengths up to 550 meters. 1000BaseFX supports distances up to 10 kilometers. 1000BaseZX has a maximum segment length of up to 100 km. 1000BaseCX and 1000BaseT use copper cabling instead of fiberoptic.

You want to implement an Ethernet network at very long distances using fiber optic cables. Which standard and cable type would you choose? (Select two.)

1000BaseLX

Single mode fiber

1000BaseCX

Mutimode fiber

1000BaseSX

1000BaseLX

Single mode fiber

Explanation

Of the standards listed in this question, 1000BaseLX provides the greatest cable length (think of the " L" in 1000BaseLX as " long"). When using long distances for fiber optic, use single mode fiber. Multimode fiber is cheaper but has a shorter maximum distance than single mode fiber. 1000BaseSX is for short fiber optic, and 1000BaseCX uses short copper within a wiring closet.

You have been tasked with designing an Ethernet network. Your client needs to implement a very highspeed network backbone between campus buildings; some of which are around 300 m apart. Fiberoptic cabling has already been installed between buildings. Your client has
asked that you use the existing cabling that operates in fullduplex. Which Ethernet standard meets these guidelines? (Choose two.)

1000BaseSX

1000BaseT

10GBaseSR

10BaseFL

1000BaseCX

1000BaseSX

10GBaseSR

Explanation

10GBaseSR and 1000BaseSX can operate within these parameters. Both will support segment lengths 300 meters long and operate using full-duplex. 10BaseFL isn't a good choice because its data transmission rate is relatively slow. 1000BaseCX and 1000BaseT both use copper wiring.

Which of the following are requirements of the 1000BaseT Ethernet standards? (Select three.)

SC or ST connectors

RJ45 connectors

Fiber optic cable

CAT 5 cabling

The cable length must be less than or equal to 100m

The cable length must be less than or equal to 1000m

RJ45 connectors

CAT 5 cabling

The cable length must be less than or equal to 100m

Explanation

Gigabit Ethernet (1000BaseT) has similar requirements to 100BaseT with connectors, cabling,

and distances. The network cards are simply designed to transfer data ten times as fast.

Your network follows the 100BaseTx specifications for Fast Ethernet. What is the maximum cable segment length allowed?

500 meters

1, 000 meters

412 meters

2, 000 meters

100 meters

100 meters

Explanation
Fast Ethernet using twisted pair cables (either 100BaseT4 or 100BaseTx) has a maximum cable segment length of 100 meters. Tip: All Ethernet networks that use twisted pair cable (Ethernet, Fast Ethernet, Gigabit Ethernet) have a distance limitation of 100 meters.

You have purchased a new router that you need to configure. You need to connect a workstation to the router's console port to complete the configuration tasks. Which type of cable would you most likely use?

RG6

Straight-through

Crossover

Rollover

Rollover

Explanation

Use a rollover cable to connect a workstation to the console port of a router or a switch. The rollover cable has an RJ45
connector on one end to connect to the console port, and a serial connector on the other end to connect to the serial port of the workstation. You then run a terminal emulation program on the workstation to connect to the console of the router or switch to perform configuration and management tasks. Use a straight-through or crossover Ethernet cable to connect devices using the Ethernet RJ45
ports. An RG6 cable is a coaxial cable.

You have two switches that you need to connect using their uplink ports. The switches do not support auto-MDI. Which type of cable should you use?

Straight-through

Loopback

Crossover

Rollover

Crossover

Explanation

Use a crossover cable to connect two switches through their uplink ports, or to connect the two switches through regular ports. Use a straight-through cable to connect the uplink port on one switch to a regular port on another switch. Use a rollover cable to connect a workstation to the console port of the switch. Use a loopback plug connected to a single port for troubleshooting.

You want to connect the LAN port on a router to the uplink port on a switch. The switch does not support auto-MDI. Which type of cable should you use?

Crossover

Rollover

Straight-through

Loopback

Crossover

Explanation

Use a crossover cable to connect a workstation or a router to the uplink port on a switch. Use a straight-through cable to connect the router to a regular switch port. Use a rollover cable to connect a workstation to the console port of a router. Use a loopback plug to allow a device
to communicate with itself through its own network adapter.

You need to transfer data from one laptop to another and would like to use an Ethernet cable. You do not have a hub or a switch.

Which type of cable should you use?

Loopback

Crossover

Straight-through

Rollover

Crossover

Explanation

Use a crossover cable to connect two devices together in a back-to-back configuration. Use a straight-through cable to connect a workstation to a hub or switch port. Use a rollover cable to connect a workstation to the console port of a router or a switch. Use a loopback plug to allow a device to communicate with itself through its own network adapter.

Which of the following standards is typically used in a rollover cable?

RS-232

RG-58

RG-6

R-J11

RS-232

Explanation

A rollover cable has a serial connector on one end and an RJ-45 connector on the other end. RS-232 is the standard for serial communications. RJ-11 connectors are used for analog telephone lines. RG-6 and RG-58 are coaxial cable standards.

You need to connect a workstation to a switch using a regular port on the switch (not an uplink port). The switch does not support auto-MDI. Which type of cable should you use?

Straight-through

Crossover

Loopback

Rollover

Straight-through

Explanation

Use a straight-through cable to connect a workstation or router to a regular switch port. Use a crossover cable to connect the workstation to the uplink port. Use a rollover cable to connect the workstation to the console port of the switch. Use a loopback plug to allow a workstation to communicate with itself through its own network adapter.

Which of the following connectors is typically used on one end of a rollover cable?

ST

BNC

F-type

Serial

LC

SC

Serial

Explanation

A rollover cable has a serial connector on one end and an RJ45 connector on the other end. Alternatively, it might have an RJ45 connector on both ends, and a serial converter is used to convert from the RJ45 connector to a serial connector. BNC and F-type connectors are used with coaxial cables. ST, SC, and LC connectors are used with fiber optic cables.

You want to create a rollover cable that has an RJ45 connector on both ends. How should you connect the wires within the connectors?

Connect pin 1 to pin 8, pin 2 to pin 7, pin 3 to pin 6, and pin 4 to pin 5.

Use the T568A standard on one end and the T568B standard on the other end.

Connect each pin on one end to the same pin on the other end (i. e. pin 1 with pin 1, pin 2 with pin 2, etc.).

Connect pin 1 with pin 3 and pin 2 to pin 6.

Connect pin 1 to pin 8, pin 2 to pin 7, pin 3 to pin 6, and pin 4 to pin 5.

Explanation

When terminated with an RJ45 connector on both ends, the wires within the connectors are rolled over to the opposite connector as follows:

• Pin 1 is connected to pin 8

• Pin 2 is connected to pin 7

• Pin 3 is connected to pin 6

• Pin 4 is connected to pin 5

A crossover cable uses the T568A standard on one end and the T568B standard on the other end. The crossover cable connects pin 1 with pin 3 and pin 2 to pin 6. Connecting each pin to the same pin on the other end creates a straight-through cable.

Which three of the following IP addresses are Class C addresses?

222. 55. 0. 0

240. 0. 0. 0

189. 189. 5. 2

192. 15. 5. 55

125. 166. 11. 0

223. 16. 5. 0

222. 55. 0. 0

192. 15. 5. 55

223. 16. 5. 0

Explanation

The following are Class C addresses: 192. 15. 5. 55, 222. 55. 0. 0, and 223. 16. 5. 0. The first octet of Class C addresses is in the range of 192 to 223.

In an IP addressing scheme using default subnet masks, which of the following IP addresses can you assign to a host?

127. 0. 0. 1

199. 45. 207. 0

127. 35. 88. 92

132. 70. 254. 15

132. 70. 254. 15

Explanation

Addresses starting with 127 are reserved and cannot be assigned to hosts. The address 199. 45. 207. 0 is a network ID, and is therefore not assigned to a host.

You manage a subnet that uses the following subnet address: 198. 162. 1. 0/23. Which of the following best describes how addressing is configured for the subnet?

Supernetting

Private

Subnetting

Classful

Supernetting

Explanation

The subnet address 198. 162. 1. 0/23 is an example of a supernetted address. With supernetting, multiple smaller subnets are combined into a single larger subnet. Supernetting is performed by taking the default subnet mask and making it smaller (using less bits). For this address, the default subnet mask uses 24 bits (255. 255. 255. 0). With supernetting, the mask is altered to use only 23 bits (255. 255. 254. 0) to combine multiple subnets together. Subnetting is the process of dividing a larger network into smaller networks. With the subnet address in this example, a subnetted address would use a larger subnet mask (using more bits). A subnetted address might use 25 bits (255. 255. 255. 128) or more to subdivide the network into multiple smaller subnets. Sometimes the term subnetting can be used to refer to both subnetting and supernetting, but in this example, supernetting better describes what is being done. Classful addressing uses the default subnet mask based on the address class. If classful addressing were used, the subnet would use a 24 bit mask. Private addresses are within the following ranges:

• 10. 0. 0. 1 to 10. 255. 255. 254

• 172. 16. 0. 1 to 172. 31. 255. 254

• 192. 168. 0. 1 to 192. 168. 255. 254

Consider the following IP addresses.

1. 124. 77. 8. 5

2. 131. 11. 0. 9

3. 190. 66. 250. 10

4. 196. 5. 89. 44

Which list represents the IP address class of each listed IP address?

Class A, Class B, Class B, Class C

Class B, Class B, Class C, Class D

Class B, Class B, Class C, Class C

Class A, Class B, Class C, Class C

Class A, Class B, Class C, Class C

Class B, Class C, Class C, Class D

Class A, Class B, Class B, Class C

Explanation

The IP addresses listed are of the following classes: Class A, Class B, Class B, Class C. You can identify the IP address class by memorizing the range of values for the first octet.

• 0-126 = Class A

• 128-191 = Class B

• 192-223 = Class C

• 223-239 = Class D

• 240-255 = Class E

Which of the following is the last IP address that can be assigned to hosts on the 166. 70. 0. 0 network using the default subnet mask?

166. 70. 0. 255

166. 70. 0. 254

166. 71. 0. 0

166. 70. 255. 255

166. 70. 255. 254

166. 70. 255. 254

Explanation

The last address you can assign to hosts on the 166. 70. 0. 0 network is 166. 70. 255. 254. The network address is a Class B address and uses a default subnet mask of 255. 255. 0. 0. The last two octets are used for host addresses. 166. 70. 0. 0 cannot be used as a host address because it is the network address. 166. 70. 255. 255 cannot be used as a host address because it is the broadcast address.

A host on the network has an IP address of 129. 11. 99. 78 using the default subnet mask. How would you identify the address and mask using CIDR notation?

129. 11. 99. 78/24

129. 11. 99. 78/16

129. 11. 99. 78/8

129. 11. 99. 78: 8

129. 11. 99. 78: 24

129. 11. 99. 78: 16

129. 11. 99. 78/16

Explanation

Use 129. 11. 99. 78/16 for the address and the mask. With CIDR notation, follow the IP address with a slash (/) and the number of bits in the mask. The default subnet mask for this address is 255. 255. 0. 0 which uses 16 bits in the mask. A mask value of 255. 0. 0. 0 uses 8 bits, and a mask value of 255. 255. 255. 0 uses 24 bits.

Your network has been assigned the Class C network address of 200. 78. 151. 0. Which three of the following addresses can be assigned to hosts on your network?

200. 78. 151. 0

200. 78. 151. 111

200. 78. 151. 257

200. 78. 151. 12

200. 78. 152. 14

200. 78. 151. 252

200. 78. 151. 255

200. 78. 151. 111

200. 78. 151. 12

200. 78. 151. 252

Explanation

All hosts on this network must share the first three octets of the IP address (200. 78. 151). Youcannot assign 200. 78. 151. 0 to a host because this address indicates the address of the network. You cannot assign 200. 78. 151. 255 because this address is reserved for the broadcast address.

Which of the following best describes the purpose of using subnets?

Subnets let you connect a private network to the Internet.

Subnets place each device within its own collision domain.

Subnets combine multiple IP network addresses into one network address.

Subnets divide an IP network address into multiple network addresses.

Subnets divide an IP network address into multiple network addresses.

Explanation

Subnets divide an IP network address into multiple network addresses. This allows you to have

several smaller networks while using only one network address.

Which three of the following are not valid IP addresses?

45. 22. 156. 256

116. 0. 0. 116

1. 55. 254. 3

132. 64. 32. 8

145. 8. 260. 7

257. 0. 122. 55

122. 0. 0. 0

145. 8. 260. 7

257. 0. 122. 55

Explanation

IP addresses have a value between 0 and 255 within each octet. In this list, 45. 22. 156. 256, 145. 8. 260. 7, and 257. 0. 122. 55 are not valid IP addresses.

What is the decimal format of the following binary IP address? 11001110. 00111010. 10101010. 01000011

238. 90. 202. 99

206. 58. 170. 67

190. 42. 154. 51

205. 57. 169. 66

206. 58. 170. 67

Explanation

206. 58. 170. 67 is the decimal form of the IP address. To convert binary to decimal, remember the following numbers: 128, 64, 32, 16, 8, 4, 2, 1
Each number represents the decimal value for a binary 1 in the corresponding position. For example, 10000000 is equal to 128, and 00010000 is equal to 16. To find the decimal form of a binary number, add up each decimal equivalent for each 1 bit in the address. For example, the number 11001110 would be: 128 + 64 + 8 + 4 + 2 = 206.

Which of the following is the last IP address that can be assigned to hosts on the 211. 70. 0. 0 network using the default subnet mask?

211. 70. 0. 255

211. 70. 255. 255

211. 70. 0. 254

211. 71. 0. 0

211. 70. 255. 254

211. 70. 0. 254

Explanation

The last address you can assign to hosts on the 211. 70. 0. 0 network is 211. 70. 0. 254. The network address is a Class C address and uses a default

subnet mask of 255. 255. 255. 0. The last octet is used for host addresses. 211. 70. 0. 0 cannot be used as a host address because it isthe network address. 211. 70. 0. 255 cannot be used as a host address because it is the broadcast address.

What is the default subnet mask for the IP address 203. 111. 3. 3?

255. 0. 0. 0

255. 255. 255. 255

255. 255. 0. 0

255. 255. 255. 0

255. 255. 255. 0

Explanation

IP addresses are divided into classes. The most common of these are classes A, B, and C. Each address class has a different default subnet mask. To identify the class of an IP address, look at its first octet.

• Class A networks use a default subnet mask of 255. 0. 0. 0 and have 0-126 as their first octet.

• Class B networks use a default subnet mask of 255. 255. 0. 0 and have 128-191 as their first octet.

• Class C networks use a default subnet mask of 255. 255. 255. 0 and have 192-223 as their first octet.

In this question, the IP address falls in the Class C range and therefore has a default subnet mask of 255. 255. 255. 0.

What is the binary format for the following decimal IP address?

131. 9. 202. 111

10000001. 00001010. 11000011. 01010111

10000110. 00001011. 11000101. 10101110

10000111. 00001101. 11001110. 01011101

10000011. 00001001. 11001010. 01101111

10000011. 00001001. 11001010. 01101111

Explanation

10000011. 00001001. 11001010. 01101111 is the binary format of the address. To convert binary to decimal, remember the following numbers: 128, 64, 32, 16, 8, 4, 2, 1 Each number represents the decimal value for a binary 1 in the corresponding position. For example, 10000000 is equal to 128, and 00010000 is equal to 16. To find the binary form of a decimal number, try to subtract each decimal value from the value
in the octet. For example, for 131, you can subtract 128 leaving a remainder of 3. You can then subtract 2 and then 1. For each number you can subtract, write a 1 in the binary position of the address.

A host has the address 100. 55. 177. 99/16. Which of the following is the broadcast address for the subnet?

255. 255. 255. 0

100. 255. 255. 255

100. 55. 255. 255

100. 55. 177. 255

255. 255. 0. 0

100. 55. 255. 255

Explanation

The broadcast address for the subnet is the last address on the subnet. In this example, the address uses 16 bits in the subnet mask (255. 255. 0. 0), meaning that the first two octets indicate the subnet address (100. 55. 0. 0), and the last two octets are used for host addresses.

The last possible address on this subnet is 100. 55. 255. 255.

Which of the following IP addresses have a default subnet mask of 255. 255. 0. 0? (Select all that apply.)

129. 0. 0. 1

123. 254. 19. 6

1. 6. 45. 254

168. 16. 5. 1

191. 168. 2. 15

228. 62. 18. 6

129. 0. 0. 1

168. 16. 5. 1

191. 168. 2. 15

Explanation

IP addresses are divided into classes. The most common of these are classes A, B, and C. Each address class has a different default subnet mask. To identify the class of an IP address, look at its first octet.

• Class A networks use a default subnet mask of 255. 0. 0. 0 and have 0-126 as their first octet.

• Class B networks use a default subnet mask of 255. 255. 0. 0 and have 128-191 as their first octet.

• Class C networks use a default subnet mask of 255. 255. 255. 0 and have 192-223 as their first octet.

In this question, the IP addresses that fall in the Class B IP address range are 191. 168. 2. 15, 129. 0. 0. 1, and 168. 16. 5. 1.

Which of the following is not a reason to use subnets on a network?

Combine different media type on to the same subnet.

Extend the network.

Improve security.

Isolate network problems.

Combine different media type on to the same subnet.

Explanation

Subnets cannot be used to combine networks of different media type on to the same subnet. Each network with a distinct media type has its own subnet. Subnets can be used to combine networks with different media types within the same internetwork.

Which of the following is the first IP address that can be assigned to hosts on the 166. 70. 0. 0 network using the default subnet mask?

166. 71. 0. 0

166. 70. 1. 0

166. 70. 0. 0

166. 70. 1. 1

166. 70. 0. 1

166. 70. 0. 1

Explanation

The first address you can assign to hosts on the 166. 70. 0. 0 network is 166. 70. 0. 1. The network address is a Class B address and uses a default subnet mask of 255. 255. 0. 0. The last two octets are used for host addresses. The host address range is 166. 70. 0. 1 to 166. 70. 255. 254.

166. 70. 0. 0 cannot be used as a host address because it is the network address. 166. 70. 255. 255 cannot be used as a host address because it is the broadcast address.

You have been told to assign the IP address 21. 155. 67. 188 to a host on the network using the default subnet mask. Which mask should you use?

21. 155. 0. 0

255. 255. 0. 0

21. 155. 67. 0

255. 0. 0. 0

255. 255. 255. 0

21. 0. 0. 0

255. 0. 0. 0

Explanation

The default subnet mask for this address is 255. 0. 0. 0. The address is a class A address, which begins with a number between 1 and 126 in the first octet. 21. 0. 0. 0 is the subnet address. 255. 255. 0. 0 is the default subnet mask for a class B address, and 255. 255. 255. 0 is the default subnet mask for a class C address.

Which of the following is a valid IP (version 4) address? (Select two.)

172. 16. 1. 26

192. 168. 1. 512

1. 254. 1. 1024

254. 7. 1. 417

10. 384. 0. 3

256. 0. 0. 1

2. 2. 2. 2

172. 16. 1. 26

2. 2. 2. 2

Explanation

A valid IPv4 address consists of 4 8bit (1 byte) numbers separated by periods. For example, 10. 0. 0. 65. Because they are 8 bits long, these numbers are frequently called octets. Even though we typically express these numbers using decimal notation, it's important to remember that these numbers are binary numbers. The lowest value one of these numbers can have is 00000000. The decimal equivalent for this number is simply 0. The highest value one these numbers can take is 11111111. The decimal equivalent of this number is 255. Therefore, in decimal notation, each octet must contain a number between 0 and 255inclusively.

Which three of the following IP addresses are Class B addresses?

132. 12. 0. 0

224. 15. 55. 2

64. 2. 2. 64

129. 0. 0. 0

115. 33. 0. 0

195. 155. 0. 0

190. 65. 2. 0

132. 12. 0. 0

129. 0. 0. 0

190. 65. 2. 0

Explanation

The following are Class B addresses: 129. 0. 0. 0, 132. 12. 0. 0, and 190. 65. 2. 0. The first octet of Class B addresses is in the range of 128 to 191.

Your network has been assigned the Class B address of 130. 15. 0. 0. Which of the following is not an address you can assign to a node on your network?

130. 15. 60. 0

130. 16. 61. 3

130. 15. 60. 220

130. 15. 0. 1

130. 16. 61. 3

Explanation

If you plan to use the Class B address for all nodes on the network, the nodes must all have

the same network address. In this case, all IP addresses must begin with 130. 15.

You are configuring the IP address for a host and have been asked to use the address 192. 160. 99. 110/16. What subnet mask value would you use?

255. 0. 0. 0

255. 255. 0. 0

255. 255. 252. 0

255. 255. 255. 0

255. 255. 0. 0

Explanation
With CIDR notation, the number of bits in the subnet mask is indicated by the /16 following the IP address. A mask that uses 16 bits is written 255. 255. 0. 0 in decimal format. Each octet in the mask uses 8 bits, so a mask with 16 bits uses two full octets. Use /8 for the mask 255. 0. 0. 0 and /24 for the mask 255. 255. 255. 0. In this example, a /24 mask would be the default subnet mask, but the address is using a nondefault
mask of 255. 255. 0. 0.

Your network has been assigned the Class B network address of 179. 113. 0. 0. Which three of the following addresses can be assigned to hosts on your network?

179. 113. 89. 0

179. 113. 0. 0

180. 113. 0. 67

179. 114. 88. 0

179. 113. 0. 118

179. 112. 95. 64

179. 113. 65. 12

179. 113. 89. 0

179. 113. 0. 118

179. 113. 65. 12

Explanation

All hosts on this network must share the first two octets of the IP address (179. 113). You cannot assign 179. 113. 0. 0 to a host because this address indicates the address of the network.

Which three of the following IP addresses belong to the Class A network 114. 0. 0. 0? (Assume the network is indicated by the default portion of the IP address.)

114. 58. 12. 0

114. 122. 66. 12

114. 0. 0. 15

115. 77. 89. 4

115. 88. 0. 55

115. 0. 0. 66

114. 58. 12. 0

114. 122. 66. 12

114. 0. 0. 15

Explanation

With a Class A network, the first octet indicates the network address. All hosts on the network must have the same value in the first octet (114).

Which of the following IP address ranges is reserved for Automatic Private IP Addressing?

192. 168. 0. 1 192. 168. 254. 255

169. 254. 0. 1 169. 254. 255. 254

169. 192. 0. 0 169. 192. 254. 255

192. 168. 0. 0 192. 168. 255. 254

169. 168. 0. 1 169. 168. 255. 255

169. 254. 0. 1 169. 254. 255. 254

Explanation

The Internet Assigned Numbers Authority (IANA) has reserved 169. 254. 0. 1 through 169. 254. 255. 254 for Automatic Private IP Addressing (APIPA). APIPA also sets the subnet mask on the network to 255. 255. 0. 0.

What is the network address and subnet mask used by APIPA? (Select two.)

255. 0. 0. 0

255. 255. 255. 0

169. 0. 250. 0

255. 255. 0. 0

169. 254. 0. 0

169. 255. 0. 0

255. 255. 0. 0
169. 254. 0. 0

Explanation
Automatic Private IP Addressing (APIPA) uses a network address of 169. 254. 0. 0 with the default Class B subnet mask of 255. 255. 0. 0. Host addresses will be within the range of169. 254. 0. 1 and 169. 254. 255. 254.

You have a TCP/IP network with 50 hosts. There have been inconsistent communication problems between hosts. You run a protocol analyzer and discover that two hosts have the same IP address assigned. Which protocol can you implement on your network to help prevent problems such as this?

IP

TCP

ICMP

DHCP

SNMP

IGMP

DHCP

Explanation

You can use the Dynamic Host Configuration Protocol (DHCP) to set up a DHCP server that will assign IP addresses automatically to network hosts. DHCP servers will not assign the same IP address to two different hosts.

You have a network with 50 workstations. You want to automatically configure workstations with the IP address, subnet mask, and default gateway values. Which device should you use?

DNS server

Gateway

Router

DHCP server

DHCP server

Explanation

Use a DHCP server to deliver configuration information to hosts automatically. Using DHCP is easier than configuring each host manually. Use a gateway to provide access to a different network, or to a network

using a different protocol. Use a router to connect multiple subnets. Use a DNS server to provide name resolution, for example to get the IP address associated with a logical host name.

Which of the following strategies are used to prevent duplicate IP addresses being used on a network? (Select two.)

Install the DHCP client on all workstations

Set the Windows networkmonitoring

utility to identify potential IP conflicts

Configure a HOSTS file for local IP resolution

Use Automatic Private IP Addressing

Install a DHCP server on the network

Configure client systems to use static IP assignment

Use Automatic Private IP Addressing
Install a DHCP server on the network

Explanation
To avoid duplicate IP addresses being used by network systems, automatic IP assignment is used. Both the DHCP service and APIPA can automatically assign addresses to client systems. Clients configured to use static IP addressing may inadvertently have duplicate IP addresses
assigned to them. In such a case, one of the systems will not be able to log on to the network.

Which two of the following statements about the Dynamic Host Configuration Protocol (DHCP) are true?

It can deliver other configuration information in addition to IP addresses.

It cannot be configured to assign the same IP address to the same host each time it boots.

A DHCP server assigns addresses to requesting hosts.

It is used only to deliver IP addresses to hosts.

A DHCP server assigns addresses to requesting hosts.
It can deliver other configuration information in addition to IP addresses.

Explanation
DHCP servers deliver IP addresses as well as other host configuration information to network hosts. DHCP can be configured to assign any available address to a host, or it can assign a specific address to a specific host.

You want to implement a protocol on your network that allows computers to find the IP address of a host from a logical name. Which protocol should you implement?

Telnet

ARP

DHCP

DNS

DNS

Explanation

DNS is a system that is distributed throughout the internetwork to provide address/name resolution. For example, the name www. mydomain. com would be identified with a specific IP address. ARP is a protocol for finding the IP address from a known MAC address. DHCP is a protocol used to assign IP addresses to hosts. Telnet is a remote management utility.

You need to enable hosts on your network to find the IP address of logical names such as srv1. myserver. com. Which device would you use?

IPS

DNS server

Bandwidth shaper

IDS

Load balancer

DNS server

Explanation

Use a DNS server to provide hostname-to-IP address resolution. A bandwidth shaper modifies the flow of traffic to keep traffic within predefined limits. A load balancer accepts incoming client requests, and distributes those

requests to multiple other servers. An IDS detects security threats, while an IPS can both detect and respond to security threats.

A router is connected to network 192. 168. 1. 0/24 and network 192. 168. 2. 0/24. The router is configured to use RIP and has learned of networks 192. 168. 3. 0/24 and 192. 168. 4. 0/24. The next hop router for network 192. 168. 3. 0 has changed. You need to make the change with the least amount of effort possible. What should you do?

Manually reconfigure the default route to point to the new next hop router.

Stop and restart the RIP protocol on the router.

Wait for convergence to take place.

Force RIP to perform an immediate update.

Wait for convergence to take place.

Explanation
When using a routing protocol, changes in routing information take some time to be propagated to all routers on the network. The term convergence is used to describe the condition when all routers have the same (or correct) routing information. Static routes in the routing table must be updated manually. Restarting RIP might actually increase the time required for changes to be learned. Forcing an update (if the router supports it) is not a requirement as the periodic sharing of routes will eventually update the routing table
entry.

Which of the following statements about RIP is true?

RIP uses hop counts as the cost metric.

RIP is the routing protocol used on the Internet.

RIP is suitable for large networks.

RIP is a link state routing protocol.

RIP uses hop counts as the cost metric.

Explanation

RIP is a distance vector routing protocol. As such, it is susceptible to the count-to-infinity problem. RIP uses the hop count as the cost metric. Because it has a limitation of 15 hops in one route, it is not suited for large networks.

Which of the following routing protocols is classified as a balanced hybrid routing protocol?

EIGRP

OSPF

ISIS

RIP

EIGRP

Explanation

EIGRP is a hybrid routing protocol developed by Cisco for routing within an

AS. RIP is a distance vector protocol, while OSPF and ISIS are link state protocols.

You have a router configured to share routing information using RIP. In addition, you have a single static route that identifies a default route for all other networks. The next hop router for the default route has changed. You need to make the change with the least amount of effort possible. What should you do?

Manually reconfigure the default route to point to the new next hop router.

Stop and restart the RIP protocol on the router.

Force RIP to perform an immediate update.

Wait for network convergence to take place.

Manually reconfigure the default route to point to the new next hop router.

Explanation
With a static route, when changes to the network occur, routing table entries must be modified, added, or removed manually. In this example, the default route was configured manually, so must be manually updated. When using a routing protocol, routing changes are made automatically by routers sharing routing information. To make a change for a dynamic route, simply wait for convergence to occur (the term convergence describes the condition when all routers have the same routing information).

Which of the following is a characteristic of static routing when compared to dynamic routing?

All routes must be manually updated on the router.

Routers use the hop count to identify the distance to a destination network.

Routers can only use static routing when not connected to the Internet.

Routers send packets for destination networks to the next hop router.

All routes must be manually updated on the router.

Explanation

Static routing requires that entries in the routing table are configured manually. Network entries remain in the routing table until manually removed. When changes to the network occur, static entries must be added or removed. The next hop router is used with most routes to identify the next router in the path to the destination, regardless of whether the route is a static or dynamically-learned route. The hop count can be used by static or dynamic routes, depending on the routing protocol used. Static routing can be used for private and public networks, whether connected to the Internet or not.

You manage a server that uses an IP address of 192. 168. 255. 188 with a mask of 255. 255. 0. 0. Which of the following describes the address type?

Classless

Classful

Multicast

Public

Broadcast

Classless

Explanation

Because the IP address is not using the default subnet mask, it is using classless addressing. Classless addressing modifies the length of the subnet mask, using a custom mask value instead of the default subnet mask. Classful addressing uses the default subnet mask. Devices that only support classful addressing assume the subnet mask based on the IP address class. A broadcast address is an address that is sent to all hosts. Broadcast addresses are the last possible address on a subnet. A multicast address is an address that identifies a group of computers. Members of the group share the same multicast address. Multicast addresses are in the range of 224. 0. 0. 0 to 239. 255. 255. 255. A public address is an address that is registered for use on the Internet.

What are the main differences between the OSPF and ISIS routing protocols?

OSPF is a link state protocol, while ISIS is not.

OSPF is a classful protocol, while ISIS is a classless protocol.

OSPF requires an area 0, while ISIS does not.

OSPF is an IGP routing protocol, while ISIS is a BGP routing protocol.

OSPF requires an area 0, while ISIS does not.

Explanation

Like OSPF, ISIS uses areas when designing the network. However, ISIS does not require an

area 0 like OSPF does. Because ISIS was originally designed for non-IP protocols, it can more easily support IPv6 routing.

Both OSPF and ISIS have the following characteristics:

• Both are link state protocols.

• Both are classless protocols, supporting CIDR and VLSM.

• Both are Interior Gateway Protocols (IGPs) that are used within an AS.

Which of the following terms are often synonymous with or made possible with CIDR? (Select two.)

NAT

Classless

VLSM

OSPF

Classful

Classless

VLSM

Explanation

Classless InterDomain Routing (CIDR) allows for non-default subnet masks (variable length subnet mask or VLSM). Routers use the following information

to identify networks:

• The beginning network address in the range

• The number of bits used in the subnet mask

For example, the subnet 199. 70. 0. 0 with a mask of 255. 255. 0. 0 is represented as 199. 70. 0. 0/16 (with 16 being the number of 1 bits in the subnet mask). Classful addresses rely on the IP address class to identify the subnet mask. Network Address Translation (NAT) allows you to connect a private network to the Internet without obtaining registered addresses for every host. Private addresses are translated to the public address of the NAT router. OSPF is a routing protocol that supports CIDR features.

You have a network configured to use the OSPF routing protocol. Which of the following describes the state when all OSPF routers have learned about all other routes in the network?

Link state

Convergence

Classful

VLSM

Distance vector

Convergence

Explanation

The term convergence is used to describe the condition when all routers have the same (or correct) routing information. Convergence requires some

time, but once reached means that any router has learned about all other networks that are being advertised (or shared) on the
network. Link state and distance vector describe general methods that routers use to share routes with other routers. Classful describes a routing protocol that assumes the subnet mask based on the address class of the network. Variable

Which of the following best describes OSPF?

OSPF is a classful link-state routing protocol.

OSPF is a classless distance vector routing protocol.

OSPF is a classless link-state routing protocol.

OSPF is a classful distance vector routing protocol.

OSPF is a classless link-state routing protocol.

Explanation
OSPF is a classless link-state routing protocol. RIP version 1 and IGRP are both classful distance vector routing protocols. EIGRP is a hybrid protocol that supports classless addressing.

Which of the following protocols has a limit of 15 hops between any two networks?

BGP

EIGRP

OSPF

RIP

ISIS

RIP

Explanation

RIP networks are limited in size to a maximum of 15 hops between any two networks. A network with a hop count of 16 indicates an unreachable network. The other routing protocols do not use the hop count as the metric. EIGRP uses bandwidth and delay for the metric. OSPF and ISIS use a relative link cost. BGP uses paths, rules, and polocies for the metric.

What information does the next hop entry in a routing table identify?

The first router in the path to the destination network.

The number of routers that the packet must go through to reach the destination network.

The last router in the path to the destination network.

A backup router that is used for forwarding packets addressed to unknown networks.

The first router in the path to the destination network.

Explanation

The next hop router is the first (or next) router in the path to the destination

network. Each router looks at the destination network in the packet, then consults the routing table to identify the next hop router to the destination network. The hop count identifies the number of routers in the path to the destination network. A default gateway router is a router that is used for packets used to external networks. Most routers do not have a default gateway setting, but instead use a default route setting which identifies a next hop router for all unknown networks.

Which of the following routing protocols divides the network into areas, with all networks required to have an area 0 (area 0 identifying the backbone area)?

RIP

EIGRP

ISIS

OSPF

OSPF

Explanation
OSPF divides a large network into areas. Each autonomous system requires an area 0 that identifies the network backbone. All areas are connected to area 0, either directly or indirectly through another area. Routes between areas must pass through area 0. ISIS uses areas but does not have an area 0 requirement. Neither RIP nor EIGRP use areas.

Under which of the following circumstances might you implement BGP on your company network and share routes with Internet routers?

If the network is connected to the Internet using multiple ISPs.

If the network has over 15 areas and uses IPv6.

If the network is connected to the Internet using public addressing.

If the network has over 15 hops.

If the network is connected to the Internet using multiple ISPs.

Explanation
Very large networks can use BGP internally, but typically only share routes on the Internet if the AS has two (or more) connections to the Internet through different ISPs. If your network has over 15 hops, use a routing protocol other than RIP. Use OSPF or ISIS to divide your network into areas. Private networks that use public IP addresses do not need to share routes with Internet routers; it is typically the responsibility of the ISP to configure routes into the private network, even when public addressing is being used. A single route out of the private network is all that is required if the network has a single connection to the Internet.

A router is connected to network 192. 168. 1. 0/24 and network 192. 168. 2. 0/24. The router is configured to use RIP and has learned of networks 192. 168. 3. 0/24 and 192. 168. 4. 0/24. There is no default route configured on the router. The router receives a packet addressed to network 10. 1. 0. 0/16. What will the router do with the packet?

Drop the packet.

Send the packet to both networks 192. 168. 3. 0 and 192. 168. 4. 0 to the next hop router.

Hold the packet in cache until a matching route is learned or configured.

Send the packet out both of its directly connected networks as a broadcast frame.

Drop the packet.

Explanation
If a packet does not match any route in a routing table, the router will simply drop the packet. In this example, the router does not know about the destination network, and also is not configured with a default route. With a default route, the router will forward the packet to the
next hop router specified by the default route.

A router is connected to network 192. 168. 1. 0/24 and network 192. 168. 2. 0/24. The router is configured to use RIP and has learned of networks 192. 168. 3. 0/24 and 192. 168. 4. 0/24. The router is also configured with a static route of 0. 0. 0. 0 with a mask of 0. 0. 0. 0. The router receives a packet addressed to network 10. 1. 0. 0/16. What will the router do with the packet?

Send the packet out both of its directly connected networks to the next hop router.

Send the packet out both of its directly connected networks as a broadcast frame.

Forward the packet to the next hop router specified by the route to network 0. 0. 0. 0.

Drop the packet.

Forward the packet to the next hop router specified by the route to network 0. 0. 0. 0.

Explanation

A route of 0. 0. 0. 0 with a mask of 0. 0. 0. 0 identifies a default route. The default route is used

when no other route is a better match. Packets that match no other networks are sent to the

next hop router specified by default route.

What is the main difference between RIP and RIPv2?

RIP has a limit of 15 hops, while RIPv2 increases the hop count limit.

RIP is a distance vector protocol, while RIPv2 is a link state protocol.

RIP is a classful protocol, while RIPv2 is a classless protocol.

RIP use the hop count for the metric, while RIPv2 uses a relative link cost.

RIP is a classful protocol, while RIPv2 is a classless protocol.

Explanation

RIP v1 is a classful protocol, meaning that the subnet mask is not included in routing updates. With RIP, only the default subnet mask is used to identify networks. RIP v2 is a classless protocol, meaning that the subnet mask is

included in routing updates. RIPv2 supports variable
length subnet masks (VLSM). Both RIP and RIPv1 are distance vector protocols and use the hop count for the metric. RIP and RIPv2 have a limit of 15 hops between any two networks.

Which of the following routing protocols is used by routers on the Internet for learning and sharing routes?

EIGRP

BGP

RIP

ISIS

OSPF

BGP

Explanation
BGP is the protocol used on the Internet: ISPs use BGP to identify routes between ASs. Very large networks can use BGP internally, but typically only share routes on the Internet if the AS has two (or more) connections to the Internet through different ISPs. RIP is used on small private networks, while OSPF and EIGRP are used on larger private networks. ISIS is used on very large private networks and within the Internet Service Provider (ISP) network.

Which of the following routing protocols are classified as link state routing protocols? (Select two.)

EIGRP

OSPF

RIP

ISIS

RIPv2

OSPF & IS-IS

Explanation

Both OSPF and ISIS are link state protocols. Using the link state method, routers share only their directly connected routes using special packets called link-state advertisements (LSAs) and link-state packets (LSPs). These route advertisements are flooded (forwarded) throughout the network. Routers use this information to build a topology database of the network. RIP and RIPv2 are classified as distance vector protocols. Using the distance vector method, routers share their entire routing table with their immediate neighbors. Routes learned from
neighboring routers are added to the routing table, then shared with that router's neighbors. EIGRP is a balanced hybrid protocol. A hybrid method combines characteristics of both the distance vector and link state methods. It shares its full routing table at startup, followed by
partial updates when changes occur.

You have a private network connected to the Internet. Your routers will not share routing information about your private network with Internet routers.

Which of the following best describes the type of routing protocol you would use?

Static

Link state

IGP

Dynamic

Distance vector

BGP

IGP

Explanation

You would use an Interior Gateway Protocol (IGP) on routers within your network. Routing protocols can be classified based on whether they are routing traffic within or between autonomous systems: An Interior Gateway Protocol (IGP) routes traffic within an AS; an Exterior Gateway Protocol (EGP) routes traffic between ASs. Link state and distance vector describe how routing protocols share routing information. The network size might determine which protocol is best for your network. Static routing uses manually defined routes in the routing table, while dynamic routing uses a protocol so routers learn and share routes with other routers. You can use either static or dynamic routing (or both) on a private network.

Which of the following is not one of the ranges of IP addresses defined in RFC 1918 that are commonly used behind a NAT server?

192. 168. 0. 1 192. 168. 255. 254

172. 16. 0. 1 172. 31. 255. 254

10. 0. 0. 1 10. 255. 255. 254

169. 254. 0. 1 169. 254. 255. 254

169. 254. 0. 1 169. 254. 255. 254

Explanation

169. 254. 0. 1 169. 254. 255. 254 is the range of IP addresses assigned to Windows DHCP clients if a DHCP server does not assign the client an IP address. This range is known as the Automatic Private IP Addressing (APIPA) range. The other three ranges listed in this question are defined as the private IP addresses from RFC 1918 which are commonly used behind a NAT server.

Which organization is responsible for allocating public IP addresses?

IANA

CompTIA

IEEE

IETF

IANA

Explanation

The Internet Assigned Numbers Authority (IANA) is responsible for allocating IP addresses used on the Internet. When you want to obtain a public IP address, you would typically get the address from your ISP, which has received it from a Regional Internet Registry (RIR), which has been assigned a block of addresses from IANA. IANA is operated by the Internet Corporation for Assigned Names and Numbers (ICANN), so you might also see that ICANN is responsible for assigning public IP addresses. The IETF is an organization that is responsible for settings standards used on the Internet. For example, the IETF has defined the standards for NAT as well as other protocols. The IEEE is an organization that sets networking standards such as for Ethernet or wireless networking. CompTIA is a professional organization that represents computing technology companies and individuals.

You have a small network at home that is connected to the Internet. On your home network you have a server with the IP address of 192. 168. 55. 199/16. All computers on your home network can connect to the Internet. From your work office, you try to access your home computer using its IP address, but are unable to communicate with the server. You are able to connect to other hosts on the Internet.

Why can't you access the server?

Private addresses are not accessible through the Internet.

The server has been assigned a multicast address.

The server must have an entry on a DNS server that exists on the Internet.

The server isn't using the default subnet mask.

Private addresses are not accessible through the Internet.

Explanation

The server has been assigned a private IP address. Private addresses are not accessible from the Internet. Instead, a NAT router translates the private address into a public address, and the public address is used to gain access to the private host.

Your computer has an IP address of 161. 13. 5. 15. Your computer is on a:

Public network

Class C network

Private network

Multicast network

Public network

Explanation

Most IP addresses are public IP addresses. However certain ranges have been reserved for private networks. These 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

Because your computer's IP address does not fall into these ranges, it is a public IP address.

Which of the following associates a port number with a host on a private network?

NAT

CIDR

PAT

VLSM

PAT

Explanation

Port address translation (PAT) associates a port number with the translated address. Use PAT to allow multiple private hosts to share a single public address. Each private host is associated with a unique port number. Technically speaking, NAT translates one address to another. With only NAT, you would have to have a public address for each private host. NAT would associate a single public address with a single private address. Because virtually all NAT routers perform port address translation, most routers that are configured with NAT are really performing PAT. When you use a NAT router, you are normally using PAT and not just NAT. (NAT is typically used synonymously with PAT.) Classless InterDomain Routing (CIDR) allows for non-default subnet masks (variable length subnet mask or VLSM).

You have a computer that is connected to the Internet through a NAT router. You want to use a private addressing scheme for your computer. Which of

the following IP addresses could you assign to the computer? (Select all that apply.)

172. 18. 188. 67

192. 168. 12. 253

10. 0. 12. 15

32. 188. 99. 10

224. 15. 166. 12

240. 12. 188. 1

127. 0. 0. 1

172. 18. 188. 67

192. 168. 12. 253

10. 0. 12. 15

Explanation

Of the addresses listed here, the following are in the private IP address ranges:

• 10. 0. 12. 15 (private range = 10. 0. 0. 0 to 10. 255. 255. 255)

• 172. 18. 188. 67 (private range = 172. 16. 0. 0 to 172. 31. 255. 255)

• 192. 168. 12. 253 (private range = 192. 168. 0. 0 to 192. 168. 255. 255)

Which of the following IP addresses is a valid IP address for a host on a public network?

192. 168. 16. 45

10. 3. 125. 2

142. 15. 6. 1

172. 16. 254. 12

142. 15. 6. 1

Explanation

A public network is a network that does not limit traffic to members of a corporation or other group. The Internet is an example of a public network. Certain sets of IP addresses are reserved for private networks only and cannot be used on public networks. They are:

• 10. 0. 0. 0 to 10. 255. 255. 255

• 172. 16. 0. 0 to 172. 31. 255. 255

• 192. 168. 0. 0 to 192. 168. 255. 255

You have a small network at home that is connected to the Internet. On your home network you have a server with the IP address of 192. 168. 55. 199/16. You have a single public address that is shared by all hosts on your private network. You want to configure the server as a Web server and allow Internet hosts to contact the server to browse a personal Web site. What should you use to allow access?

DNS A record

Static NAT

DNS CNAME record

Multicast

Dynamic NAT

Static NAT

Explanation

Static NAT maps an internal IP address to a static port assignment. Static NAT is typically used to take a server on the private network (such as a Web server) and make it available on the Internet. External hosts contact the internal server using the public IP address and the static port. Using a static mapping allows external hosts to contact internal hosts. Dynamic NAT automatically maps internal IP addresses with a dynamic port assignment. On the NAT device, the internal device is identified by the public IP address and the dynamic port number. Dynamic NAT allows internal (private) hosts to contact external (public) hosts but not vice versa. External hosts cannot initiate communications with internal hosts. DNS records associate a host name with an IP address. With multicast, a single data stream can be forwarded to all computers that are members of the same multicast group.

Which of the following are valid IPv6 IP addresses? Select all that apply.

343F: 1EEE: ACDD: 2034: 1FF3: 5012

165. 15. 78. 53. 100. 1

127. 0. 0. 1

141: 0: 0: 0: 15: 0: 0: 1

192. 168. 2. 15

6384: 1319: 7700: 7631: 446A: 5511: 8940: 2552

141: 0: 0: 0: 15: 0: 0: 1

6384: 1319: 7700: 7631: 446A: 5511: 8940: 2552

Explanation

An IPv6 IP address is a 128-bit address listed as eight 16-bit hexadecimal sections. Leading zeros can be omitted in each section. Therefore, 6384: 1319: 7700: 7631: 446A: 5511: 8940: 2552 and 141: 0: 0: 0: 15: 0: 0: 1 are both valid IPv6 IP addresses. A single set of all zero sections can be abbreviated with two colons (::). Therefore, 141:: 15: 0: 0: 1 would also be a valid address.

Which of the following is a valid IPv6 address?

FEC0:: AB: 9007

FEC0: 9087: AB04: 9900: 7GA2: 7788: CEDF: 349A

199. 12. 254. 11

FEC0: AB98:: A7:: 9845: 4567

FEC0: AB04: 899A

FEC0:: AB: 9007

Explanation

FEC0:: AB: 9007 is a valid IPv6 address. The :: in the address replaces blocks of consecutive 0's. The longer form of this address would be FEC0: 0000: 0000: 0000: 0000: 0000: 00AB: 9007. Leading 0's within a quartet can also be omitted. You can only omit one block of 0's using the double colon. Each number in the IPv6 address must be between 0-9 or A-F; G is not a valid number for the IPv6 address. An address without double colons should have a total of 32 hexadecimal numbers in 8 blocks.

Which of the following address types is shared by multiple hosts, and is used to form groups of computers that should receive the same data stream?

Simplex

Half-duplex

Multicast

Unicast

Broadcast

Multicast

Explanation

A multicast address is an address that identifies a group of computers. Members of the group share the same multicast address. A unicast address is an address that identifies a single host. A broadcast address is an address that is sent to all hosts. Broadcast traffic is typically only forwarded within (but not between) a subnet. Simplex communication uses a single channel

for both sending and receiving. Half-duplex uses a separate channel for sending and receiving, but the channels are shared by multiple devices and can only be used by a single device at a time.

Which type of address is the IP address 232. 111. 255. 250?

Multicast

Unicast

Private

Broadcast

Multicast

Explanation
The address 232. 111. 255. 250 is a multicast address. A multicast address is an address that identifies a group of computers. Members of the group share the same multicast address. Multicast addresses are in the range of 224. 0. 0. 0 to 239. 255. 255. 255. A unicast address is an address that identifies a single host. A broadcast address is an address that is sent to all hosts. Broadcast addresses are the last possible address on a subnet (typically ending in 255). The private IPv4 address ranges are:

• 10. 0. 0. 1 to 10. 255. 255. 254

• 172. 16. 0. 1 to 172. 31. 255. 254

• 192. 168. 0. 1 to 192. 168. 255. 254

Which type of address is used in a packet to address the packet to a single host?

Multicast

Fullduplex

Unicast

Simplex

Broadcast

Unicast

Explanation

A unicast address is an address that identifies a single host. A broadcast address is an address that is sent to all hosts. Broadcast traffic is typically only forwarded within (but not between) a subnet. A multicast address is an address that identifies a group of computers. Members of the group share the same multicast address. Simplex communication uses a single channel for both sending and receiving. Full-duplex has a dedicated send and receive channel between any two hosts.

Which protocol does an IP host use to inform a router that it wants to receive specific multicast frames?

SNMP

IP

IGMP

ICMP

MGP

IGMP

Explanation

IP hosts use the IGMP or Internet Group Management Protocol to inform multicast-enabled routers that they want to receive specific multicast frames.

Which type of address is the IP address 198. 162. 12. 254/24?

Unicast

Private

Multicast

Broadcast

Unicast

Explanation

The address 198. 162. 12. 254 is a unicast address that identifies a single host on the 198. 162. 12. 0 subnet. 198. 162. 12. 255 is the broadcast address for the subnet. Multicast addresses are in the range of 224. 0. 0. 0 to 239. 255. 255. 255.

The private IPv4 address ranges are:

• 10. 0. 0. 1 to 10. 255. 255. 254

• 172. 16. 0. 1 to 172. 31. 255. 254

• 192. 168. 0. 1 to 192. 168. 255. 254

Which of the following features is used with digital IP phones to supply power through a switch port?

VPN

Spanning tree

PoE

802. 1x

Trunking

PoE

Explanation

Power over Ethernet (PoE) supplies power to end devices through the RJ45 Ethernet switch port. Power to the phone is carried on unused wires within the drop cables. Spanning tree is a protocol on a switch that allows the switch to maintain multiple paths between switches within a subnet. The spanning tree protocol runs on each switch and is used to select a single path between any two switches. Trunking allows a switch to forward VLAN traffic between switches. 802. 1x is an authentication protocol used with port security (or port authentication).

Which of the following protocols are used with VoIP? (Select two.)

SNMP

SIP

SMTP

RTP

NTP

SIP & RTP

Explanation

Voice over IP (VoIP) uses the following protocols:

• Real-Time Transport Protocol (RTP) packets contain the actual voice data.

• Session Initiation Protocol (SIP) is used to set up, maintain, teardown, and redirect the call.

NTP is used for synchronizing time between devices. SNMP is used by devices for sending configuration information. SMTP is used for sending email.

Which of the following protocols is used by VoIP to set up, maintain, and terminate a phone call?

TLS

SIP

NTP

RTP

SSH

SIP

Explanation

The Session Initiation Protocol (SIP) is used to set up, maintain, teardown, and redirect the call. The Real-Time

Transport Protocol (RTP) contains the actual voice data. SSH is used for secure remote administration of a network device. TLS is used to add security to other protocols. NTP is used for synchronizing clocks on network devices.

You need to provide DHCP and file share services to a physical network. These services should be deployed using virtualization. Which type of virtualization should you implement?

Virtual networks

Network as a Service (NaaS)

Virtual servers

Virtual desktops

Virtual servers

Explanation

Server virtualization runs multiple instances of a server operating system on a single physical computer. With server virtualization, you can migrate servers on older hardware to newer computers, or add virtual servers to computers with extra unused hardware resources. Virtual desktops do not provide DHCP services. Virtual networks allow virtual servers and desktops to communicate with each other, and they can also allow communication (via

the host operating system) to network devices out on the physical network. Network as a Service (NaaS) servers and desktops that are all virtualized and managed by a contracted third-party.

In virtualization, what is the role of the hypervisor?

A hypervisor is a software implementation of a computer that executes programs like a physical machine.

A hypervisor allows virtual machines to interact with the hardware without going through the host operating system.

A hypervisor has the actual hardware in place on the machine, such as the hard disk drive(s), optical drive, RAM, and motherboard.

A hypervisor is created within the host operating system and simulates a hard disk for the virtual machine.

A hypervisor allows virtual machines to interact with the hardware without going through the host operating system.

Explanation
A hypervisor is a thin layer of software that resides between the virtual operating system(s) and the hardware. A hypervisor allows virtual machines to interact with the hardware without going through the host operating system. A hypervisor manages access to system resources
such as:
• CPU
• Storage

• RAM

A physical machine (also known as the host operating system) has the actual hardware in place on the machine, such as the hard disk drive(s), optical drive, RAM, motherboard, etc. A virtual machine is a software implementation of a computer that executes programs like a physical machine. The virtual machine(s) appear to be a self-contained and autonomous system(s). A virtual hard disk (VHD) is a file that is created within the host operating system and that simulates a hard disk for the virtual machine.

Which component is most likely to allow physical and virtual machines to communicate with each other?

Host operating system

Virtual desktop

Virtual switch

VHD

Virtual switch

Explanation

Virtual switches allow multiple virtual servers and/or desktops to communicate on virtual network segments and/or the physical network. Virtual switches are often configured in the hypervisor. A virtual hard disk (VHD) is a file that is created within the host operating system and that simulates a hard disk for the virtual machine. A physical machine (also

known as the host operating system) has the actual hardware in place on the machine, such as the hard disk drive(s), optical drive, RAM, motherboard, etc. A virtual desktop is a virtual machine in a software implementation of a computer that executes programs like a physical machine.

What type of virtualization completely simulates a real physical host?

Full virtualization

Semi-virtualization

Paravirtualization

Partial virtualization

Full virtualization

Explanation

In full virtualization, the virtual machine completely simulates a real physical host. This allows most operating systems and applications to run within the virtual machine without being modified in any way. In partial virtualization, only some of the components of the virtual machine are virtualized. Be aware of the following:

•The operating system uses some virtual components and some real physical hardware components in the actual device where the hypervisor • The operating system or application must be modified to run in a partial virtualization environment.

In paravirtualization, the hardware is not virtualized. Be aware of the following:

• All of the guest operating systems running on the hypervisor directly access various hardware resources in the physical device; components are not virtual.
• The guest operating systems run in isolated domains on the same physical hardware.
• The operating system or application must be modified before they can run in a paravirtualization environment.

- Vector