Exam :   640-861

Title   :   Designing for Cisco Internetwork
             Solutions (DESGN)

Ver   :   09-26-07

QUESTION 1:

What is the next step in the design methodology a network designer would take
after identifying customer requirements?

A. Design the topology.
B. Design network solutions.
C. Characterize the existing network.
D. Build a pilot network.
E. Plan the implementation.

Answer: C

Explanation:
Before beginning the design phase of a new network, the network designer must first
identify the customer needs and requirements so that a full understanding of what the
network is used for is accomplished. The next step is to characterize the existing network,
and then finally once that step is done the network designer should extract the new
customer requirements so that they can be compared to the existing network.

QUESTION 2:

Certkiller is planning to upgrade its current network. The chief technology officer
(CTO) has supplied a topology diagram and IP addressing scheme of the current
network during an interview. Certkiller has been growing at about twenty percent
per year and it has been difficult to maintain customer support at a satisfactory
level. The Certkiller board has met and directed the CTO to look into network
improvements.
Which two items are most relevant in documenting Certkiller 's business
requirements?

A. Improved customer support
B. Existing network topologies
C. IP addresses assigned by the ISP
D. Projected growth
E. Frequency of board meetings

Answer: A, D

Explanation:
Based on the facts provided about this network, it is clear that the chief concerns that
need to be addressed is the rate of growth of the company and the network, and the level
of customer support. When any growing company expands quickly, it is common for the
company to outgrow the capacity of the network, requiring additional network equipment
and resources.

QUESTION 3:

Proof of concept is required for a proposed design of a new campus network that utilized multilayer switching. The production network is business critical and no network disruptions are tolerated.
Which approach should be used to verify this design?

A. Pilot network
B. Prototype network
C. Hardware simulation
D. Expert consensus
E. None of the above

Answer: B

Explanation:
A prototype is a complex and full trial run of the network design used to prove that the design works. A prototype is usually a large-scale, fully functional form of a new design and thus is used to prove a large implementation. The customer would have to decide whether the need to prove the design justifies the cost of setting up a prototype. If the prototype is not appropriate for your customer, you might consider recommending a pilot, which is a smaller test designed for smaller businesses. The pilot usually tests more basic functions of the design, and it also usually requires less time and fewer resources. The criteria for choosing either test plan involves comparing the cost of the test against the need to prove that the design works. In this case, the network elements being tested are critical, so a full blown prototype should be used to test the design fully.
Reference: CCDA Exam Certification Guide, A. Anthony Bruno, CCIE #2738, p.286

QUESTION 4:

Which factor is a social requirement that will help you to identify current and future needs of your customer as you develop a new design plan?

A. Improved communications
B. Business partnerships
C. Improved customer-support services
D. The use of the network by its users as it relates to investors

Answer: C

Explanation:
Social requirements define the use of the network based on the company's business goals by its users and can include locations, market position, investors, vendors and customers. Developing the customer relations aspects such as identifying their future needs fall into this category.

QUESTION 5:

Which organizational constraint most directly affects the social requirements of a business?

A. Budget
B. Personnel
C. Policy
D. Schedule

Answer: B

Explanation:
Social requirements define the use of the network based on the company's business goals by its users and can include locations, market position, employees, unions, investors, vendors and customers. Employee relations and changes in personnel fall under the category of business social requirements.

QUESTION 6:

Certkiller wants to improve the security of their network.
Which information supplied by Certkiller would be most relevant to the new design?

A. The network topology.
B. The speed of the network.
C. The company's user policy.
D. The number of network users.
E. The applications permitted on the network.

Answer: C

Explanation:
Since the security policy of the Certkiller network is the chief concern, the current user policy would be most beneficial for the new design.
Incorrect Answers:
A: The network topology is not the primary issue.
B: Speed affect the number of users and applications and is an important consideration, but in this case we are more concerned with the security aspects.
D: Number of users matters in case of performance issue. It is not the primary issue in this case.
E: One can add or delete applications. It will not play major role

---

QUESTION 7:

Certkiller users have online access to sales records, customer records and billing

data in various branch office databases. Certkiller want to open a new branch office in the Midwest. The new branch office will have a dispatch center which will require constant communication with the local retailers.
What additional information should you obtain about applications in use on the network?

A. The authentication used by the application.
B. The routing protocols supported by the application.
C. The applications' integration in the network.
D. The application data-link layer overhead.
E. The applications' level of criticality.

Answer: E

Explanation:
It is always very important to first understand all of the major applications that will be running within the network, as well as their importance. In order to design the network properly, the critical applications must first be identified.

QUESTION 8:

Which three factors will you take into account when asked to characterize an existing network? (Select three.)

A. Traffic analysis
B. Impact on future business
C. Customer staff input
D. Visual inventory
E. Network audit
F. Server statistics
G. Ping analysis

Answer: A, C, E

Explanation:
To characterize a customer's network, you will need to:
* Identify any bottlenecks
* Determine whether the anticipated growth will cause problems
* Recognize legacy systems that must be incorporated into the new design
* Recognize business constraints and inputs to the design; business constraints are business-related issues that may place a limitation on your network design.
Reference: Designing Cisco Networks (Cisco Press) page 45

QUESTION 9:

Which of the following sources of information will prove to be most helpful and accurate when you are collecting data about a customer's existing network? (Choose

two.)

A. Existing network topology diagram
B. The resident IT specialist at the customer's company
C. User interviews
D. Configuration obtained from network equipment
E. Traffic analysis
F. Customer-supplied server list

Answer: A, D

Explanation:
Documenting the customer's current network is important before any changes are made.
Items you should be most attentive to include the following:
1. Network Topology
2. Addressing schemes
3. Concerns about the network
Reference: Designing Cisco Networks (Ciscopress) page 55

QUESTION 10:

You work as a network consultant. You are contracted by Certkiller to help with the
expansion of the Certkiller network.
Certkiller users have online access to sales records, customer records and billing
data in various branch office databases. Certkiller want to open a new branch office
in the Midwest. The new branch office will have a dispatch center which will require
constant communication with the local retailers.
You want to obtain information about current network availability. Which question
would you ask?

A. Is clustering technology in use by servers on the network?
B. Is full-duplex Ethernet technology deployed on the network?
C. Which routers have HSRP implemented?
D. Are the switches configured for auto-sensing?

Answer: C

Explanation:
The key is at the end of the question when it asks about current network availability,
which directly implies HSRP. HSRP is the Cisco Hot Standby Routing Protocol, which is
used to provide for router redundancy and network availability should one of the routers
or upstream links fail.

QUESTION 11:

You are contracted as the network administrator, for a gaming software company,

Certkiller . The CEO wants an improved communication infrastructure and thus
wants you to redesign the existing network.
The following is the Certkiller CEO's opinion:
* The goal is to become one of the top three peer-to-peer online gaming software
companies.
* There are currently 200 employees around the globe, of which 150 is located in
London, the head quarters.
* Anticipated staff growth is set at around 500 employees in two year's time. Of the 500
employees, 40% will work remotely as a cost reduction method.
* With such a growth rate, the release of 20 titles in the next 12 months is anticipated.
Which additional pieces of information are necessary to design the campus core? (Choose
all that apply?)

A. The current operating system.
B. The authenticity and security policy
C. The traffic pattern
D. The current implementation
E. The company's position in the gaming market industry

Answer: C, D
Explanation
Certkiller wants to redesign the network based on growth, therefore the below are needed
in the assessment:
Network Topology
Address Schemes
Concerns about the network
Incorrect Answers:
A: The OS is not relevant in the network redesign
B: Security and authenticity are not objectives and should already be in place given the
scenario.
E: Company position is irrelevant
Reference: Designing Cisco Networks, Page 55

QUESTION 12:

Which three sources does the network engineer use to collect information for
characterizing an existing network? (Choose tree)

A. Staff input
B. Visual inventory
C. Network Audit
D. Traffic analysis
E. Server Statistic

Answer: A, C, D

Explanation:
According to the Cisco Press CCDA Study Guide the steps for characterizing an existing network are:
Step 1 - Customer Input
Step 2 - Network Audit
Step 3 - Traffic Analysis

QUESTION 13:

Which two information sources will provide the most accurate data if you were tasked to find information regarding a customer's existing network? (Select two)

A. Existing network topology diagram
B. Customer interview
C. Traffic analyst
D. Configuration obtain from network equipment
E. Customer supply server list

Answer: A, D

Explanation:
Although gathering information from the customer is the 1st step it is usually not the most accurate. The most accurate sources of data can be found directly from the configuration files of the equipment and from documentation sources such as the existing network topology exams.

QUESTION 14:

The Certkiller network is upgrading their core LAN to a switched network. Which group of requirements is the primary reason to upgrade a client's network to a switched network?

A. Business requirements
B. Performance requirements
C. Manageability requirements
D. Application requirements
E. None of the above

Answer: B

Explanation:
With the recent developments in Gigabit Ethernet and LAN switching technologies, LAN designs are now capable of 1000 Mbps speeds. High-speed Gigabit links can connect servers to LAN switches. At these speeds, the capacity is there to meet the performance requirements of current high-bandwidth applications. Although upgrading a LAN to a

switched environment may mean additional up front costs, the performance of the
network will increase greatly.

QUESTION 15:

A stock brokerage firm is opening a new office in Melbourne. A dozen stock traders
will require constant data access to exchanges all around the world. This access
must be fast and without interruption.
Which two features can help provide this level of service? (Select two)

A. CDP
B. IGRP
C. CoS
D. QoS
E. GoS

Answer: C, D

Explanation:
Quality of Service/Class of Service:
More and more services running over converged, wireless or wireline networks require
Quality of Service (QoS) commitments in order to guarantee delivery of mission critical
traffic and applications across a network. Enterprise customers also increasingly require
Class of Service (CoS) control that allows them to implement priority queuing to classify
and prioritize packets based on factors such as type of application or by user.

QUESTION 16:

What are three valid methods of gathering information about an existing data
network? (Choose three)

A. Perform an audit at packet level detail (PLD) and for carrier service guarantees.
B. Use organizational input.
C. Perform a network audit to gather more detailed information of the network.
D. Analyze the user-mapping of a running application.
E. Perform a traffic analysis.
F. Use reports that have the ability to measure metrics.

Answer: C, D, E

Explanation:
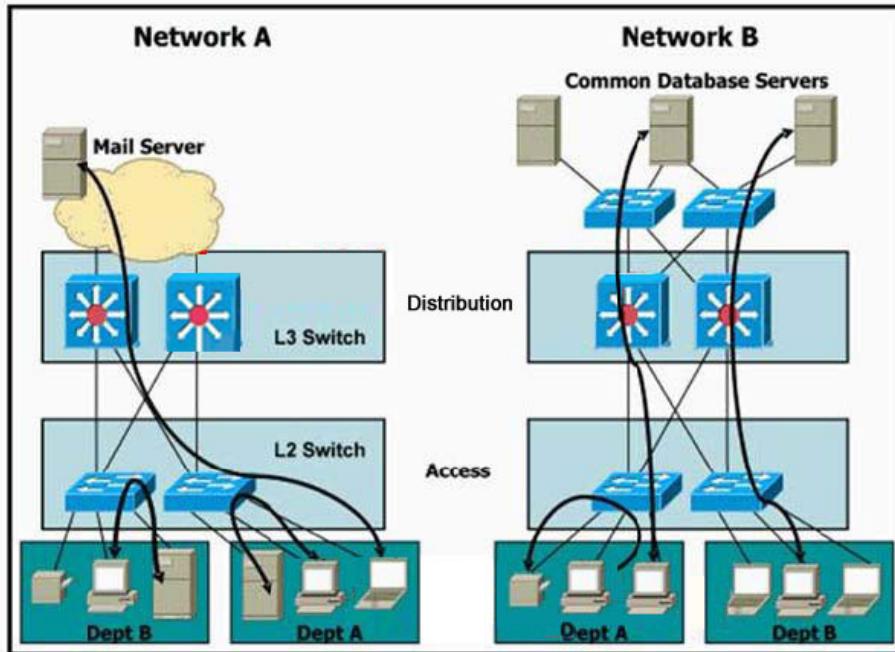The network information gathering aspects of the design phase comprise the following
steps:
1. Performing a network audit
2. Performing traffic analysis

3. Analyzing user applications
All of the above steps should be taken when gathering data about an existing network.

QUESTION 17:

Two different Certkiller networks are displayed below:

The two networks shown in the diagram have very different traffic patterns, as illustrated by the black arrows. Network A has two departments organized in separate VLANs. Each department VLAN contains the servers and printers that are used by the department personnel. The only common resource used by both departments is the email server, located on a remote network. Network B also has two departments organized in separate VLANs. All of the applications used by both departments are located on common database servers. The common database servers are located in a server farm on a separate network from the users. Which three statements are true about the networks in this diagram? (Choose three)

A. Network A is designed to accommodate file transfers from other department servers on a frequent basis.
B. The design in Network B will require a higher performance Layer 3 switch.
C. Network B illustrates the 20/80 rule.
D. Network B is designed so that distribution layer switches concentrate users in their own VLANs.
E. Network A is designed to keep 80% of the traffic within the local workgroup.
F. Network A is designed to have 80% of the traffic pass through the Layer 3 switches.

Answer: B, C, E

Explanation:

The 80/20 rule states that 80 percent of the traffic is "local" to the workgroup while 20 percent is remote or outside of the workgroup. In theory, by properly configuring VLANs or by using layer 3 devices to match workgroups, only the 20 percent of the traffic that is not local will need to pass through a router and out of the workgroup, improving performance for the 80 percent of the traffic that is within the workgroup. As shown by the traffic patterns pertaining to these two networks, only network A correctly represents this 80/20 rule, while network B shows the 20/80 rule.
In network B, a layer 3 switch should be added to increase network performance, while also decreasing the amount of broadcast traffic.

QUESTION 18:

Which of the following features will you affect when you choose a codec in your network design to carry IP telephony? (Choose all that apply.)

A. Voice packet header size
B. Bandwidth necessary for voice calls
C. Voice quality
D. Silence packet handling
E. All of the above.

Answer: B, C

Explanation:
The Codec that is chosen for VOIP will directly impact the bandwidth needed for each call, as well as the quality of that VOIP call. Generally, the codec that uses the least amount of bandwidth also has the worst voice quality. Below are the three most commonly used VOIP codecs:

Standard	Packet Size	Sample Duration	Data Rate Bits	PPS Simplex
G.711	120	15ms	64K	66
G.729A	10	10ms	8K	100
G.723.1	24	30ms	5.3/6.4K	33

Incorrect Answers:
A: This will not play any role for deciding codec
D: This is not main characteristic of codec
E: This is not a valid option.

QUESTION 19:

You are the network administrator at Certkiller . You are planning trunk capacity for the Certkiller network. You need to determine the number of circuits needed from a PBX to a converged network.
Which information would you require to make this decision? (Choose all that

apply.)

A. Busy hour traffic.
B. The number of sites.
C. Blocking probability (GoS).
D. The number of users per site.
E. The average duration of a call.

Answer: A, C

Explanation:
A: Measure network traffic load during the busiest hour because this period represents the maximum traffic load that your network must support. The result gives you a traffic load measurement commonly referred to as the Busy Hour Traffic (BHT).
C: Grade of Service (GoS) is defined as the probability that calls will be blocked while attempting to seize circuits. It is written as P.xx blocking factor or blockage, where xx is the percentage of calls that are blocked for a traffic system.
Incorrect Answers
B: Number of sites will give an idea for sizing the PBX
D: This will not play major role.
E: Most traffic models do not consider call duration. Call holding times are assumed to be exponential.

QUESTION 20:

To minimize expenses due to long distance charges, you designed a converged network to carry calls on-net as close as possible to the destination.
Why can a VoIP call go off-net earlier that designed? (Choose two.)

A. The local voice gateway sends busy-back signal.
B. The Call Manager server is too busy to process the call in a usual manner.
C. The telephone user dials an access code.
D. Destination routing not properly setup on the local and remote gateways.

Answer: A, C

QUESTION 21:

Which of the following will you cite as reasons why VoIP calls could go off-net earlier than designed when a converged network was configured to carry voice calls on-net as close as possible to the destination to minimize long distance charges? (Choose all that apply.)

A. destination routing not properly configured on both local gateways
B. local call manager server is too busy to process the call
C. local voice-gateway detects insufficient WAN bandwidth

D. the telephone user dials an access code
E. all of the above

Answer: C, D

Explanation:
If the near-end voice gateway, using quality of service (QoS) features detects that there is
not enough bandwidth to complete the call, then it reroutes the call off-net.

QUESTION 22:

A PBX is connected to a service provider that makes use of three ISDN PRI (T1)
links and no other facility. Non-Facility Associated Signaling (NFAS) is in use (only
one signaling channel for all three PRI links) and the tariff offering provides for the
maximum number of voice channels.
What is the maximum number of voice calls that can be made simultaneously?

A. 69
B. 71
C. 72
D. 90
E. 92
F. 120

Answer: B

Explanation:
ISDN Non-Facility Associated Signaling (NFAS) allows a single D channel to control multiple
Primary Rate Interfaces (PRIs). You can configure a backup D channel when the primary NFAS
D channel fails. When you configure the canalized T1 controllers for ISDN PRI, you only need to
configure the NFAS primary D channel; its configuration is distributed to all the members of the
associated NFAS group. By using a single D channel to control multiple PRIs, one extra channel
on each interface is free to carry data traffic. Any hard failure of the primary D-signaling channel
results in an immediate switchover to the backup D channel without disconnecting currently
connected users. Note: If you configure a backup D channel, only 23 B channels can be used on
the backup T1 controller because the D channel on the backup is unavailable. Therefore, only
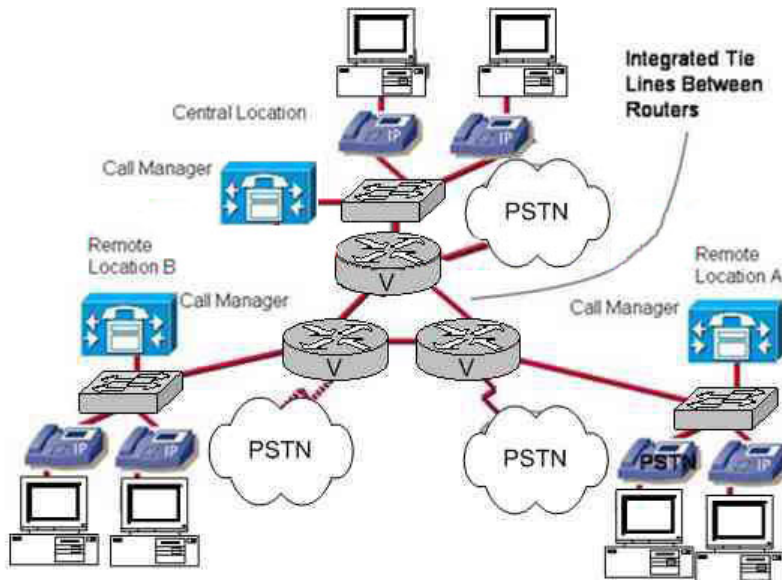those T1s that are neither primary nor backup can have 24 B channels available.
(23+1 23+1 23) = 71 last t1 D channel will used for backup
http://www.cisco.com/warp/public/793/access_dial/quadt1_nfas.pdf

QUESTION 23:

Study the exhibit below carefully:

Above is a converged voice and data network. This network is designed to carry voice calls on-net as close a possible to the destination to reduce long distance charges.

Why is it that a VoIP call can go off-net earlier than designed? (Choose two)

A. The local voice gateway detects lack of bandwidth.
B. The destination routing is not configured on both local and remote gateways.
C. The telephone user dials an access code.
D. The local call manager server is too busy to process the call.

Answer: A, C

QUESTION 24:

DRAG DROP

Drag the dial peer function to the dial peer that it describes

Mapped to a virtual circuit on the interface from which the call exits the router
Mapped to a data-link connection identifier on the interface from which the cell exist the router
May use RAS to determine the destination target by querying the H.323 gatekeeper
Maps a telephone dial string to a specific port on a **missing**

POTS dial peer	Place here
VoIP dial peer	Place here
VoFR dial peer	Place here
VoATM dial peer	Place here

Answer:

Drag the dial peer function to the dial peer that it describes

POTS dial peer	Maps a telephone dial string to a specific port on a **missing**
VoIP dial peer	May use RAS to determine the destination target by querying the H.323 gatekeeper
VoFR dial peer	Mapped to a data-link connection identifier on the interface from which the cell exist the router
VoATM dial peer	Mapped to a virtual circuit on the interface from which the call exits the router

QUESTION 25:

This is a *Testlet* - it contains 3 questions that relate to the scenario below (1 of 3):
Certkiller is a call center consulting company that has a large call center of its own.
Certkiller has been to busy with new business that the company has not moved
toward IP telephony, even while encouraging it for clients. The company has a basic
TDM network and wants to move toward a converged voice and data network.
When consulting with the decision makers, you find that they know that a
packet-switches network is a better solution but they cannot explain why.
What are two key points to communicate that will help them understand this
concept? (Choose two)

A. A packet-switches network enables more rapid development of new features and
opens up application development.

B. Circuit-switches voice calls require a dedicated duplex 64-kbps connection between two telephones for the duration of the call.
C. The packet switching model is composed of three independent layers with open standard interfaces among them.
D. The open call control layer directs voice calls to the appropriate destinations in the packet infrastructure layer.
E. Packet-switches networking only uses bandwidth for voice when it is required.
F. While the circuit-based networks allow new features to be developed quickly, the packet-based network allows APIs to be developed, which enables applications to be developed more efficiently.

Answer: A, E

Explanation:
One of the mayor benefits to packet switched networks is that it sets industry standards which allows for more rapid introduction of new features and applications.

QUESTION 26:

This is a *Testlet* - it contains 3 questions that relate to the scenario below (2 of 3):
Certkiller is a call center consulting company that has a large call center of its own.
Certkiller has been to busy with new business that the company has not moved toward IP telephony, even while encouraging it for clients. The company has a basic TDM network and wants to move toward a converged voice and data network.
When consulting with the decision makers, you find that they know that a packet-switched network is a better solution but they cannot explain why.
What are two most likely business drivers for integrating voice and data networks?
(Choose two)

A. Voice has overtaken data as the primary traffic on voice networks.
B. Companies want to reduce WAN costs by migrating to voice networks that can carry data.
C. The PSTN is sufficient for creating features but it cannot deploy them quickly enough.
D. Data, voice, and video cannot converge on the current PSTN structure.
E. The architecture that is built for voice is not flexible enough to carry data optimally unless PRI circuits are used for aggregating BRI circuits for data.
F. The PSTN is effective for carrying data signals but VoIP does not transmit efficiently.

Answer: B, D

QUESTION 27:

This is a *Testlet* - it contains 3 questions that relate to the scenario below (3 of 3):
Certkiller is a call center consulting company that has a large call center of its own.
Certkiller has been to busy with new business that the company has not moved toward IP telephony, even while encouraging it for clients. The company has a basic

TDM network and wants to move toward a converged voice and data network.
When consulting with the decision makers, you find that they know that a
packet-switched network is a better solution but they cannot explain why.
Which are three independent layers of a converged packet-switches network?
(Choose three)

A. Open service application
B. Digital trunk subsystem
C. Open call control
D. Standards-based packet infrastructure
E. Common channel signaling complex
F. Open connection control

Answer: A, C, D

QUESTION 28:

Certkiller Technologies has a single location with headquarters in one office building
and three warehouses. Their customer base consists of 400 independent parts
resellers. The resellers connect through direct links to the Certkiller network to
access an ordering system. The servers and access routers connecting to the retail
outlets are on a separate Ethernet VLAN in the headquarters campus. The resellers
complain about poor response time when they connect to the ordering system.
Certkiller Technologies wants you to help them improve their network to increase
the performance of their customers' connections to the ordering system.
What are two additional details about Certkiller 's existing network needed for this
analysis? (Choose all that apply.)

A. The Router ACLs that provide security to the servers.
B. The bandwidth for the Internet connection.
C. Type of the connections to the resellers.
D. Utilization on the servers' VLAN.
E. The number of users on the headquarters LAN.

Answer: C, D

Explanation:
Type of connection (Leased line, ISDN, Frame Relay) determines the response time.
Monitor the Server's speed. Install more processing servers to reduce response time.
Incorrect Answers
A: ACLs provide filtering of packets. It will not improve response time.
B: Bandwidth determines type of link.
E: The headquarters LAN is not being accessed by the resellers. Therefore, the number
of users on it may not play critical role.

QUESTION 29:

Certkiller was approached by the Minister of the Education Department, to start an experiment in one of the public school districts since the government passed a Bill that all schools are to comply with the Safe Schools Initiative.
The situation at the schools in this district is as follows:
The district has approximately 3000 students dispersed in the following manner:
- one high school, one junior high school and three grade schools.
All the phone calls to these schools are switched by a local telephone company's centrex switch after which it is routed to the appropriate school.
The schools are all fitted with fractional T1 Frame Relay and Cisco routers for networking purposes. The users are on a switched 10/1/100 network utilizing Cisco switched and Category 5 cable. The high school has the Internet access through an Internet Service Provider which resides 35 miles away via a T1 Frame Relay. This internet connection is shared with the other schools in the district.
Due to the Safe Schools Initiative, phones need to be put in each classroom. Though the costs are astronomical and there are no facilities, the schools would also want to install video in each school for video conferencing purposes and it will be a definite aid in distance learning for the high school. ISDN PRI LINKS will be used to connect the video partners.
In addition to the above, there is also the student information; that is stored on the local servers and shared between the schools as learners graduate from elementary to junior high to high school as well as transfers in and out of the district; that has to be protected.
Why would you, the network administrator at Certkiller , suggest IP telephony to this particular customer? (Choose all that apply.)

A. Voice, video and data run on the same physical media, namely, Cat5 cable.
B. Reduction of long distance charges by using VoIP.
C. Eliminate reliance on local provider for any future phone calls.
D. The cost of adding additional telephones is minimal.
E. All of the above.

Answer: A, D

Explanation:

A. In a converged network, voice, video and integrated data runs on the same physical media.
D. The cost is reduced and minimized by requiring less from the telephone service provider.
Incorrect:
B: Chapter 17, CCDA Exam Certification Guide:Page 435
The introduction of packet-voice technology allows the convergence of data and voice networks --- which lets companies save toll charges on voice telephone calls and reduce their total cost of ownership by not having to build and operate networks for voice, video,

and data. Long distances charges are reducedwhen the remote site is part of the IP network. In this case, the schools are part of a local school district and any long distance calls would not apply to this rule.

C: Calls that are placed between offices through the private voice network are called on-net. If a user needs to place a call outside the private network, the call is routed to the local PSTN. If the call is forwarded to the PSTN, it is called off-net. Because not all calls are point to point the need for local company still exists.

QUESTION 30:

Certkiller was approached by the Minister of the Education Department, to start an experiment in one of the public school districts since the government passed a Bill that all schools are to comply with the Safe Schools Initiative.

The situation at the schools in this district is as follows:

The district has approximately 3000 students dispersed in the following manner:
- one high school, one junior high school and three grade schools.

All the phone calls to these schools are switched by a local telephone company's centrex switch after which it is routed to the appropriate school.

The schools are all fitted with fractional T1 Frame Relay and Cisco routers for networking purposes. The users are on a switched 10/1/100 network utilizing Cisco switched and Category 5 cable. The high school has the Internet access through an Internet Service Provider which resides 35 miles away via a T1 Frame Relay. This internet connection is shared with the other schools in the district.

Due to the Safe Schools Initiative, phones need to be put in each classroom. Though the costs are astronomical and there are no facilities, the schools would also want to install video in each school for video conferencing purposes and it will be a definite aid in distance learning for the high school. ISDN PRI LINKS will be used to connect the video partners.

In addition to the above, there is also the student information; that is stored on the local servers and shared between the schools as learners graduate from elementary to junior high to high school as well as transfers in and out of the district; that has to be protected.

Why would you, the network administrator at Certkiller , suggest moving towards a converged network to this particular customer?
(Choose all that apply.)

A. Cost savings by using a single cabling system for voice, video and data.
B. Reduction of long distance charges by making use of VoIP.
C. Can increase the number of phones without having to upgrade outside facilities.
D. Eliminate reliance on local provider for any future phone calls.
E. All of the above.

Answer: A, C

Explanation:

A. In a converged network, the need for separate cabling is eliminated because voice, video and integrated data runs on the same physical media. This saves on costs of running two different cabling systems and in wiring closets.
C. Additional phones can be added without the need of outside upgrades
Incorrect:
B: Long distance charges would not be eliminated because long distance calls are going off-net.
D. The local provider would still be needed for off-net calls.

QUESTION 31:

Certkiller was approached by the Minister of the Education Department, to start an experiment in one of the public school districts since the government passed a Bill that all schools are to comply with the Safe Schools Initiative.
The situation at the schools in this district is as follows:
The district has approximately 3000 students dispersed in the following manner:
- one high school, one junior high school and three grade schools.
All the phone calls to these schools are switched by a local telephone company's centrex switch after which it is routed to the appropriate school.
The schools are all fitted with fractional T1 Frame Relay and Cisco routers for networking purposes. The users are on a switched 10/1/100 network utilizing Cisco switched and Category 5 cable. The high school has the Internet access through an Internet Service Provider which resides 35 miles away via a T1 Frame Relay. This internet connection is shared with the other schools in the district.
Due to the Safe Schools Initiative, phones need to be put in each classroom. Though the costs are astronomical and there are no facilities, the schools would also want to install video in each school for video conferencing purposes and it will be a definite aid in distance learning for the high school. ISDN PRI LINKS will be used to connect the video partners.
In addition to the above, there is also the student information; that is stored on the local servers and shared between the schools as learners graduate from elementary to junior high to high school as well as transfers in and out of the district; that has to be protected.
Why would you, the network administrator at Certkiller , protect the learner records when in transit between schools and when being shared with other school districts over the Internet,for this particular customer?

A. Authenticate users
B. Employ dactyloscopy
C. Encrypt the data
D. Event Log all access attempts
E. All of the above.

Answer: C

Explanation: All answers seem feasible. If I have to choose ONE, I will go with

encryption. It is the single item that will render any illegal acquisition of the data unusable.

QUESTION 32:

Certkiller was approached by the Minister of the Education Department, to start an experiment in one of the public school districts since the government passed a Bill that all schools are to comply with the Safe Schools Initiative.
The situation at the schools in this district is as follows:
The district has approximately 3000 students dispersed in the following manner:
- one high school, one junior high school and three grade schools.
All the phone calls to these schools are switched by a local telephone company's centrex switch after which it is routed to the appropriate school.
The schools are all fitted with fractional T1 Frame Relay and Cisco routers for networking purposes. The users are on a switched 10/1/100 network utilizing Cisco switched and Category 5 cable. The high school has the Internet access through an Internet Service Provider which resides 35 miles away via a T1 Frame Relay. This internet connection is shared with the other schools in the district.
Due to the Safe Schools Initiative, phones need to be put in each classroom. Though the costs are astronomical and there are no facilities, the schools would also want to install video in each school for video conferencing purposes and it will be a definite aid in distance learning for the high school. ISDN PRI LINKS will be used to connect the video partners.
In addition to the above, there is also the student information; that is stored on the local servers and shared between the schools as learners graduate from elementary to junior high to high school as well as transfers in and out of the district; that has to be protected.
Which means of protection of the servers that contain the learner information would you, the network administrator at Certkiller , suggest to this particular customer?
(Choose all that apply.)

A. Encrypt VoIP call managers' traffic to and fro.
B. Implement host-based security on the servers.
C. Make use of public-key cryptography.
D. Implement a firewall between the school network and the Internet.
E. All of the above.

Answer: B, D

Explanation: A firewall will provide frontline protection against a public network.
The second-level protection will be to implement host-based sec on the servers to ensure only personnel's authorized to used the info stored on the server are allow to access them.
Incorrect Answers:
A We are interested in protecting data, not voice

C will work if we are communicating over a public network but in this case we are not.
E is negated.

QUESTION 33:

Certkiller has a campus network with five buildings. All the Certkiller servers and
the central core of the network are located in Building 1. A Catalyst 6500 multilayer
switch connects to each of the other building through Gigabit Ethernet link over
multimode fiber optic cable. Each building has a separate IP subnet with 300 to 500
devices in each. Certkiller users report some serious network performance problems.
Periodically, response time becomes very slow and then increases again. The
problem has been sporadic and very difficult to troubleshoot. Certkiller uses
Microsoft 2000 and Sun Solaris servers and Windows 2000 workstations with
default configurations.
What change in network design would you recommend to improve performance?

A. Install a dual Gigabit Ethernet uplinks to the buildings.
B. Install a layer 3 switch on each subnet.
C. Use Single mode fiber optic cable for the Gigabit Ethernet uplinks to the buildings.
D. Implement multiple VLANs in each of the buildings

Answer: D

QUESTION 34:

The accounting department and sales at Certkiller .com, a medium-sized company,
are complaining of slow network response on a common network that uses RIPv1.
Traffic analysis shows excessive broadcast traffic.
Which network design change will improve network response time?

A. The addition of a bridge between the two departments
B. The segmentation of the network into separate VLANs.
C. A migration to IPv6.
D. A migration to EIGRP.
E. None of the above

Answer: B

Explanation:
The best way to reduce the amount of broadcast traffic within a network is to segment
that network, either via the use of layer 3 devices (routers) or by implementing VLANS.
VLANs are used to segment a single large broadcast domains into multiple, smaller
broadcast domains.
Incorrect Answers:
A: Bridges are used to increase the size of the broadcast domain, by linking together
networks at layer 2. They increase the size of the broadcast domain, and as a result the

number of broadcasts normally increases with the use of bridges.
C: IPv6 also use broadcasts, so this alone will not decrease the number of broadcasts.
D: EIGRP is a routing protocol used to route traffic to different networks, but our
problem is with a single broadcast domain LAN.

QUESTION 35:

Certkiller .com has a campus network with five buildings. Building 1 contains all the
Certkiller .com servers and the central core of the network. A Catalyst 6500
multilayer switch connects to each of the other buildings through Gigabit Ethernet
links over multimode fiber optic cable. Each building has a single IP subnet with
300 to 500 devices in each.
A network technician at Certkiller .com calls you and reports some serious network
performance problems. Periodically, response times become very slow for several
minutes at a time and then speeds up. The problem has been sporadic and very
difficult to troubleshoot. Certkiller .com uses Microsoft Windows 2000 and Sun
Solaris servers and Windows 2000 workstations with default configurations.
What change in network design would you recommend to Certkiller .com to improve
performance?

A. Install dual Gigabit uplinks to the buildings
B. Put a layer 3 switch in each building
C. Use single mode fiber for the gigabit uplinks
D. Implement multiple VLANs in each of the buildings

Answer: D

Explanation:
Due to the high number of users in each IP subnet, the problems associated with this
network is most likely due to excessive broadcasts, which should be segmented via the
use of multiple VLANs. Similar to routers, VLANs offer an effective mechanism for
setting up firewalls in a switch fabric, protecting the network against broadcast problems
that are potentially dangerous, and maintaining all the performance benefits of switching.
You can create these firewalls by assigning switch ports or users to specific VLAN
groups in single switches and across multiple connected switches. Broadcast traffic in
one VLAN is not transmitted outside that VLAN. This type of configuration substantially
reduces overall broadcast traffic, frees bandwidth for real user traffic, and lowers the
overall vulnerability of the network to broadcast storms.
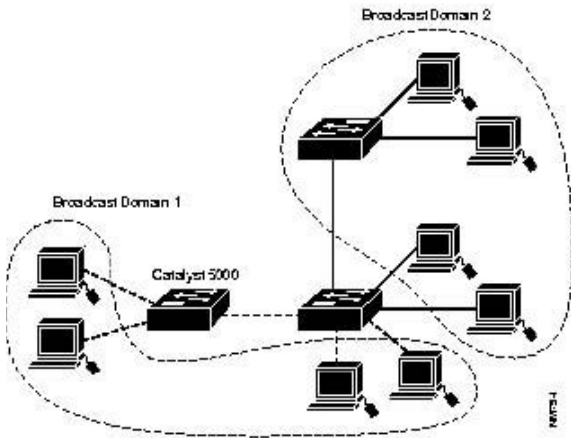
You can control the size of the broadcast domains by regulating the overall size of their associated VLANs and by restricting both the number of switch ports in a VLAN and the number of people using these ports.

QUESTION 36:

Queue investigation reveals a number of drops per hour. Which two quantities, when exceeded, suggest that network enhancement should be part of the design? (Choose two)

A. 5 output
B. 10 input
C. 50 input
D. 100 output
E. 100 input
F. 10 output

Answer: B, F

Explanation:
Input Queue Drops
When a packet enters the router, the router attempts to forward it at interrupt level. If a match cannot be found in an appropriate cache table, the packet is queued in the input queue of the incoming interface to be processed. Some packets are always processed, but with the appropriate configuration and in stable networks, the rate of processed packets must never congest the input queue. If the input queue is full, the packet is dropped.
Output Queue Drops
Output drops are caused by a congested interface. For example, the traffic rate on the outgoing interface cannot accept all packets that should be sent out. The ultimate solution to resolve the problem is to increase the line speed. However, there are ways to prevent, decrease, or control output drops when you do not want to increase the line speed. You can prevent output drops only if output drops are a consequence of short bursts of data. If

output drops are caused by a constant high-rate flow, you cannot prevent the drops. However, you can control them. In circumstances, the input and output drops should never exceed 10 per hour.

QUESTION 37:

Excessive broadcasts can cause network problems. Which two statements are characteristic of data link layer broadcasts? (Select two)

A. Broadcasts are not forwarded by routers.
B. Broadcasts do not occur at Layer 3.
C. Broadcasts are restricted to ports with active, end-user devices.
D. Broadcasts can be controlled with the use of VLANs.

Answer: A, D

Explanation:
VLANs can also be used to control broadcasts. Broadcast domains can be bounded by VLANs in a stand-alone environment. In an internetworking environment, they are typically bounded by routers because routers do not forward broadcast frames.
By default, broadcasts are not forwarded by routers. An exception to this is through the use of the "ip helper-address" command. This command will configure all broadcasts to a specific IP address destination, which is useful for DHCP when the DHCP server resides on a different subnet than the local network.

QUESTION 38:

In which three places can a network design be verified and tested? (Choose three)

A. A live network
B. A pilot network
C. A prototype network
D. A design network
E. A trial network
F. A mock-up network

Answer: B, C, E

QUESTION 39:

Which three items should be included in a summary report that validates the findings of the information you have gathered when charactering a network? (Choose three)

A. Network services map
B. Network problems and drawbacks

C. Modularized network
D. Network features
E. Network applications map
F. Actions that support network requirements

Answer: B, D, F

QUESTION 40:

You are a network consultant. You are contracted by Certkiller to subnet their network. You want to document the existing Certkiller network.
Which two Cisco router services can assist in documenting the existing network? (Choose all that apply.)

A. CDP
B. MRTG
C. NetMon
D. NetFlow
E. SNMP MIB compiler

Answer: A, D

Explanation:
A. CDP is a media- and protocol-independent protocol that runs on all
Cisco-manufactured equipment including routers, bridges, access and communication
servers, and switches. Using CDP, you can view information about all the Cisco devices
directly attached to the switch. In addition, CDP detects native VLAN and port duplex
mismatches.
Network management applications can retrieve the device type and SNMP-agent address
of neighboring Cisco devices using CDP. This allows applications to send SNMP queries
to neighboring devices. CDP allows network management applications to discover Cisco
devices that are neighbors of already known devices, in particular, neighbors running
lower-layer, transparent protocols.
D. NetFlow services consist of high-performance IP switching features that capture a rich
set of traffic statistics exported from routers and switches while they perform their
switching functions
Incorrect Answers
B: Multi -Router Traffic Grapher is used to monitor the level of activity on network
links.MRTG generates reports in HTML pages that contain Portable Network Graphic
(PNG) images that portray a visual look at the traffic on a link.
C,E: These are not related to network traffic analysis.

QUESTION 41:

You are a network administrator at Certkiller and have been instructed to present a
network design document to a customer. Which of the following elements would you
deem essential to show to the customer?

(Choose all that apply.)

A. Proof of concept
B. Vendor availability
C. Design specifications
D. Organizational chart
E. Implementation plan
F. Data source

Answer: A, C, E

Explanation:
Content of the Design Documentation
Your design should include the following sections, at a minimum, although you may
choose to include additional sections:
1. Executive summary
2. Design requirements
3. Design Solution
4. Summary
5. Appendixes
6. The cost of the proposed design may be provided separately
Reference: Designing Cisco Networks (Ciscopress) page 258

QUESTION 42:

Which of the following are essential sections of a network design document that
need to be presented to a customer?

A. Design requirements.
B. The existing network.
C. Data sources.
D. A prototype network.
E. Technical justifications.

Answer: A, B, E

Explanation:
Documenting the customer's current network is important before any changes are made.
Items you should be most attentive to include the following:
1. Network Topology - Existing network
2. Addressing schemes - Design requirements
3. Concerns about the network - technical justifications
Reference: Designing Cisco Networks (Ciscopress) page 55

QUESTION 43:

One of the Certkiller customers has a very large Cisco network. To simplify matters for future troubleshooting purposes, you need to document this network.
Following is a list of routers that are being used in the current network.
435 Cisco model 2600 routers
129 Cisco model 3600 routers
10 Cisco model 7500 routers
Which of the following items should be added to complete the documentation of these routers?

A. error statistics
B. software revisions
C. power requirements
D. interface options
E. event logs
F. management protocols

Answer: B, D

Explanation:
The network audit process should provide detailed recommendations to address the challenges, opportunities, and problems identified in the audit. The audit will also help the network engineering team proactively identify and resolve potential network troubles before major problems are encountered.
Following is a list of reports that are often generated as part of network audit:
1) Performance reports
2) Configuration reports
3) Software reports
4) Hardware reports
Reference: Ciscopress CCDA Exam Certification Guede Second Edition p.16

QUESTION 44:

Your newly appointed Certkiller trainee wants to which of the following are the main sources for documenting a customer's requirements for a network design project
What will your reply be? (Choose all that apply.)

A. network application specifications
B. interview with customer
C. conversations with resident IT staff
D. request for proposal (RFP)
E. diagram of desired network
F. network performance specifications

Answer: B, D

Explanation:
The sources for documenting the customer requirements are the original
RFP/RFI and discussions with the customer.
Page 51 in CiscoPress CCDA Self-Study: Designing for Cisco Internetwork
Solutions DESGN 640-861. ISBN : 1587051419, Third printing june 2005

QUESTION 45:

Your newly appointed Certkiller trainee wants to know which of the following items
of information are most relevant when documenting a company's business
requirements.
What will your reply be? (Choose all that apply.)

A. enhanced customer support
B. existing topologies
C. priority settings
D. projected growth
E. frequency of board meetings
F. all of the above

Answer: A, D

Explanation:
Determining Company Business Goals
Determine the company's major business goals for the next year and the next five years.
This information is important to help you design an internetwork that provides the
scalability required. Research your customer's industry and competition. Armed with
knowledge of your customer's business, you can position Cisco technologies and
products to help strengthen the customer's status in the customer' own industry.
Reference: Designing Cisco Networks (Ciscopress) page 46

QUESTION 46:

The Certkiller trainee technician wants to know which two Cisco Router services
perform network traffic analyses to assist in the documenting a customer existing
network. What will your reply be? (Choose two.)

A. MRTG
B. NetMon
C. NetFlow
D. CDP
E. SNMP MIB Comlier

Answer: C, D
Not A: MRTG is not a cisco service.

QUESTION 47:

Which of the tools listed below will be of use to a network designer that will help to automate the documentation of network infrastructure? (Choose two)

A. Syslog
B. CiscoWorks
C. IOS commands
D. WhatsUp Gold
E. Visio

Answer: B, E

QUESTION 48:

Which of the following are not included in an Executive Summary? (Choose all that apply.)

A. The cost of the project.
B. The purpose of the project.
C. The benefits of the solution.
D. Strategic recommendations.
E. Implementation considerations.

Answer: A

Explanation:
The Executive Summary describes the network requirements and how the proposed design meents those requirements. The audience for the executive summary is the decision makers for the project. The following is a list of suggested topics:
1) State the goals of the project and how it relates to the business needs.
2) Describe how your solution addresses these business needs. Outline the network-design strategy.
3) Describe the implementation concerns such as integration issues, training, support, and transition issues.
4) Outline the benefits of the solution
Reference: Ciscopress CCDA Exam Certification Guede Second Edition p.30
Incorrect Answers
B, C, D, E: All are included in Executive Summary.

QUESTION 49:

You, the network administrator, must design a network that will provide scalability for one of Certkiller 's customers. Which of the following factors will influence your design when you document the customer's business requirements?
(Choose all that apply.)

A. Router software upgrades
B. Customer support improvements
C. Future software applications
D. Future company growth
E. IP address assignments
F. Available funds
G. Current network topology

Answer: B, D

Explanation:
Determining Company Business Goals
Determine the company's major business goals for the next year and the next five years. This information is important to help you design an internetwork that provides the scalability required. Research your customer's industry and competition with knowledge of your customer's business, you can position Cisco technologies and products to help strengthen the customer's status in the customer' own industry.
Reference: Designing Cisco Networks (Ciscopress) page 46

QUESTION 50:

You work as a network consultant. You are designing a network for Certkiller , Inc. What is the first task that you should perform when documenting Certkiller 's requirements and their existing environment of the network design project?

A. Assess the cost of the design project.
B. Identify applications, both planned and installed.
C. Identify their security requirements.
D. Identify their business constraints.
E. Assess their business goals.

Answer: E

Explanation:
The network designer must document fully the new proposed network. Obviously, this document should fully describe how the new design meets the technology goals of the organization and how, in turn, the technology of the organization meets the business goals of the organization. Wherever possible, the designer should note the exact service levels possible with the new design.
Reference: Ciscopress CCDA Exam Certification Guede Second Edition p.139

QUESTION 51:

You are the technician at Certkiller and received an instruction to compile a technical report. Hence you document the routers on the network.

Which of the following items will you include in your report? (Choose all that apply.)

A. Interface loads
B. Interface configurations
C. Interface error statistics
D. Router software revision
E. Interface load requirements
F. Router power requirements

Answer: B, C, D

Explanation:
Reference: Designing Cisco Networks (Ciscopress) page

QUESTION 52:

EXHIBIT MISSING Will be provided in later versions.
What topology is represented in the above exhibit?

A. High-level topology map of the customer's current network.
B. High-level topology map of the customer's proposed e-mail packet flow.
C. High-level topology map that meets the customer's requirements.
D. High-level topology map of the customer's proposed intranet security system.

Answer: A

QUESTION 53:

Which two layers of the OSI model should have a topology map furnished in the Draft Design Document? (Choose two)

A. Physical
B. Data link
C. Session
D. Application
E. Network
F. Transport

Answer: A, E

Explanation:
A network topology design map should visually represent the physical layout of the network, such as devices used, connections, and physical topology. This will include all major layer 1 (physical layer) aspects of the network.

The network map should also contain all layer 3 (network layer) aspects, including routing protocols, IP addresses, and subnet masks.

QUESTION 54:

Which two closely related items does a Draft Design Document require that directly influence the network design? (Choose two)

A. Customer input
B. Traffic analysis
C. Design requirements
D. Existing network infrastructure
E. Logical topology map
F. Physical topology map

Answer: A, C

QUESTION 55:

You are a network consultant, you are contracted by Certkiller , Inc. to subnet their network. Before you make any changes to the network, you must document the current network.
What should you include in this documentation? (Choose all that apply.)

A. Addressing schemes.
B. Concerns about the network.
C. Protocol analysis.
D. Network topology.
E. Computer names.

Answer: A, B, D

Explanation:
Documenting the customer's current network is important before any changes are made.
Items you should be most attentive to include the following:
1. Network Topology
2. Addressing schemes
3. Concerns about the network
Reference: Designing Cisco Networks (Ciscopress) page 55

QUESTION 56:

You are a network administrator at Certkiller . You have been instructed to design IPv6 into a network that runs on IPv4.
Which of the following strategies will permit the two address schemes to coexist while the migration is underway? (Select two.)

A. Deploy stateful addressing assignments.
B. Encapsulate IPv6 packets into IPv4 packets.
C. Construct a bridge between the IPv6 and the IPv4 networks.
D. Configure translation from one protocol into the other.
E. Enable anycast capabilities in the routing protocol.

Answer: B, D

Explanation:
IPv4 to IPv6 Transition Strategies and Deployments
Several deployment models exist to migrate from an IPv4 network to IPv6. During a
transition time, both protocols can coexist in the network. The deployment models are
- IPv6 over dedicated WAN links
- IPv6 over IPv4 tunnels (B)
- IPv6 using dual-stack backbones
- Protocol translation (D)
Source: CCDA Exam Certification Guide Second Edition, Page 253

QUESTION 57:

One of Certkiller 's customers wants to monitor the activities on all the end systems
in her house via remote access. Her house consists of a large mansion that has IP
enabled end-systems such as appliances, video cameras, security systems, light
switches as well as heating systems. This network is connected to the Internet
continually through ADSL and employs Network Address Translation (NAT).
She wants some advice as to which IP addressing system would be most suitable for
all the end systems in her house.
What will you tell her?

A. Public IPv4 addresses
B. Micro-IP addresses
C. Public IPv6 addresses
D. A combination of IPv6 and Micro IP addresses.
E. Private IPv4 addresses
F. A combination of Private and Public IPv4 addresses
G. Private IPv6 addresses

Answer: E

Explanation:
Dynamic NAT using a pool of IP addresses or Port address Translation, using a Single IP
address. This will not consume Public address space.
Incorrect Answers
A, B, C, D, and F: These are public addresses. They are most expensive. Not suitable.

QUESTION 58:

The Internet Service Provider assigned an IPv6 address range to Certkiller Ltd.
However, Certkiller has decided to use the IPv6 addresses internally only and access
the Internet via port address translation (PAT).
Which of the following would Certkiller need for their domain Name Servers DNS)?

A. DNS servers would be obsolete.
B. Their DNS servers must be configured to support only IPv4 addresses.
C. Their DNS servers must be configured to support both IPv4 and IPv6 addresses.
D. Their DNS servers must be configured to support only IPv6 addresses.
E. No changes to the DNS servers are necessary.
F. More DNS servers are needed in the network to support the IPv6 addresses only.

Answer: C

Explanation:
Both are required for support downward compatibility.
Incorrect Answers
A: DNS servers are required for Name resolution
B: IPv4 is problem in this case
D: IPv6 is problem in this case
E. Changes are required in software to support IPv6.
F: This will add extra cost to the service Provider

QUESTION 59:

The translation of private addresses into registered IP addresses are permitted by which
of the following Cisco IOS features? (Choose the correct option.)

A. Cisco Address Translation
B. Network Address Translation
C. Local Address Registration
D. Cisco Address Registration
E. Global Address Registration

Answer: B

Explanation:
Network Address Translation (NAT) is a feature in the Cisco IOS software that enables
you to translate private addresses into registered IP addresses only when needed, thereby
reducing the need for registered IP addresses.
Reference: Designing Cisco Networks (Ciscopress) page 166

QUESTION 60:

In which of the following network is the IP address 136.10.63.0 a valid host address that can be assigned to a workstation?

A. 136.10.62.0 /23
B. 136.10.62.0 /24
C. 136.10.63.0 /24
D. 136.10.63.0 /25

Answer: A

Explanation:
A: Correct.
B,C,D: Incorrect, because the host address cannot consist from all zeros. The host portion of the address is 0. This could be possible if the command "ip subnet-zero" was issued, but in general it can't be.

QUESTION 61:

Which of the following fields are associated with an IPv6 packet? (Choose all that apply.)

A. Header Length
B. Payload Length
C. Header Checksum
D. Traffic Class
E. Destination Address
F. Version

Answer: B, D, E, F

Explanation:

Field	Description
Version	Similar to the Version field in the IPv4 packet header, except that the field lists number 6 for IPv6 instead of number 4 for IPv4.
Traffic Class	Similar to the Type of Service field in the IPv4 packet header. The Traffic Class field tags packets with a traffic class that is used in differentiated services.
Flow Label	A new field in the IPv6 packet header. The Flow Label field tags packets with a specific flow that differentiates the packets at the network layer.
Payload Length	Similar to the Total Length field in the IPv4 packet header. The Payload Length field indicates the total length of the data portion of the packet.
Next Header	Similar to the Protocol field in the IPv4 packet header. The value of the Next Header field determines the type of information following the basic IPv6 header. The type of information following the basic IPv6 header can be a transport-layer packet, for example, a TCP or UDP packet, or an Extension Header, as shown in Figure 9.
Hop Limit	Similar to the Time to Live field in the IPv4 packet header. The value of the Hop Limit field specifies the maximum number of routers that an IPv6 packet can pass through before the packet is considered invalid. Each router decrements the value by one. Because no checksum is in the IPv6 header, the router can decrement the value without needing to recalculate the checksum, which saves processing resources.
Source Address	Similar to the Source Address field in the IPv4 packet header, except that the field contains a 128-bit source address for IPv6 instead of a 32-bit source address for IPv4.
Destination Address	Similar to the Destination Address field in the IPv4 packet header, except that the field contains a 128-bit destination address for IPv6 instead of a 32-bit destination address for IPv4.

Reference: Implementing IPv6 for Cisco IOS Software PDF page 29

QUESTION 62:

Which of the following is NOT a step in designing Network layer addressing and naming?

A. Developing a plan for configuring user station addresses.
B. Designing a method for mapping Geographic Locations to network numbers.
C. Designing route summarization.
D. Proposing a method for mapping geographical locations to router clusters.
E. Designing a hierarchy for addressing.
F. Designing a scheme for naming servers, routers, and user stations.

Answer: D

Explanation:
Steps for Designing Network Layer Addressing
Step1: Design a Hierarchy for addressing
Setp2: Design route summarization
Step3: Design a plan for distributing administrative authority for addressing and naming at the lower levels of the hierarchy
Step4: Design a method for mapping Geographic Locations to network numbers
Step5: Develop a Plan for Identifying Special Stations such as Routers and Servers with

Specific Node IDs
Reference: Designing Cisco Networks (Ciscopress) page 170 + 171

QUESTION 63:

Which of the following protocols is responsible for IP address to MAC address resolution?

A. ARP
B. TCP/IP
C. IGRP
D. IPX
E. CDP

Answer: A

Explanation:
Address Resolution Protocol (ARP) - Allows a host to dynamically discover the MAC-layer address corresponding to a particular IP network layer address. In order for two machines on a given network to communicate, they must know the other machine's physical addresses.
Reference: Designing Cisco Networks (Ciscopress) page 16

QUESTION 64:

What is the shortest notation of the IPv6 address
1080:0000:0000:0000:0008:0000:0000:200C?

A. 1080::8::200C
B. 1080::0:8::0:200C
C. 1080:0:0:0:0008:0:0:200C
D. 1080::8:0:0:200C
E. 1080:0:0:0:8::200C
F. 1080:0:0:0:8:0:0:200C

Answer: D
IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x:x. Following are two examples of IPv6 addresses:
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:8:800:200C:417A
It is common for IPv6 addresses to contain successive hexadecimal fields of zeros. To make IPv6 addresses less cumbersome, two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros). Table 2 lists compressed IPv6 address formats.
A double colon may be used as part of the ipv6-address argument when consecutive

16-bit values are denoted as zero. You can configure multiple IPv6 addresses per interfaces, but only one link-local address.

Note Two colons (::) can be used only once in an IPv6 address to represent the longest successive hexadecimal fields of zeros. The hexadecimal letters in IPv6 addresses are not case-sensitive.

Table 2 Compressed IPv6 Address Formats

IPv6 Address Type	Preferred Format	Compressed Format
Unicast	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
Multicast	FF01:0:0:0:0:0:0:101	FF01::101
Loopback	0:0:0:0:0:0:0:1	::1
Unspecified	0:0:0:0:0:0:0:0	::

The loopback address listed in Table 2 may be used by a node to send an IPv6 packet to itself. The loopback address in IPv6 functions the same as the loopback address in IPv4 (127.0.0.1).

Reference: Implementing IPv6 for Cisco IOS Software PDF page 20 + 21

QUESTION 65:

You are a network technician at Certkiller . Certkiller 's IP addressing requirements exceed the public class C address range assigned to the company. Therefore, you have implemented private addressing. You now want to provide all Certkiller users with simultaneous access to the Internet.
Which mechanism would allow you to do this?

A. Translate using static NAT.
B. Translate using dynamic NAT.
C. Implement VLANs.
D. Secondary IP network.
E. None of the above.

Answer: B

Explanation:
Cisco Support NAT features include the following:
* Static translation
* Dynamic source address translation - Establishes a dynamic mapping between the inside local and global addresses. This is accomplished by describing the local addresses to be translated, the pool of addresses from which to allocate global addresses, and associating the two. The router will create translation as needed.
* Address overloading
* TCP load distribution
Reference: Designing Cisco Networks (Ciscopress) page 167

QUESTION 66:

Which of the following does not fall within an IPv6 address scope?

A. Unicast
B. Broadcast
C. Anycast
D. Multicast
E. None of the above.

Answer: B

Explanation:

Table 2   Compressed IPv6 Address Formats

IPv6 Address Type	Preferred Format	Compressed Format
Unicast	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
Multicast	FF01:0:0:0:0:0:0:101	FF01::101
Loopback	0:0:0:0:0:0:0:1	::1
Unspecified	0:0:0:0:0:0:0:0	::

The loopback address listed in Table 2 may be used by a node to send an IPv6 packet to itself. The loopback address in IPv6 functions the same as the loopback address in IPv4 (127.0.0.1).
Reference: Implementing IPv6 for Cisco IOS Software PDF page 20 + 21

QUESTION 67:

Your newly appointed Certkiller trainee wants to know how IPv6 manages to achieve subnetworking.
What will your reply be?

A. Subnetworks are assigned by Public Authorities such as Internet Service Providers
B. Subnetworking is not permitted in IPv6
C. Site Level Aggregator in IPv6 addresses
D. IPv4 compatible IPv6 addresses
E. All of the above

Answer: C

Explanation:
The aggregatable global address typically consists of a 48-bit global routing prefix and a 16-bit subnet ID or Site-Level Aggregator (SLA). In the IPv6 aggregatable global unicast address format document (RFC 2374), the global routing prefix included two other hierarchically structured fields named Top-Level Aggregator (TLA) and Next-Level Aggregator (NLA).The IETF decided to remove the TLS and NLA fields form the RFCs because these fields are policy-based. Some existing IPv6 networks deployed before the change might still be using networks based on the older architecture.
A 16-bit subnet field called the Subnet ID could be used by individual organizations to create their own local addressing hierarchy and to identify subnets. A subnet ID is similar to a subnet in IPv4, except that an organization with an IPv6 subnet ID can support up to

65,535 individual subnets.
Reference: Implementing IPv6 for Cisco IOS Software Page 22

QUESTION 68:

Which statement represents an accurate description of IPv6 address route summarization?

A. IPv6 addresses must be converted to IPv4 addresses to facilitate router summarization
B. IPv6 address have default router summarization abilities based on Top level aggregators, Next Level aggregators and Site Level aggregators
C. Classless inter domain routing (CIDR) for IPv6 perform route summarization by default
D. IPv6 address is unable to use route summarization
E. The routers in the IPv6 network use proprietary protocols to optimize router summarization based on the size of their routing tables

Answer: B

Explanation:
In addition to required protocols, infrastructure address space needs to be identified since this is the space the ACL will be protecting. Infrastructure address space includes any addresses that are used for the internal network and should rarely, if ever, be accessed by external sources such as router interfaces, point-to-point link addressing and critical infrastructure services. Since these addresses will be used for the destination portion of the infrastructure ACL, summarization is critical and, wherever possible, these addresses should be grouped into classless interdomain routing (CIDR) blocks.
Reference:
http://www.cisco.com/en/US/tech/ CK6 48/ CK3 61/technologies_white_paper09186a00801a1a55.shtml

QUESTION 69:

What impact does IPv6 have on the BGP protocol?

A. There is a new version of BGP for IPv6
B. Hosts convert BGP to IS-IS for IPv6
C. Routers convert BGP to IS-IS for IPv6
D. There is no change to BGP for IPv4 and IPv6
E. BGP cannot be used with IPv6

Answer: A

Explanation:
When IPv6 is first implemented in a network, it will co-exist with a larger IPv4 network. During this transition period, using tunnels is a method to allow IPv6 and IPv4 networks to exist at the same time. A method to connect various IPv6 locations throughout a

company network is to tunnel the IPv6 through the IPv4 network.
Reference:
http://www.cisco.com/en/US/tech/ CK8 28/ CK3
63/technologies_configuration_example09186a00800b49a5.shtml

QUESTION 70:

Which strategy allows IPv4 and IPv6 address schemes to coexist and facilitates a
migration from IPv4 to IPv6? (Select one.)

A. A bridge between the IPv6 and the IPv4 networks.
B. Deploy stateless addressing assignments.
C. Run Ipv6 and Ipv4 stacks on all devices.
D. Enable anycast capability in the routing protocol

Answer: C
Explanation
IPv4 to IPv6 Transition Strategies and Deployments
Several deployment models exist to migrate from an IPv4 network to IPv6. During a
transition time, both protocols can coexist in the network. The deployment models are
- IPv6 over dedicated WAN links
- IPv6 over IPv4 tunnels
- IPv6 using dual-stack backbones
- Protocol translation
Source: CCDA Exam Certification Guide Second Edition, Page 253

QUESTION 71:

Which of the following statements describe the use of Dynamic Host Configuration
Protocol (DHCP) for the assignment of Ipv6 addresses?

A. DHCP is one of the ways for dynamic Ipv6 address assignment.
B. DHCP is the only way for dynamic Ipv6 address assignment.
C. DHCP cannot assign Ipv6 addresses.
D. DHCP servers can only assign Ipv4 compatible Ipv6 addresses.
E. DHCP servers can only assign Ipv4 mapped Ipv6 addresses.

Answer: A

Explanation: An IPv6 host can obtain its address through autoconfiguration or
from the DHCP.
Source: CCDA Exam Certification Guide Second Edition, Page 251

QUESTION 72:

You are a network administrator at Certkiller and have been instructed to propose a

network design. The Certkiller IT manager wants you to describe route summarization to the trainees.
Which of the following statements would you use to describe route summarization as best possible?

A. Using one Class A IP address to reduce routing table size in the routers.
B. Grouping multiple contiguous networks and advertising as one large network.
C. Rendering the use of subnetworks obsolete will enhance routing performance.
D. Advertising a singular IP network to simplify routing table maintenance.
E. Load sharing between the organization's routers and the ISP's routers.

Answer: B

QUESTION 73:

Certkiller .com is an international corporation whose network consists of more than 2,000,000 hosts and more than 10,000 routers internally. There is connectivity to the Internet and high volumes of traffic with business partners and the general public is at the order of the day. A decision was taken to start employing IPv6.
Which of the following statements would best describe a flexible IPv6 strategy for this international corporation?

A. IPv4 hosts with IPv6 routers.
B. Dual stack hosts with dual stack routers
C. Ipv6 hosts with Ipv6 routers
D. Dual stack hosts with Ipv4 routers
E. Ipv6 hosts with Ipv4 routers

Answer: B

Explanation: B is the best answer, because note that the question says the company uses Internet access and do high volumes of traffic with their business partners. It's only internally that they're migrating to IPv6, so they should use dual-stack hosts and routers. Another suitable answer might be IPv6 host and dual-stack routers (since they'll use IPv6 internally but IPv4 externally) but no such option is available.

QUESTION 74:

Study the Exhibit below carefully:
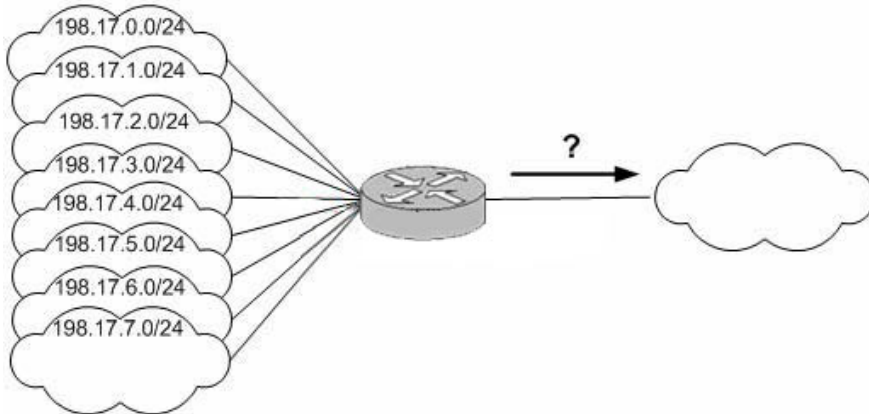
Illustrated above is a router that is summarising the networks on the left as it advertises them to the singular network on the right. Which summarization route will be advertised?

A. 198.17.0.0/21
B. 198.17.0.0/22
C. 198.17.0.0/24
D. 198.17.0.0/26
E. 198.17.0.0/27

Answer: A

Explanation:
Advertised would be the network address which consists of bits, which are common for all networks. Hence, here it is 198.17.0.0/21

QUESTION 75:

You are a network administrator at Certkiller and have been instructed to provide the new tenant in your building with a unique VLAN. There are two other workgroups with 80 users respectively present at this site.
Both these groups have a subnet out of a Class B address with a subnet mask of 255.255.255.128
The new tenant will start with 18 users with the potential to move up to 24 users.
EIGRP is routing protocol in use.
To assure efficient IP addressing that will satisfy the new tenants' requirements which subnet mask will you use?

A. 255.255.255.128
B. 255.255.255.192
C. 255.255.255.224
D. 255.255.255.240

Answer: C

Explanation:
The mask 255.255.255.224 uses 27 bits for the network part of the address. So, 32-27=5
bits is left for the host address. 2^5=32 in each network. 5 bits is a minimum of bits
needed to support 18 hosts (4 bits can support only 2^4=16<18 hosts).

QUESTION 76:

Which Ipv6 address type achieves the same purpose as an IPv4 range of private IP
addresses, where organizations can use it freely without having to consult with any
external IP address assigning authority?

A. Global Aggregatable IPv6 addresses
B. Ipv4 mapped Ipv6 addresses
C. Site Local addresses
D. Anycastaddresses
E. Link Local addresses
F. Unicast addresses

Answer: C

Explanation:
IPv6 site-local addresses are equivalent to IPv4 private addresses.
Source: CCDA Exam Certification Guide Second Edition, Page 544

QUESTION 77:

Your Certkiller trainee Jack asks you what effect does IPv6 have on the RIP
protocol. What should you tell her?

A. There is a new version of RIP for IPv6
B. RIP cannot work with IPv6
C. Routers convert RIP routes to IPv6
D. There is no change for RIP for IPv6
E. IS-IS can be used to convert RIP routes for IPv6

Answer: A
RIPng for IPv6 : RFC 2080 describes changes to the RIP to support IPv6 networks, called RIP
next generation (RIPng). RIP mechanisms remain the same. RIPng still has a 15-hop limit,
counting to infinity, and user User Datagram Protocol (UDP) port 521. RIPng version supports
IPv6 addresses and prefixes. Cisco IOS Software currently supports RIPng.
Reference : Page 252 of CiscoPress - CCDA 640-861 2nd Edition.

QUESTION 78:

Certkiller company store has internal network connecting their stores to two
locations, namely: Head office and backup site. They do mainly file transfer and use

private addressing 10.0.0.0/8. They want to provide E-commerce services by connecting their two main sites to the ISP. Four E-Commerce servers (Two in the head office and two in the backup site) will be accessible by public. No other inbound public access and outbound public access will be allowed. Their ISP assigned Class C subnet for their server is 201.13.6.136 /29. In setting up router connecting to the ISP (one in the head office and one in the backup site) what routing advertisements would be sent by their two routers to ISP?

A. Route 201.13.6.136/30 and 201.13.6.140/30
B. Route 201.13.6.136/29 and 10.0.0.0/8
C. Route 10.0.0.0/8
D. Address translation will be required to advertise active routes to ISP
E. No route advertisement are sent
F. proxy server will be configure static route and will only response route request to by ISP

Answer: A
Each network form each router must be sent to ISP to have a valid introduction.
Nat is nonsense answer because NAT does not advertise to anyone.

QUESTION 79:

How many bits are there in between each colons ":" in an IP V6 environment?

A. 4
B. 8
C. 16
D. 32
E. 64

Answer: C
CCDA Exam Certification Guide Second Edition
Page 241: For display, the IPv6 addresses have eight 16-bit groups.

QUESTION 80:

Which of the following descriptions are features of the basic IPV6 header? (Choose two.)

A. It carries the full 128 bit source and destination IP address.
B. It makes fragmentation performed at routers easier.
C. It is twice as big as an IPv4 header, 40 octets.
D. It is always encrypted and hence is more secure than IPv4.
E. It allows IPv6 datagram to go through more hops, router than IPv4

Answer: A, C

CCDA Exam Certification Guide Second Edition
Page 240 The use of 128 bits for source and destination addresses provides a significant improvement over IPv4.
Page 241 Notice that although the IPv6 address if four times the length of an IPv4 address, the IPv6 header is only twice the length.

QUESTION 81:

Why would you advice the Certkiller trainee to segment each area into continuous block of addresses when designing an IP address scheme for Inter-Area connectivity?

A. To Control Route cost
B. For the purposes of Route Aggregation
C. To Reduce Address assignment
D. To Accommodate future move to IPv6

Answer: B

QUESTION 82:

Which of the following characteristics are associated with IPv6 addresses? (Choose three.)

A. Colons (::) are used to represent successive hexadecimal fields of zero
B. Colons (::) are used to separated fields of zero
C. Leading zeros are required
D. Leading zeros may be omitted
E. An IPv6 node requires more than one IP address.
F. There are only four major type IPv6: Unicast, Multicast, Anycast & Broadcast

Answer: A, B, D

QUESTION 83:

A network design includes private addressing, but there is a need for several network devices to be assigned a unique public address for access from the internet. Which of the following techniques will satisfy this requirement?

A. Static NAT
B. DHCP
C. Dynamic NAT
D. VPN tunneling

Answer: A
The devices need static IP addresses.

QUESTION 84:

The Certkiller administrator is assigned the task of providing a unique VLAN for the sales group that is moving into an existing building. There are presently two other workgroups in this building with 82 users each. Both of these groups have a subnet within a private class B address with a 255.255.255.128 mask. The sales group initially has 30 users, with a potential for growth to 52 users. The network uses RIPv1 routing protocol.
Which subnet mask should be used for this new sales VLAN?

A. 255.255.255.128
B. 255.255.255.192
C. 255.255.255.224
D. 255.255.255.240

Answer: A

Explanation:
The last line in the question states the Network uses RIPv1 routing protocol and the other two network subnet masks are 255.255.255.128, the answer here has to be A because RIPv1 is a classful routing protocol and all the subnets have to have the same subnet mask.
Not B: Answer B only addresses the first part of this question, but fails the classful issues with RIPv1.

QUESTION 85:

Which IPv4 to IPv6 transition strategy makes use of an intermediate device that can translate either at the transport layer or the network layer?

A. dual-stack
B. DSTM
C. NAT-PT
D. tunneling
E. automatic

Answer: C

Explanation:
Not D:
With tunneling Ipv6 traffic is encapsulated within ipv4 packets so that they are sent over the Ipv4 WAN. The advantage of this method is that you do not need separate circuits to connect the ipv6 networks. The disadvantage of this method is the increased protocol overhead of he encapsulated ipv6 headers.
Reference: Cisco CCDA self-study v2 (Page 285), Knowlednet Design cap. 5.67

QUESTION 86:

For which of the following devices would static DNS entry be a necessity?

A. DHCP server
B. Default gateway
C. Border router
D. E-mail server
E. None of the above

Answer: D

Explanation:
Email servers are used to send and receive the emails. When the user wants to send the email for example on address aaa@ Certkiller .com, the email server would need the help of DNS to resolve the name Certkiller .com to the normal IP address. Then the email server will send the message.

QUESTION 87:

Under which circumstances would you recommend static IP addressing?

A. When a given number of IP addresses are expected to change.
B. When a variable number of IP addresses are required per subnet.
C. When a given number of each IP addresses need to be reserved for distribution to dial-in clients
D. When it is desirable to administratively track a given number of IP addresses.

Answer: D
Not C: Remote dial-in users can dynamically be assigned IP address from an address pool.

QUESTION 88:

The newly appointed Certkiller trainee wants to know for which of the following environments static routing would be most appropriate. What would your reply be? (Choose two)

A. Smaller expanding networks
B. Stub networks
C. Noncritical hosts
D. Single-homed ISP connection
E. Larger expanding networks

Answer: B, D

QUESTION 89:

Certkiller is designing a worldwide IPv6 network with duplicate file servers at multiple locations. Each file server contains identical reference information.
Which IPv6 address type would be used to allow end stations to send a request to the nearest file server using the same destination address regardless of the location of the end station?

A. Unicast
B. Anycast
C. Multicast
D. Broadcast

Answer: B

Explanation:
The IPv6 addressing scheme has been developed to be compatible with the current IPv4 addressing standard, which allows the new IPv6 networks to coexist with IPv4 networks. IPv6 increases the size of the address space from 32 bits to 128 bits, which provides 40,282, 366,920, 938,463, 463,374, 607, 431, 768 ,211,456, or 3.4 × 1038, addresses. IPv6 also improves routing, security, and quality of service (QoS) features, while simplifying the IP header.
An IPv6 anycast address is a global unicast address that is assigned to many interfaces in different devices on the network. This means that this same network address is assigned to more than one interface on the network. A packet that is sent to an anycast address will be delivered to the closest interface with that anycast address. The closest interface is determined by the routing protocol being used. Because anycast addresses are global unicast addresses, there is no way to tell that a global unicast address is also an anycast address

QUESTION 90:

Given the fact that IPv6 addresses are represented as a series of hexadecimal fields separated by colons (:); how many bits are in each hexadecimal field?

A. 4
B. 8
C. 16
D. 32
E. unlimited

Answer: C

Explanation:
Unlike the usual dotted-decimal format of the IPv4 address, IPv6 is represented by

hexadecimal numbers. A hexadecimal number is equivalent to four bits, also known as a nibble because it is half a byte, and is numbered 0-9 and A-F. A represents 10 and F represents 15, and they are not case-sensitive. The IPv6 address is a 32-digit hexadecimal numeric value, in eight four-digit clusters, known as fields, separated by colons (:), representing the 128-bit address. Here is an example of a valid IPv6 address: 1041:0000:130B:0000:0000:09C0:586C:1305.

There are some techniques used to shorten the IPv6 address. One of these techniques is to omit leading 0s in the address field, so 0000 can be compressed to just 0 and 09C0 can be compressed to 9C0. You can omit leading 0s but not trailing 0s. The previous IPv6 address example could be shortened to 1041:0:130B:0:0:9C0:586C:1305. Another technique is to use double colons (::) to represent a contiguous block of 0s. Again, the previous IPv6 address can be further shortened to 1041:0:130B::9C0:586C:1305. For some IPv6 addresses, this technique can really shorten the address. For example, the IPv6 address FF01:0:0:0:0:0:1 can be compressed to FF01::1. There is a limitation in using double colons on the address. You can use it only once in any address, because if two double colons are placed in the same address, there will be no way to identify the size of each block of 0s.

QUESTION 91:

Certkiller is migrating from IPv4 to IPv6. IP addresses are assigned to workstations using DHCP.
Which of the following options can be taken into consideration when assigning addresses to workstations using IPv6? (Choose three)

A. Manual configuration
B. Distributed address resolution
C. Link local address
D. DHCPv6
E. DNS server

Answer: A,C,D

Explanation:
Not E: DNS server is more for resolution issues and its isnt what the question is asking.
Address autoconfiguration - This capability provides for dynamic assignment of IPv6 address. IPv6 hosts can automatically configure themselves, with or without a Dynamic Host Configuration Protocol (DHCP) server.

QUESTION 92:

What is the shortest notation of IPv6 address
2080:0000:0000:0000:0008:0000:0000:200C?

A. 2080::8::200C
B. 2080::0:8:0:0:200C

C. 2080:0000:0000:0000:0008:0000:000:200C
D. 2080::8:0:0:200C
E. 2080:0:0:0:8::200C
F. 2080:0:0:0:8:0:0:200C

Answer: D

Explanation:
According to RFC 1884, there are three conventional forms for representing IPv6 addresses as text strings:
1. The preferred form is x:x:x:x:x:x:x:x, where the 'x's are the hexadecimal values of the eight 16-bit pieces of the address.
Examples:
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:8:800:200C:417A
Note that it is not necessary to write the leading zeros in an individual field, but there must be at least one numeral in every field (except for the case described in 2.).
2. Due to the method of allocating certain styles of IPv6 addresses, it will be common for addresses to contain long strings of zero bits. In order to make writing addresses containing zero bits easier a special syntax is available to compress the zeros. The use of "::" indicates multiple groups of 16-bits of zeros. The "::" can only appear once in an address. The "::" can also be used to compress the leading and/or trailing zeros in an address.
For example the following addresses:
1080:0:0:0:8:800:200C:417A a unicast address
FF01:0:0:0:0:0:0:43 a multicast address
0:0:0:0:0:0:0:1 the loopback address
0:0:0:0:0:0:0:0 the unspecified addresses
may be represented as:
1080::8:800:200C:417A a unicast address
FF01::43 a multicast address
::1 the loopback address
:: the unspecified addresses
3. An alternative form that is sometimes more convenient when dealing with a mixed environment of IPv4 and IPv6 nodes is x:x:x:x:x:x:d.d.d.d, where the 'x's are the hexadecimal values of the six high-order 16-bit pieces of the address, and the 'd's are the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation). Examples:
0:0:0:0:0:0:13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38
or in compressed form:
::13.1.68.3

::FFFF:129.144.52.38
Reference: http://www.faqs.org/rfcs/rfc1884.html

QUESTION 93:

Why would a Certkiller network designer recommend variable-length subnet masking for a network?

A. to minimize convergence time
B. to increase security and availability
C. to suit the flat structure of the network
D. to accommodate a mixed vendor environment
E. to implement classless routing

Answer: E

Explanation:
Classless Inter-Domain Routing (CIDR), introduced starting in 1993, is the latest refinement to the way IP addresses are interpreted. It replaced the previous generation of IP address syntax, classful networks. It allowed increased flexibility when dividing ranges of IP addresses into separate networks.
A subnet mask is a bitmask which shows where the network address ends and the host address begins. CIDR uses variable length subnet masks (VLSM) to allocate IP addresses to subnets according to individual need, rather than some general network-wide rule. Thus the network/host division can occur at any bit boundary in the address. The process can be recursive, with a portion of the address space being further divided into even smaller portions, through the use of masks which cover more bits.
Because the normal class distinctions are ignored, the new system was called classless routing. This led to the original system being called, by back-formation, classful routing.

QUESTION 94:

DRAG DROP

Several factors determine whether to apply static or dynamic IP addresses.
Drag the factor on the left to the IP address assignment method that is
easiest to apply

More than 30 end systems
High availability
Renumbering likely with numerous systems
Security
Address tracking
Additional parameters

Static address assignment

Place here
Place here
Place here

Dynamic address assignment

Place here
Place here
Place here

Answer:

Several factors determine whether to apply static or dynamic IP addresses.
Drag the factor on the left to the IP address assignment method that is
easiest to apply

Static address assignment

High availablity
Security
Address tracking

Dynamic address assignment

More than 30 end systems
Renumbering likely with numerous systems
Additional parameters

QUESTION 95:

Certkiller has received its IPv6 address range from their Internet Service Provider
and intend to use only IPv6 internally. Certkiller .com will access the Internet
through port address translation (PAT).
Based on this information, what is a requirement for their Domain Name Servers?

A. They no longer need DNS servers.
B. Their DNS servers need to support both IPv4 and IPv6 addresses.
C. Their DNS servers need to support only IPv6 addresses.
D. Their DNS servers need to support only IPv4 addresses.
E. They need additional DNS servers in their network just for IPv6 addresses.
F. There are no changes required to their DNS servers.

Answer: B

Explanation:
Since Certkiller plans on using IPv6 internally, including the internal DNS servers, they will need to support IPv6 since the actual IP address assigned to the physical servers will be an IPv6 address. They will also need to support classical IPv4 addresses, because the servers will be translating domain names to external IPv4 IP addresses.

QUESTION 96:

Study the IP table shown below:
192.128.168.0
192.128.169.0
192.128.170.0
192.128.171.0
192.128.172.0
192.128.173.0
192.128.174.0
192.128.175.0
What is the route address that correctly summarizes all eight routes shown above?

A. 192.128.0.0/24
B. 192.128.171.128/3
C. 192.128.168.0/21
D. 192.128.175.0/3
E. 192.128.0.0/16

Answer: C

Explanation:
On very large networks, there may be hundreds or even thousands of individual networks and subnetworks being advertised. All these routes can be very taxing on a router's memory and processor. For example, routers on the Internet were starting to be overwhelmed with a couple of hundred thousand routes. After summarizing routes and using CIDR, the number of routes has been dramatically reduced.

Table 2.11: Summary Example	
IP Network Address	**Binary Equivalent**
172.16.100.0	**10101100.0001000.0110**0100.0
172.16.101.0	**10101100.0001000.0110**0101.0
172.16.102.0	**10101100.0001000.0110**0110.0
172.16.103.0	**10101100.0001000.0110**0111.0
172.16.104.0	**10101100.0001000.0110**1000.0
172.16.105.0	**10101100.0001000.0110**1001.0
172.16.106.0	**10101100.0001000.0110**1010.0

Examine the table to determine the maximum number of bits (starting from the left) that all of the addresses have in common. (Where they are lined up, we boldfaced them to make them easier for you to see.) The number of common bits is the prefix length for the summarized address (/20).

In this example, we can see from the table that all of the addresses have the first 20 bits in common. The decimal equivalent of these first 20 bits is 172.16.96.0. So, we can write our new summarized address as 172.16.96.0/20. If we were to later add a network 172.16.98.0, it would need to be behind the router summarizing this address space. If we didn't, it could cause problems.

QUESTION 97:

What are the advantages of using static routes? (Choose all that apply.)

A. More efficient use of router resources.
B. Increased security.
C. A single path to and from a network.
D. Route calculations made by network administrators.
E. None of the above.

Answer: A, B

Explanation:
A: Administrator manually programmed the route and update this entry whenever a network topology changed. It will not consume router's CPU and use fixed memory.
B: Static route is Private and by default it is not conveyed to other routers as part of an update process.
Reference: CCDA Study guide by Damon Merchant. Syngress Press
Incorrect Answers
C: It is not an advantage
D: No Route calculations performed for static route .When configuring the static routes one can specify either the next hop address that the packet will take or the packet to route out an interface. Both methods work properly.

QUESTION 98:

Which of the following features characterize routing protocols? (Choose all that apply.)

A. Operates at the highest layer of the OSI reference model.
B. Upper-layer protocols existing in a given protocol suite.
C. Operates at the Data-Link Layer of the OSI reference model.
D. Responsibility for path determination and traffic switching.
E. Operates at the Network Layer of the OSI reference model.

Answer: D, E

Explanation:
D: Routing protocols make routers work together. Routers keep track of the networks they are directly connected to, as well as other routers on the networks in order to forward packets to foreign networks. A router maintains this info in its routing table and periodically shares information from that table to other routers on the network. This info is used to determine the best route for an incoming packet to take its destination.
E: Routing protocols operate at the Network Layer of the OSI model.
Reference:
CCDA Study guide by Damon Merchant. Syngress Press
Incorrect Answers
A: It operates at the Network Layer (Layer 3) of the OSI model.
B: They operate at Layer 3. It will not use upper layer protocols.
C: Routing protocols operates network layer instead of session layer.

QUESTION 99:

Which of the following routing protocols have high speed convergence? (Choose all that apply.)

A. EIGRP
B. BGP
C. OSPF
D. RIPv2
E. IS-IS
F. IGRP
G. All of the above.

Answer: A, C, E

Explanation:
IS-IS and OSPF are link state protocols. It converges quickly because updates are sent not periodically, but only when changes occur. The routing changes are flooded, and computing is accomplished in parallel. EIGRP is Hybrid protocol. It uses DUAL algorithm to achieve rapid convergence across a network
Reference:
Incorrect Answers
D: RIP V2 sends updates periodically. It converges slowly.
F: IGRP also sends updates periodically. It converges slowly
G: This option is not valid.

QUESTION 100:

You work as a network consultant. Certkiller is expanding into a multinational organization and has contracted you to assist them with planning a new network design. You recommend that Certkiller use a routing protocol that will support a network design that cannot be structured into a hierarchy.

Which of the following routing protocol would you recommend?

A. OSPF
B. EIGRP
C. AARP
D. IS-IS
E. GRP

Answer: B

Explanation:
EIGRP can support a network design that cannot be structured into a hierarchy.
Incorrect answers:
A: OSPF is oriented on networks which are structured into a hierarchy. All OSPF areas in the network should connect to Area 0.
D: IS-IS is also oriented on networks which are structured into a hierarchy.L2,L1 areas.
C,E: AARP and GRP are not routing protocols.

QUESTION 101:

You are a network consultant. You are contracted by Certkiller , Inc to design a new network for the company. The IS Manager at Certkiller informs you that the company is considering a hub and spoke topology with links that will be low bandwidth and rarely changing routes.
Which of the following should you recommend?

A. Static Routing
B. Dynamic Routing
C. IGRP
D. RIP-2
E. AARP

Answer: A

Explanation:
Administrator manually programmed the route and updates this entry whenever a network topology changed. It will not consume router's CPU and use fixed memory. Static route is Private and by default it is not conveyed to other routers as part of an update process.
Incorrect Answers
B: Dynamic routing uses more CPU resources. Not required for low bandwidth routes
C,D: Both are dynamic routing protocols. Consume more router resources.
E: AARP is Apple Talk Address Resolution Protocol. This will not play any role in determining routes.

QUESTION 102:

What are the advantages of having classless routing protocols for a network?

A. Minimize convergence time.
B. Increase security.
C. Accommodating various and mixed vendor environment.
D. Support variable length subnet masking.
E. More availability.

Answer: D

Explanation:
Classless routing protocols carry Variable subnet masking details in Routing updates.
This is Main Advantage compared to class routing protocols like RIP & IGRP
Incorrect Answers
A: It is Second advantage in classless routing protocol
B, C, E: Not specific advantages

QUESTION 103:

Which of the following metrics can the IGRP protocol use when making routing decisions? (Choose all that apply.)

A. Bandwidth
B. Hops
C. Reliability
D. Fault Tolerance
E. Link Cost

Answer: A, C

Explanation:
IGRP is a distance vector interior gateway protocol and uses combination of metrics;
internetwork delay, bandwidth, reliability, and load are all factored into the routing
decision.
Reference: Designing Cisco Networks (Ciscopress) page 189

QUESTION 104:

You are contracted as a network administrator for a small company, Certkiller Inc.
that employs variable length subnet masking (VLSM) in their network.
Which of the following routing protocols would be suitable for the Certkiller
network? (Choose all that apply.)

A. OSPF

B. RIPv1
C. EIGRP
D. RIPv2
E. IGRP
F. All of the above

Answer: A, C, D

Explanation:
Enhanced Interior Gateway Routing Protocol (EIGRP)
1. Classless addressing (prefix based)
2. Variable length subnet mask (VLSM)
3. Address summarization
4. Route filtering
5. Periodic and incremental updates
RIP v2:
1. Classless addressing (prefix based)
2. VLSM
3. Triggered updates
4. Full routing-table updates
Open Shortest Path First (OSPF):
1. Hierarchical scaling (two levels)
2. VLSM
3. Address summarization
4. Stub areas
5. Incremental updates
6. Per-area topology database
7. Dijkstra's shortest path first algorithm (SPF)
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ios_abcs_ios_networking_the_enterprise0900aecd800a4e11.
h

QUESTION 105:

Certkiller Electronics has in more than of 1000 small outlets scattered around the
country. These outlets accommodate the needs of electronic and PC enthusiasts. On
average each outlet sports twenty computers and requires interconnection to the
head office and to a regional office using a router and frame relay network.
Which of the following routing protocols would be most suitable for a design that
should cater for the needs of Certkiller Electronics? (Choose all that apply.)

A. IBGP
B. OSPF
C. BGP
D. EIGRP
E. RIPv2

F. IGRP

Answer: B, D

Explanation:
B,D are correct.
Incorrect answers:
A,C: This are EGP routing protocols. They are used for routing between autonomous systems.
E,F: This are routing protocols for small networks. Ripv2 supports the networks with not more then 15 routers in diameter and IGRP with not more then 255. In this scenario there would be more then 1000 routers so this protocols don't pass.

QUESTION 106:

With regard to routing protocols, which of the following statements is true?

A. Routing protocol convergence time is determined by Enhanced IGRP.
B. Routing protocol convergence time is affected by the data link-layer technology in use.
C. Routing protocol convergence time is the same for distance vector protocols and link-state protocols.
D. Routing protocol convergence time includes the time to detect a fault, but not time to determine a new route.

Answer: B

Explanation:
The convergence time is affected by the data link-layer technology in use. The speed of packets traversing the network and the timers of routing protocols depend on layer 2 technology. In such a way a convergence time depends on data link-layer technology.
Incorrect answers:
A: EIGRP is a separate routing protocol. The convergence time of other routing protocols doesn't depend on EIGRP.
C: The convergence time of link-state protocols is faster then distance vector protocols convergence time.
D: It includes the time to determine a new route.

QUESTION 107:

You are the technician at Certkiller and received an instruction to choose a routing protocol for a network design. You are aware that you must keep in mind IP addressing limitations.
Which of the following IP addressing constraints do classful routing protocols have? (Choose all that apply.)

A. fixed length subnet masking
B. variable length subnet masking
C. no private addressing support
D. subnetted networks must be contiguous
E. all of the above

Answer: A, D

Explanation:
Classful routing protocol - do not transmit any information about the prefix length.
When receiving information about routes within the same major network, hosts and
routers assume the same prefix length as that on the incoming interface of the route
information. Classful routing protocols therefore do not accommodate different prefix
lengths being used within a major network.
Reference: Designing Cisco Networks (Ciscopress) page 161

QUESTION 108:

How does IPv6 impact on OSPF protocol?

A. Hosts convert OSPF to IS-IS for IPv6
B. There is a new enhanced version of OSPF for IPv6
C. Routers convert OSPF to IS-IS for IPv6
D. There is no change in OSPF between IPv4 and IPv6
E. None of the above

Answer: B

Explanation:
OSPF is a routing protocol for IP. It is a link-state protocol, as opposed to a
distance-vector protocol. Think of a link as being an interface on a networking device. A
link-state protocol makes its routing decisions based on the states of the links that
connect source and destination machines. The state of a link is a description of that
interface and its relationship to its neighboring networking devices. The interface
information includes the IPv6 prefix of the interface, the network mask, the type of
network it is connected to, the routers connected to that network, and so on. This
information is propagated in various types of link-state advertisements (LSAs).
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6/ipv6imp/sa_ospf
3

QUESTION 109:

You are the only experienced network engineer for a small independently owned
chain of companies, Certkiller Inc. The CEO wants to have all the offices
interconnected to the head office due to most IT personnel being based at the head

office. Certkiller wants a simple network topology where branch offices are to
connect to regional offices and regional offices will connect to the head office.
The headquarters consists of a large campus. To be cost effective, the CEO does not
want redundant links. Also, they want maximum throughput for the branch offices
and little or no overhead traffic.
Which routing option would you suggest for the small office?

A. Dynamic routing distance vector protocol
B. Static routing protocol
C. Dynamic routing, hybrid protocol
D. Variable length subnetwork masking protocol
E. Multi protocol label switching protocol

Answer: B

QUESTION 110:

You are contracted as a network administrator for a large company, Certkiller Inc.
and manage a large Metropolitan Area Network that stretches over 25 locations
around the city. The CEO has decided to publish a monthly webcast for all company
employees showcasing the latest product and company news.
Your greatest concern now is the performance of the network when all the
employees connect to this audio/video stream. And thus decide to enable multicast
on the network.
Which of the following Layer two features on Cisco switches will allow you to enable
and optimize multicast on the network?

A. IGMP Snooping
B. Express Forwarding
C. CGMP
D. RGMP
E. RSTP

Answer: A, C

Explanation:
When campus LANs use multicast media, end hosts that do not participate in multicast
groups might get flooded with unwanted traffic. Two solutions are
- CGMP
- IGMP snooping
Source: CCDA Exam Cerification Guide Second Edition, Page 103

QUESTION 111:

Which of the following routing protocols would you consider as suitable for a
network that uses VLSM?

(Choose all that apply.)

A. RIPv2B. OSPFC. TFTP
D. RIPv1
E. EIGRPF. IGRP
G. BGP

Answer: A, B, E

QUESTION 112:

Which of the following routing protocols would you consider when you design a
network with a classless routing protocol?
(Choose all that apply.)

A. RIPv1
B. EIGRP
C. SNMP
D. OSPF
E. IGRP

Answer: B, D

Explanation:
Classless routing protocols are:
1) RIPv2
2) OSPF
3) EIGRP
4) IS-IS
5) BGP
Reference: cisco press CCDA exam certification guide second edition p.273

QUESTION 113:

Which of the following routing protocols would you regard as ideal for a large
company that has multi-vendor routers around the globe organized in a hierarchical
structure?

A. BGP
B. EIGRP
C. OSPF
D. RIPv2

Answer: C

Explanation:

OSPF can support very large networks with hierarchical structure. OSPF is an open standard, so OSPF can be used for networks with multi-vendor routers.
Incorrect answers:
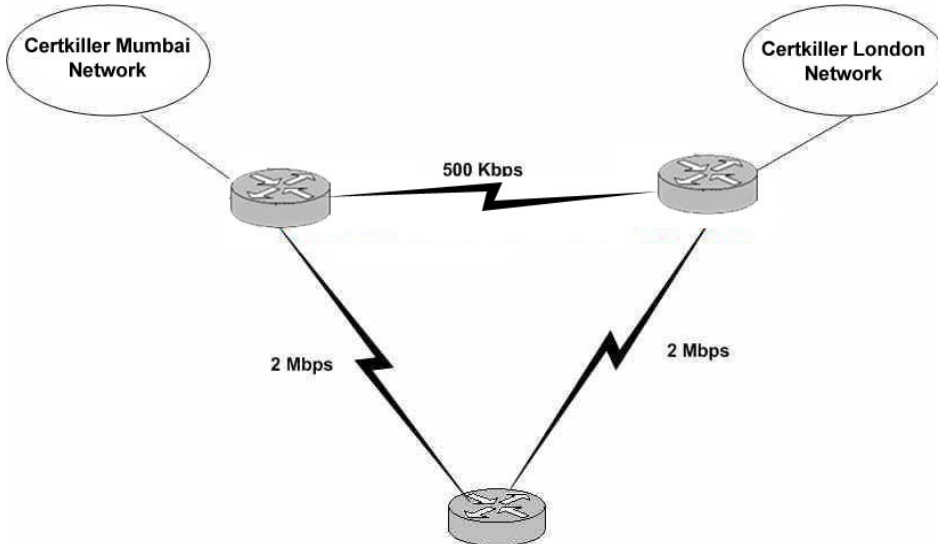A: BGP is Exterior Gateway Protocol, it is used to route between autonomous systems.
B: EIGRP is Cisco proprietary protocol
D: RIPv2 can support only small networks.

QUESTION 114:

Exhibit

Based on Exhibit , if traffic were to be routed from Certkiller Mumbai Network to Certkiller London Network y the best path (based on bandwidth).
Which is the best routing protocol that should be used on the routers?

A. RIPv2
B. IGRP
C. EIGRP
D. OSPF
E. BGP

Answer: C

Explanation: Because EIGRP supports unequal cost load balancing.

QUESTION 115:

The large organization Certkiller has made several acquisitions. each with its own network. All network use only Cisco systems equipment and IP address do not overlap. The organization doesn't desire to redesign the address space to support hierarchical design
Which routing protocol would be most suitable connect the entire network

A. BGP
B. IS-IS
C. IGRP
D. EIGRP
E. OSPF

Answer: D

QUESTION 116:

Certkiller , a large manufacturing company, wants performance improvements in the enterprise edge functional area of its network. Only Cisco routers are used in Enterprise Edge functional area of various sites. Certkiller Staff is very familiar with IETF protocol. Rapid convergences is a requirement for the new design
Which two routing protocols can be considered for the new design? Select two.

A. RIPv1
B. OSPF
C. EIGRP
D. BGP
E. IGRP
F. IS-IS

Answer: B, D
B: the routing protocols should be OSPF, as it's an IETF standard.
D: BGP is the only other IETF standard protocol which has fast convergence.
Protocol RIP HELLO IGRP OSPF EIGRP IS-IS EGP
BGP4--------------------------Type IGP IGP IGP
IGP IGP IGP EGP EGPAlgorithm DV DV DV SPF DUAL SPF DV PVMetrics Hopcnt
Delay Speed Arb. Speed Arb. Policy PolicyConvergence Slow Unstb Mdt Fast Fast Fast
Slow FastStandard? IETF No No IETF No ISO Hist. IETFComplexity Simple Simple
Simple Complx Complx Complx Simple ComplxMultipath? Yes Yes Yes Yes Yes Yes
Yes [*]Var-netmask? No No No Yes Yes Yes No YES
Not C: EIGRP would also be the right answer but it is not an IETF standard.

QUESTION 117:

Which routing protocol is capable of supporting snap-shot routing?

A. RIPv2
B. IS-IS
C. EIGRP
D. OSPF

Answer: A

Snapshot allows the use of all "distance vector" routing protocols over DDR lines. They include:
1. RIP and IGRP for IP
2. RTMP for Appletalk
3. RIP and SAP for IPX
4. RTP for Vines

QUESTION 118:

Which one of the following Routing protocols supports snapshot routing ?

A. RIP V2
B. IS-IS
C. EIGRP
D. OSPF

Answer: A

QUESTION 119:

The newly appointed Certkiller trainee technician wants to know which two routing protocols have features that will enable proper operation over NBMA point-to-multipoint network without use of point-to-point subinterfaces. What will your reply be? Select two.

A. RIP
B. OSPF
C. IGRP
D. EIGRP
E. IS-IS

Answer: B, D
D: EIGRP is well suited for NBMA since the split-horizon can be disabled for EIGRP
Not E: IS-IS does not adapt to NBMA point to multipoint networks.
Page 391- 392 in CiscoPress CCDA Self-Study: Designing for Cisco Internetwork
Solutions DESGN 640-861. ISBN : 1587051419, Third printing june 2005

QUESTION 120:

Which of the following link-state routing protocols is capable of supporting IP and CLNP protocols and is used for large routed internetwork?
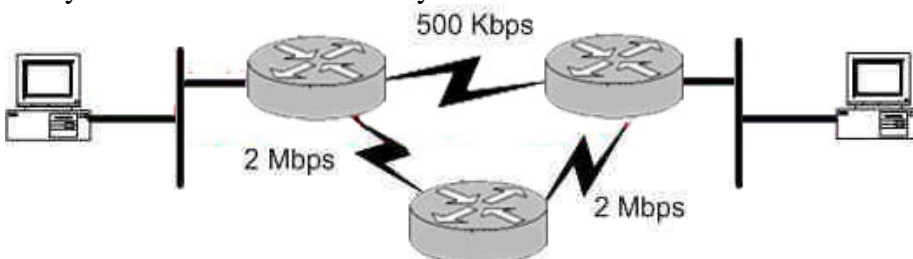
A. RIP v2
B. EIGRP
C. OSPF
D. IS-IS

E. BGP

Answer: D
CCDA Exam Certification Guide Second Edition
Page 334: IS-IS is a link-state routing protocol that floods link-state information throughout the network to build a picture of network topology. IS-IS was primarily intended for routing OSI Connectionless Network Protocol (CNLP) packets but has the capability to route IP packets. IS-IS is a common alternative to other powerful routing protocols such as OSPF and EIGRP in large networks.

QUESTION 121:

Study the exhibit below carefully:

In order for the two sites, as shown in the diagram, to transfer a large amount of data in an efficient manner (utilization available bandwidth), which routing protocols could you deploy in the routers? (Choose three)

A. OSPF
B. EIGRP
C. RIPv2
D. RIPv1
E. IGRP
F. BGP

Answer: A, B, E

QUESTION 122:

Which of the following would be the best reason for choosing a link-state routing protocol when designing a network?

A. The network design is flat.
B. The administrators have a good knowledge of the protocol.
C. Router processor overhead is a concern.
D. The network is being implemented as a hub-and-spoke design.
E. The convergence times are not a concern.

Answer: B

Explanation:
Link-state and distance vectors share a common goal-to fill the routing tables with the current best routes. They differ significantly in how they each accomplish the task. The largest difference between the two is that distance vector protocols advertise sparse information; in fact, distance vector protocols know only that other routers exist if the other router broadcasts a routing update to them. When a distance vector protocol in a router hears a routing update, the update says nothing about the routers beyond that neighboring router that sent the update. Conversely, link-state protocols advertise a large amount of topological information about the network, and the routers perform some CPU-intensive computation on the topological data. They even discover their neighbors before bothering to exchange routing information.

QUESTION 123:

Under which circumstances would static routing be the most appropriate?

A. For dial-on demand routing
B. For expending networks
C. For large enterprise backbone segments with redundant paths
D. For parallel WAN links

Answer: A

Explanation:
With dial on demand routing the link are established once there is interesting traffic to be sent. If the hello packets of routing protocols are interesting traffic then the connection will be up forever and it will be very expensive. If the hello packets are not, so the routing updates are not received in time and the routes will not be in routing tables. The static routing will be the best choice here.

QUESTION 124:

Certkiller recently made several acquisitions, each with its own network. All the networks use only Cisco Systems equipment, and there are no overlapping IP addresses. Certkiller does not desire to redesign the address spaces to support a hierarchical design.
Which routing protocols listed below would be most suitable to connect the entire network?

A. BGP
B. IS-IS
C. IGRP
D. EIGRP
E. OSPF
F. None of the above

Answer: D

Explanation:
EIGRP does not use distance vector or link-state logic, but instead it uses a whole new category of routing protocol. This new category has some features similar to link-state protocols, others similar to distance vector protocols, and yet others unlike either of the two. Cisco sometimes categorizes EIGRP as a balanced hybrid protocol, so you should remember the term.
The internal workings of EIGRP depend on an algorithm called the Diffusing Update Algorithm (DUAL). DUAL exchanges more topology information than a distance vector routing protocol, but it does not transmit full topology information like a link-state protocol. Also, the computations used by DUAL require far less processing than the computationintensive Dijkstra SPF algorithm.
DUAL defines a method for each router not only to calculate the best current route to each subnet, but also to calculate alternative routes that could be used if the current route fails. An alternative route, using what DUAL calls a feasible successor route, is guaranteed to be loop-free. So, if the current best route fails, the router immediately can start using the feasible successor route instead so that convergence can happen very quickly.
Incorrect answers:
B,E: IS-IS and OSPF permit an explicit hierarchical topology.
A: BGP is not IGP but EGP.
C: IGRP is old routing protocol and it supports only small networks, which are not more then 255 hosts in diameter.

QUESTION 125:

Four small ISPs amalgamated to establish a large ISP. One of their requirements is to carry autonomous system routes through their network.
Which of the following routing protocol would you include in your network design to accommodate this need?

A. MPLS
B. IBGP
C. OSPF
D. IS-IS
E. RIPv2
F. EIGRP

Answer: B

Explanation:
iBGP is the name used to describe the peering between BGP neighbors in the same AS. iBGP is used in transit autonomous system. Transit autonomous systems forward traffic from one external AS to another external AS. If transit autonomous systems did not use iBGP, the eBGP-learned routes would have to be redistributed into an IGP and then redistributed into the BGP process in another eBGP router
Reference: CCDA exam certification guide second edition page 350

QUESTION 126:

IS-IS has been configured on some of the Certkiller routers. Which link-state routing protocol supports IP and CLNP protocols and is used for large routed internetworks?

A. RIPv2
B. EIGRP
C. OSPF
D. IS-IS
E. BGP

Answer: D

Explanation:
An IS-IS routing domain is a network in which all the routers run the Integrated IS-IS routing protocol to support intradomain exchange of routing information. The network environment can be IP-only, ISO CLNP-only, or both. The IS-IS protocol was originally intended to support only CLNP. RFC 1195 adapts the original IS-IS specification (ISO 10589) to support IP, in what is referred to as Integrated IS-IS.
Reference: http://www.ciscopress.com/articles/article.asp?p=26850&rl=1

QUESTION 127:

A network designer is presenting a proposal that included route summarization. The IT manager asks the designer to describe route summarization. Which statement can the designer use to correctly describe route summarization to the IT manager?

A. Grouping multiple contiguous subnets into one Class A, B, or C IP address to minimize routing table size.
B. Grouping multiple discontinuous subnets together to increase routing performance.
C. Grouping ISP network addresses to minimize routes to the Internet.
D. Grouping multiple contiguous networks and advertising as one large network.

Answer: D

Explanation:
In large internetworks, hundreds, or even thousands, of network addresses can exist. It is often problematic for routers to maintain this volume of routes in their routing tables. Route summarization (also called route aggregation or supernetting) can reduce the number of routes that a router must maintain, because it is a method of representing a series of network numbers in a single summary address.
For example, in Figure 1-16, router D can either send four routing update entries or summarize the four addresses into a single network number. If router D summarizes the information into a single network number entry, the following things happen:

1. Bandwidth is saved on the link between routers D and E.
2. Router E needs to maintain only one route and therefore saves memory.
3. Router E also saves CPU resources, because it evaluates packets against fewer entries in its routing table.
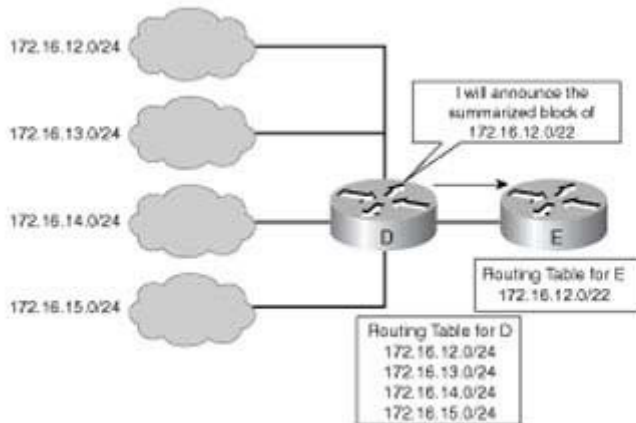
A summary route is announced by the summarizing router as long as at least one specific route in its routing table matches the summary route.

QUESTION 128:

You are a technician at Certkiller . Your newly appointed Certkiller trainee wants to know which principal components an SNMP-managed network consist of.
What would your reply be? (Choose all that apply.)

A. Agents
B. Firewalls
C. Managed devices
D. Demilitarized Zones
E. Network-management systems

Answer: A, C, E

Explanation:
A: Agents are actual software pieces that are run on the managed devices.
C: Managed devices are network nodes that run an SNMP software agent and are located on a SNMP managed network. They generate and store management related info and then provide this info to a network management system via SNMP. These nodes can be routers, access servers, switches etc.
E: They are core in SNMP. An NMS runs a network management application that is responsible for receiving and presenting all of the information collected from the agents to the network administrator.
Reference:
CCDA Study guide by Damon Merchant. Syngress Press.

Incorrect Answers
B, D: Firewalls and DMZs are not related to SNMP.

QUESTION 129:

You are the technician at Certkiller . Your supervisor instructs you to aid a Certkiller
customer in designing enhancements for scalability and availability to her network.
The routers currently on the customer's network are multi-vendor routers and are
owned by the departments where they are located. The customer's business runs on
an outsourcing agreement that she has for the maintenance of the network
equipment. This outsourced service vendor uses CiscoWorks with SAA to manage
the network.
Which Service Level Management challenges will you need to overcome in your
attempt to address the design proposal for this customer? (Choose all that apply.)

A. Your customer is not the owner of the switches on the network.
B. She has no way to monitor SLA conformance.
C. She can not manage the network internally with her own staff.
D. The switches and routers come from different vendors.
E. She is unable to utilize NetFlow on the network.
F. All of the above.

Answer: A, C, D

Explanation:
A: Customer does not own switches, because they are not Cisco Switches.
C: Because Switches are different vendor, she can not manage with her staff
D: CiscoWorks with Cisco devices. But Switches came from Different vendor.
Incorrect Answers
E: Netflow can not be used, because all the equipment is not from Cisco.
F: This possibility is not valid.

QUESTION 130:

Which goals will you keep in mind when you choose components in the design of a
new network that will incorporate fault management? (Choose all that apply.)

A. Log network events
B. Notify network administrators
C. Determine network topology
D. Incorporate intrusion detection
E. Detect network error conditions
F. All of the above.

Answer: A, B, E

Explanation:
When network grows beyond few nodes, fault management is used to isolate areas where the trouble lies and generally sounds an audible alarm to alert administrator to the existence of the fault. Log all network events before and after the fault .In WAN circuit fault it may alert both client-side and carrier side personal of the fault.
Incorrect Answers
C: It is for Accounting Management
D: This is mainly for security management
F: this possibility is negated by options A, B and E.

QUESTION 131:

You are a network technician at Certkiller . Your newly appointed Certkiller trainee wants to know which network security issue is addressed by encryption.
What will your reply be?

A. Data integrity
B. User authentication
C. Data authority
D. Data confidentiality
E. Data authentication

Answer: D

Explanation:
To safeguard sensitive corporate data Encryption is used. Data confidentiality is main concern.
Incorrect Answers
A, B, C, E:
These will not play any critical role in network security while performing Encryption.

QUESTION 132:

You work as a network administrator for Certkiller Inc. Some Certkiller users complain that they experience isolated DoS attacks directed at certain hosts in the e-commerce module.
In an attempt to address this concern, you turned off all unnecessary services since the operating systems on those servers have been patched. However, the problem is still experienced.
What else can you do to minimize the effect of these DoS attacks?

A. Block all TCP traffic to and from these servers.
B. Block all UDP traffic to and from these servers.
C. Limit the connection rate to these servers at the Internet firewall.
D. Block all incoming traffic whether it is TCP or UDP at the Internet firewall.

E. Load-balance between multiple servers running the same applications.

Answer: C

Explanation:
Prioritize the user connection to servers and limit the connection rate.
Incorrect Answers
A, B, D: one can not block TCP and UDP traffic.
E: Load Balancing will not solve the problem in greater extent.

Explanation:
DoS attacks deny legitimate users access to services. DoS attacks are characterized by disrupting connectivity between devices, preventing access to specific services, halting processes on devices by sending bad packets, and flooding networks.
Some ways to prevent DoS attacks follow:
1) Properly configure firewalls and routers to prevent DoS attacks. You can find these configurations on vendor and security websites.
2) Prevent spoofing.
3) Prevent traffic rates from getting out of control.
Reference: Cisco press p. 388

QUESTION 133:

What is used to measure network performance? (Choose all that apply.)

A. Utilization
B. Efficiency
C. Bandwidth size
D. Capacity
E. Response time
F. Packet size

Answer: A, D, E

Explanation:
You can perform assessments on network performance prior to implementing latency-sensitive applications and use them afterward for monitoring. Examples of performance variables are network throughput, user response times, and line utilization.
Reference: Cisco p.483.

QUESTION 134:

Which enhancements that did not exist in SNMP version 1 or 2 were added to SNMPv3?

A. Http transport.

B. Vendor-specific MIBs.
C. Increased reliability.
D. Secure transmission.
E. Interoperability.

Answer: D

Explanation:
Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable
standards-based protocol for network management. SNMPv3 provides secure access to
devices by a combination of authenticating and encrypting packets over the network. The
security features provided in SNMPv3 are:
* Message integrity---Ensuring that a packet has not been tampered with in-transit.
* Authentication---Determining the message is from a valid source.
* Encryption---Scrambling the contents of a packet prevent it from being seen by an
unauthorized source.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide09186a00800878fa.html

QUESTION 135:

Which of the following methods' function is the provision of data integrity? (Choose
two.)

A. Secure fingerprints
B. Single factor authorization
C. Token cards
D. Digital signatures
E. Two-factor authentication

Answer: A, D

Explanation:
Provided by Secure Fingerprints or Digital Signatures. If data is transmitted with a
Digital Signature and the received data doesn't match what the signature says it is, the
data has been compromised

QUESTION 136:

You are a network administrator at Certkiller and have been instructed to examine
the current system of one of the customers. You do this and find that the customer's
network facilities provides detection and correction of network device failures,
monitoring device and bandwidth usage and that they use SSH to manage devices.
Which functional areas of network management did the customer neglect? (Choose
all that apply.)

A. Configuration management
B. Fault management
C. Accounting management
D. Security management
E. Performance management
F. None of the above

Answer: C, D

Explanation:
C: Accounting management, such as usage tracking is not being used
D: Security management, such as filtering or physical security is not being used
Note: Secure Shell provides an encrypted configuration management session, not security management.
Incorrect Answers:
A: SSH is being used to manage devices.
B: A means to detect and correct network device failures is being used
E: A meansto monitor devices and bandwidth utilization is being used.
F: Not applicable.

QUESTION 137:

The statements below refer to SNMP commands, which of them is not valid?

A. Control of managed devices occurs when the NMS issues the write command.
B. The trap command is issued when the NMS requests events from the managed devices.
C. When the managed device issues the trap command, an agent will report an event.
D. To report events to the NMS, managed devices make use of the trap command.
E. All of the above.

Answer: B

Explanation:
Trap operations allow Simple Network Management Protocol (SNMP) agents to send asynchronous notifications that an event has occurred. Traps are sent on a best-effort basis and without any method to verify whether they were received.
Reference:
http://www.cisco.com/en/US/tech/ CK6 48/ CK3
62/technologies_configuration_example09186a0080094aa1.shtml

QUESTION 138:

At what stage are SNMP Trap messages sent?

A. When NMS need to initialize agents.

B. When an NMS requests events from the managed devices.
C. When agents have events to report to an NMS.
D. When an NMS wants agents to begin recording events.
E. When an NMS wants a proxy station to take over agent monitoring.

Answer: C

Explanation:
Trap operations allow Simple Network Management Protocol (SNMP) agents to send asynchronous notifications that an event has occurred. Traps are sent on a best-effort basis and without any method to verify whether they were received.
Reference:
http://www.cisco.com/en/US/tech/ CK6 48/ CK3
62/technologies_configuration_example09186a0080094aa1.shtml

QUESTION 139:

DRAG DROP
Match the following network management component with its function.

Select from these	Place here	Description
Agent	Place here	periodically collects object information
MIB	Place here	management transport mechanism
SNMP	Place here	generate traps of events
Manager	Place here	store information about network objects

Answer:

Select from these	Place here	Description
	Manager	periodically collects object information
	SNMP	management transport mechanism
	Agent	generate traps of events
	MIB	store information about network objects

Explanation:
a. MIB (Management Information Base)
A MIB is nothing more than a database of objects. The MIB has a tree- like structure,

similar to a file system. Each leaf object represents a parameter on the managed device. A common understanding of the MIB between NMSand agent is what allows SNMP communications to work.

b. SNMP (Simple Network Management Protocol)

Simple Network Management Protocol (SNMP) is the de facto standard network management protocol for the IP protocol suite. Developed in the late 1980s by the IETF (Internet Engineering Task Force), SNMP provides asimple means for vendors to provide management capabilities to their networking devices

SNMP defines a manager/agent relationship for network management. A manager device essentially has two functions: monitor and control. It monitors network devices (agents) by sending queries for performance, configuration, and status information. It controls agents by sending directives to change configuration parameters.

An example of an SNMP manager is an NMS (network management station) running CiscoWorks2000, while an agent might be a Cisco 7500 router. The NMS, acting as manager, communicates with the 7500, acting as agent, for information about its performance. SNMP is the protocol they use to communicate.

An NMS can manage systems that include hosts, servers, routers, switches, hubs, UPSs, or most any network-attached device. The NMS runs the network management applications, such as CiscoWorks2000, that present management information to network managers and other users. The processing of SNMP is mostly performed by the NMS.

QUESTION 140:

Your newly appointed Certkiller trainee wants to know which of the following you would describe as characteristics of CDP.
What will your reply be? (Choose two.)

A. It supports any SNMP device
B. It uses the UDP protocol
C. It is media and protocol independent
D. It reports on directly connected Cisco devices like routers, bridges, switches and access servers
E. It does not use UTP protocol
F. It uses RMON to gather utilization statistics

Answer: C, D

Explanation:
The CDP is a Cisco proprietary layer two protocol that is media- and protocol-independent, and runs on all Cisco-manufactured equipment including the following:
1. routers
2. bridges
3. access servers
4. switches
A Cisco device enabled with CDP sends out periodic interface updates to a multicast

address in order to make itself known to neigbors. Since it is a layer two protocol, these
packets (frames) are not routed. Use of SNMP with the CDP MIB allows network
management applications to learn the device type and the SNMP agent address of
neighboring devices, and to send SNMP queries to those devices. CDP uses the
CISCO-CDP-MIB.
Reference:
http://www.cisco.com/en/US/tech/ CK6 48/ CK3 62/technologies_tech_note09186a00801aa000.shtml

QUESTION 141:

You are a network administrator at Certkiller and have been instructed to design as
well as implement a SAFE network. You have done so, but now the users on the
network complain that they still encounter some DoS attacks on specific hosts in the
E-commerce module. You already place limits on the connection rate at the firewall,
but the problem prevails.
What else can you do to ameliorate the effects of these attacks?

A. Block all UDP traffic to these servers at the internet firewall
B. Practice Load-balancing between multiple servers with similar applications
C. Ensure all relevant OS patches have been applied
D. Block all TCP traffic to these servers at the internet firewall
E. Move the affected servers to the DMZ

Answer: C

Explanation:
To secure hosts, pay careful attention to each of the components within the systems.
Keep any systems up-to-date with the latest patches, fixes, and so forth. In particular, pay
attention to how these patches affect the operation of other system components. Evaluate
all updates on test systems before you implement them in a production environment.
Failure to do so might result in the patch itself causing a denial of service (DoS).
Reference: SAFE Extending the Security Blueprint to Small, Midsize, and Remote-User
Networks Page 8

QUESTION 142:

Which network analysis tool can display traffic utilization on router interfaces in
the form of a graph?

A. NBAR
B. MRTG
C. NetFlow
D. Cisco NetProfiler

Answer: B
Explanation

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing graphical images which provide a LIVE visual representation of this traffic.

QUESTION 143:

Your newly appointed Certkiller trainee wants to know which of the following Cisco device management features is best suited to meet network traffic and provide data for billing network usage needs.
What will your reply be?

A. IGMP
B. NetFlow
C. RMON
D. CDP
E. QoS

Answer: B

Explanation:
Converged networks increase the bandwidth requirements for the common transport network, which makes bandwidth an important resource to manage. However, it doesn't make sense to deny services to departments that need it. With a tool such as the Cisco NetFlow you can measure resource utilization to make charge-back decisions and measure the compliance of service providers with the terms of service.
Reference: Cisco press p.482-483.

QUESTION 144:

When using Ethernet, which frame size will impact on network performance?

A. A frame size (MTU) that is the minimum supported.
B. A frame size (MTU) that is the maximum supported.
C. A frame size (MTU) that uses the largest data block size.
D. A frame size (MTU) that uses the smallest data block size.
E. None of the above.

Answer: B

Explanation:
MTU (Maximum Transmission Unit): The largest packet size, measured in bytes, that an interface can handle.

QUESTION 145:

Which Cisco management feature would be the most appropriate to use when

metering network traffic and providing data for billing for network usage?

A. NetFlow
B. RMON
C. CDP
D. QoS
E. BGP

Answer: A

Explanation:
Converged networks increase the bandwidth requirements for the common transport network, which makes bandwidth an important resource to manage. However, it doesn't make sense to deny services to departments that need it. With a tool such as the Cisco NetFlow you can measure resource utilization to make charge-back decisions and measure the compliance of service providers with the terms of service.
Reference: Cisco press p.482-483.

QUESTION 146:

Which of the following items are definitive of Network Performance? (Choose three.)

A. Throughput
B. Response time
C. Packet size
D. Utilization
E. Efficiency

Answer: A, B, D

Explanation:
You can perform assessments on network performance prior to implementing latency-sensitive applications and use them afterward for monitoring. Examples of performance variables are network throughput, user response times, and line utilization.
Reference: Cisco p.483.

QUESTION 147:

Which two of the following capabilities of Netflow account can assist design with network planning?

A. NetFlow can perform packet decoding and analysis.
B. NetFlow can give a time-based view of application usage on the network.
C. NetFlow can meter packet and byte counts of network traffic.
D. NetFlow can monitor processor time on network devices.
E. NetFlow can allow monitoring of user network utilization.

Answer: B, E

Explanation:
NetFlowswitching is really more of an administrative tool than a performance-enhancement tool. It collects detailed data for use with circuit accounting and application-utilization information. Due to all the additional data that NetFlowcollects (and may export), expect an increase inrouter overhead possibly as much as a five percent increase in CPU utilization.
NetFlowswitching can be configured on most interface types and can be used in a switched environment. ATM, LAN, and VLAN technologies all support NetFlow switching; the Cisco 7200 and 7500 series routers provide its implementation.
NetFlowswitching does much more than just switching-it also gathers statistical data, including protocol, port, and user information. All of thisis stored in the NetFlow switching cache according to the individual flow that's defined by the packet information (destination address, source address, protocol, source and destination port, and the incoming interface). The data can be sent to a network management station to be stored and processed there.
The NetFlow switching process is very efficient. An incoming packet is processed by the fast or optimum switching process, and then all path and packet information is copied to the NetFlow cache. The remaining packets that belong to the flow are compared to the NetFlow cache and forwarded accordingly.
The first packet that's copied to the NetFlow cache contains all security and routing information, and if an access list is applied to an interface, thefirst packet is matched against it. If it matches the access list criteria, the cache is flagged so that the remaining packets in the flow can be switched without being compared to the list. (This is very effective when a large amount of access list processing is required.)

QUESTION 148:

A mission critical requirement of a new network update at a travel agency is access to Airline scheduling. A Service Level Agreement (SLA) is included in the design to assure a high level of availability. Which three capabilities should be included in the network design to manage the SLA?

A. The determination of fault when an SLA is violated
B. The restoration of the configuration of failed devices covered by the SLA
C. Identification and Isolation of the SLA device that cause outage.
D. The monitoring for conformance to the SLA
E. The reporting of SLA violation and performance trend.

Answer: A, D, E
CCDA Exam Certification Guide Second Edition
Page 485: You can use several SLAs to define a service because each SLA can represent a specific metric than can be measured, reported and monitored.

QUESTION 149:

Which two Internet Standards form part of the foundation of the Internet Standard Management Framework? (Choose two.)

A. NMS
B. SNMP
C. CDP
D. AAA
E. MIB

Answer: B, E

Explanation:
Simple Network Management Protocol (SNMP) is the de facto standard network management protocol for the IP protocol suite. Developed in the late 1980s by the IETF (Internet Engineering Task Force), SNMP provides asimple means for vendors to provide management capabilities to their networking devices
SNMP defines a manager/agent relationship for network management. A manager device essentially has two functions: monitor and control. It monitors network devices (agents) by sending queries for performance, configuration, and status information. It controls agents by sending directives to change configuration parameters.
A MIB is nothing more than a database of objects. The MIB has a tree- like structure, similar to a file system. Each leaf object represents a parameter on the managed device. A common understanding of the MIB between NMSand agent is what allows SNMP communications to work.

QUESTION 150:

Your intrusion detection system shows a high number port scans directed at specific hosts in your network looking for services and known vulnerabilities. You also detect ping attempts to your networks whole IP address range.
Which of the following solutions in the Internet Connectivity module will help manage these risks? (Choose two.)

A. Router ACL
B. Host application filtering
C. Firewall
D. Strong cryptography
E. Public and Private Key

Answer: A, C

Explanation:
We can gather the information regarding the remote hosts, using nmap etc tools.

After gathering the information of remote host, hacker starts to attack on remote host. In Security every services are labiality, So run the services required to you and implement the security as per needs.
Firewall is used to filter the packets entering into LAN or exiting from LAN. In Cisco Router to allow or deny the services to access can use ACL or PIX firewall.

QUESTION 151:

Enterprise Edge Functional Area
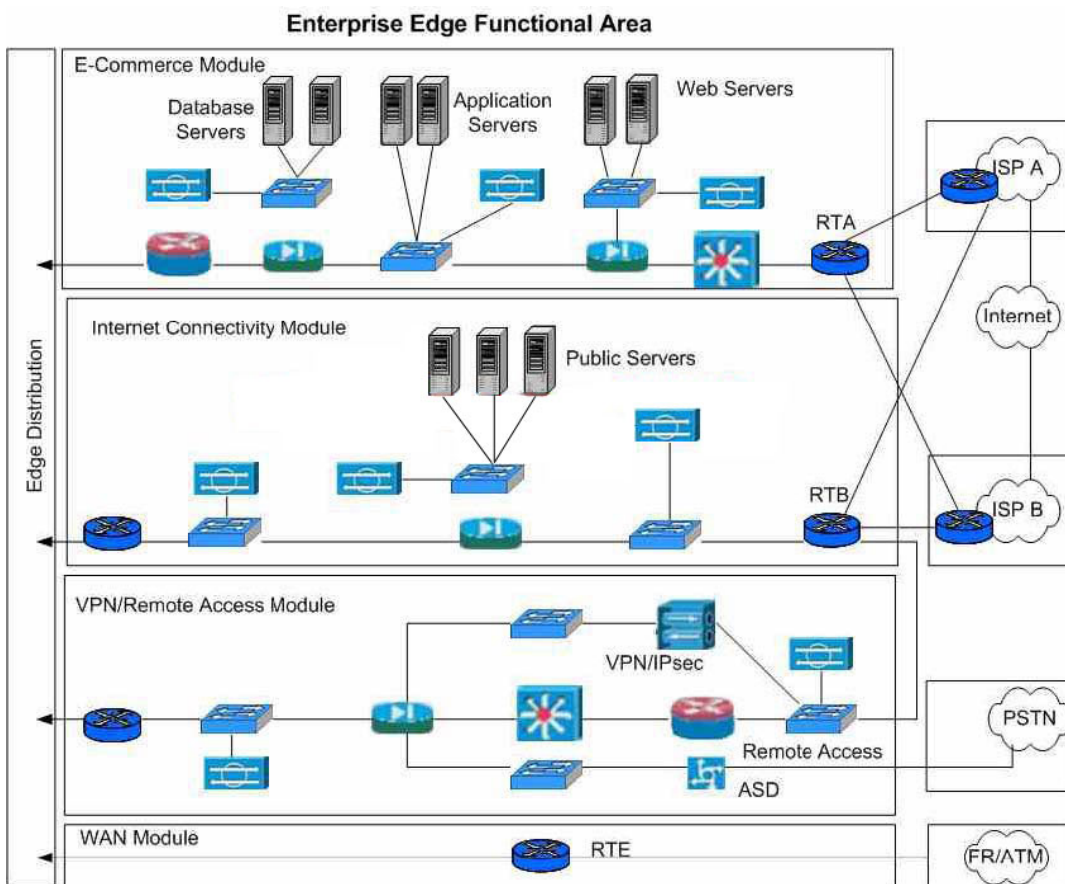
In which two devices would you expect DoS attacks from the Internet in the enterprise edge functional area? (Choose two)

A. VPN/IPsec
B. Public servers
C. WAN module
D. Database servers
E. Web servers

Answer: B, E

Explanation:
Denial of Service (DoS) is an attack designed to render a computer or network incapable of providing normal services. The most common DoS attacks will target

the computer's network bandwidth or connectivity. Bandwidth attacks flood the network with such a high volume of traffic, that all available network resources are consumed and legitimate user requests cannot get through. Connectivity attacks flood a computer with such a high volume of connection requests, that all available operating system resources are consumed and the computer can no longer process legitimate user requests.

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include
* attempts to "flood" a network, thereby preventing legitimate network traffic
* attempts to disrupt connections between two machines, thereby preventing access to a service
* attempts to prevent a particular individual from accessing a service
* attempts to disrupt service to a specific system or person

QUESTION 152:

Your newly appointed Certkiller trainee wants to know what the primary functions of an Access Layer in a campus design hierarchy is.
What will your reply be? (Choose all that apply.)

A. Provides connectivity to remote offices.
B. Provides policy-based routing services.
C. Connects shared LAN devices.
D. Provides connectivity to end-users.
E. Provides route summarization services.

Answer: A, C, D

Explanation:
Access Layer
The access layer provides user access to local segments on the network. The access layer is characterized by switched and shared bandwidth LANs in a campus environment. Microsegmentation, using LAN switches, provides high bandwidth to workgroups by dividing collision domains on Ethernet segments and reducing the number of stations capturing the token on Token Rings LANS. For small office/home office environments, the access layer provides access for remote sites into the corporate networks using WAN technologies such as ISDN, Frame Relay, and leased lines. Features such as dial-on-demand and static routing can be implemented to control costs.
Reference: Designing Cisco Networks (Ciscopress) page 93

QUESTION 153:

You are the network administrator at Certkiller . You are in the process of designing some changes to the Certkiller network. Your design goals are as follows:
* Replace hubs in several wiring closets with switches.
* Provide 30% more ports than currently exist on the hubs.

* Provide Fast Ethernet speeds to the workstations.
* Separate each closet into a different IP subnet.
* All users that will connect to these switches use standard file and print applications plus Internet browsing.
When designing the access layer of the network, which three questions should you consider? (Choose all that apply.)

A. How will VLANs be deployed?
B. What uplink cabling exists?
C. What level of redundancy is needed?
D. Will QoS be needed?
E. Will Gigabit uplinks be used?

Answer: B, C, E

Explanation:
Access layer
The access layer provides user access to local segments on the network. The access layer is characterized by switched and shared bandwidth LANs in a campus environment. Microsegmentation, using LAN switches, provides high bandwidth to workgroups by dividing collision domains on Ethernet segments and reducing the number of stations capturing the token on Token Ring LANs.
Reference: Designing Cisco Networks (Ciscopress) page 93

QUESTION 154:

What are the layers in the Cisco Systems hierarchical model of network design topology called? (Choose all that apply.)

A. Distribution
B. Designated
C. Core
D. Access
E. All of the above.

Answer: A, C, D

Explanation:
Hierarchical Network Design
* The core layer provides optimal transport between sites.
* The distribution layer provides policy-based connectivity.
* The access layer provides workgroup/user access to the network.
Reference: Designing Cisco Networks (Ciscopress) page 91

QUESTION 155:

The Exhibit below is a diagram of a Certkiller customer's network.
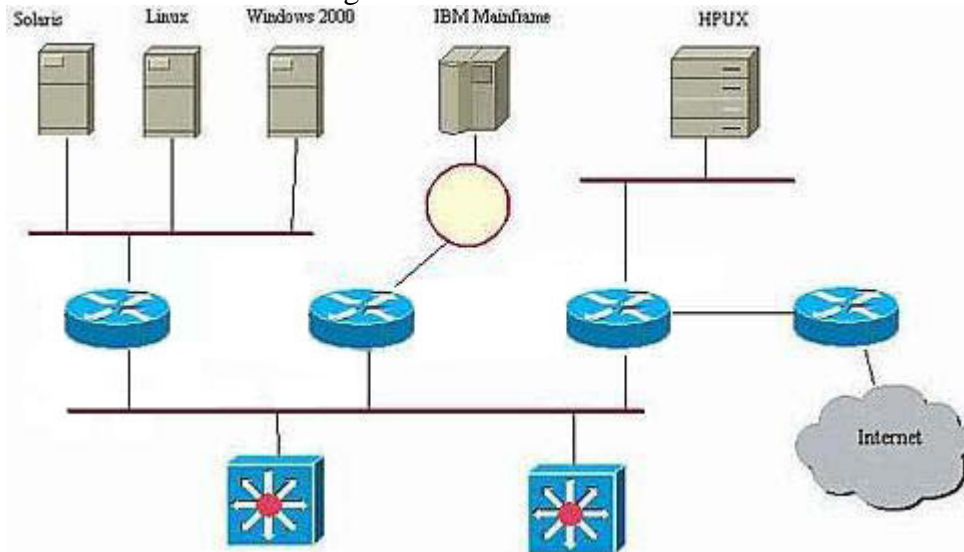
Referring to the information in the diagram, which Layer 2 or Layer 3 protocols needs to be supported in the new network design? (Choose all that apply.)

A. Appletalk
B. SNA
C. Frame Relay
D. Token Ring
E. IPX
F. NFS

Answer: B, D

Explanation:
IBM networking today consists of essentially two separate architectures that branch from a common origin. Before contemporary networks existed, IBM's system network Architecture (SNA) ruled the networking landscape, so it is often referred to as traditional or legacy SNA.
Page 130 of the DCN book list the Token Ring Design Rules
Reference: Designing Cisco Networks (Ciscopress) page 28 + 130

QUESTION 156:

Your newly appointed Certkiller trainee wants to know what the primary functions of a Distribution Layer in a campus design hierarchy is.
What will your reply be? (Choose all that apply.)

A. End-user connectivity.
B. Connects access devices to the core backbone.
C. Provides WAN connections.
D. Enforces security policies.

E. Provides QoS services.
F. High speed transport

Answer: B, D, E

Explanation:
Distribution Layer
The distribution layer of the network is the demarcation point between the access and core layers of the network. The distribution layer can have many roles, including implementing the following functions:
* Policy
* Security
* Address or area aggregation or summarization
* Departmental or workgroup access
* Broadcast/multicast domain definition
* Routing between VLANs
* Media translations
* Redistribution between routing domains
* Demarcation between static and dynamic routing protocols
Several Cisco IOS software features can be used to implement policy at the distribution layer, including the following.
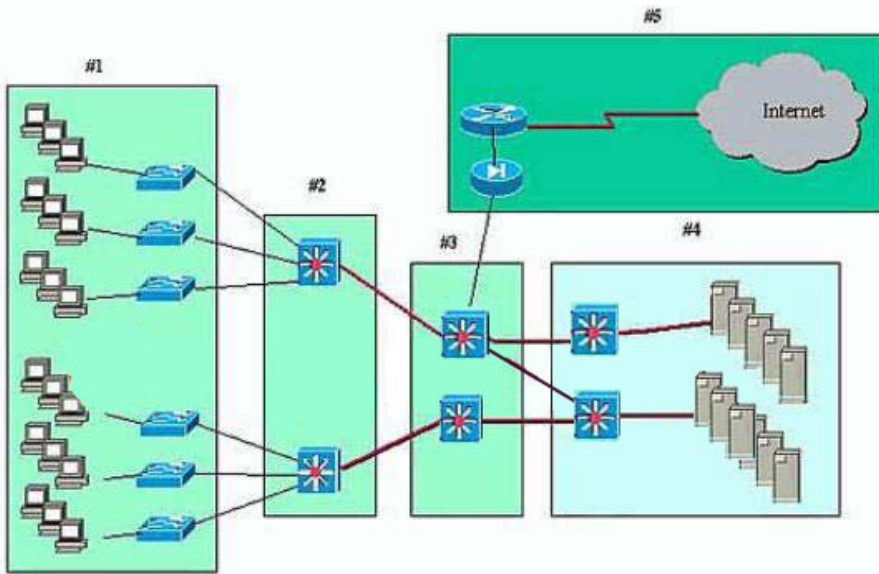* Filtering by source or destination address
* Filtering on input or output ports
* Hiding internal network numbers by route filtering
* Static routing
* Quality of service mechanisms
Reference: Designing Cisco Networks (Ciscopress) page 92

QUESTION 157:

The Exhibit below is a diagram of a Certkiller customer's network showing a standard Layer 2 campus design.

Which numbered box is representative of the Core Layer?

A. #1
B. #2
C. #3
D. #4
E. #5

Answer: C

Explanation:
In this block are routers which are situated in the middle of the network, what minimizes the network diameter. So it is a core layer.
The core layer is the high-speed switching backbone of the network, which is crucial to corporate communications. When a network uses routers, the number of router hops from edge to edge is called the diameter. As noted, it is considered good practice to design for a consistent diameter within a hierarchical network. The trip from any end station to another end station across the backbone should have the same number of hops. The distance from any end station to a server on the backbone should also be consistent. Limiting the diameter of the network provides predictable performance and easy of troubleshooting.
Reference: Cisco p.51

QUESTION 158:

The Exhibit below is a diagram of Certkiller 's network.
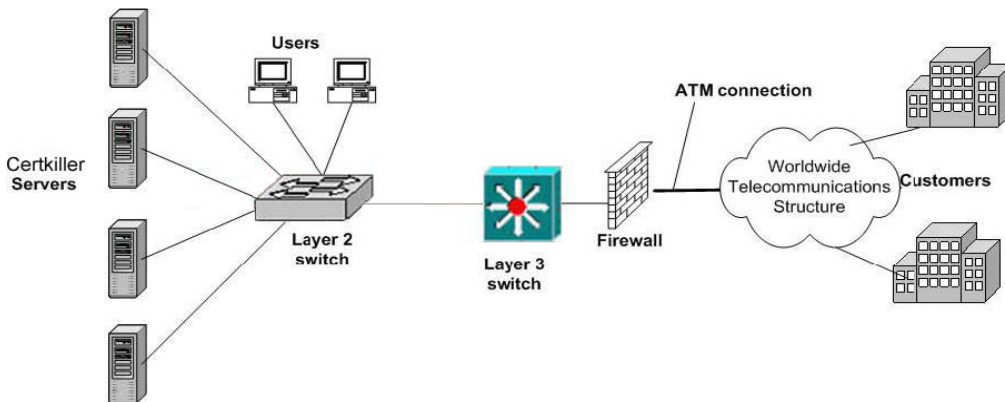
The Certkiller network has approximately 100 users and four servers that can be accessed via the Internet. Certkiller has 40 customers in several countries and would like to improve availability of their servers to these customers as illustrated in the exhibit.
Which components must be duplicated to attain this goal? (Choose all that apply.)

A. The Certkiller Layer 2 switch
B. User connections within Certkiller
C. The Certkiller Layer 3 switch
D. The Certkiller ATM connection
E. Customers connection to the Certkiller network

Answer: A, C, D

Explanation:
You would duplicate the layer 2, layer 3 and ATM connection to speed the access and redundancy of the network.

QUESTION 159:

Certkiller , Inc. is located in Redmond. The company recently signed a merger agreement with another company named Test Technologies, Ltd. Test Technologies, Ltd. is located on the other side of town. Test Technologies employees will be moving into the Certkiller building. They will occupy two floors in the building. They will bring with them their email, file servers and an advanced web-based database system primarily accessed at the office.
The current Certkiller network has become very slow. Therefore, Certkiller wants to upgrade their network before the Test Technologies employees move into the building. Certkiller employees say that they can access the company's website quicker from their homes over the Internet than on their local office network. They want you to make their LAN "as fast as their WAN". You must also design enough capacity to accommodate the Test Technologies users who are more technically advanced.
Certkiller would like to adopt VoIP throughout the combined company. Lastly, Certkiller wants to make sure that network security measures are in place for the new company's web site and e-mail servers. In particular, they want to make sure that no hackers can

access the Test Technologies servers from the Internet and want to protect the servers
from Internet-based viruses.
Which data-link layer features will you need to include in the scope of this design
project? (Choose all that apply.)

A. VLANs.
B. 10/100 auto sensing.
C. Redundant WAN links.
D. Intrusion detection.
E. Gigabit Ethernet.

Answer: A, B, E

Explanation:
The data-link layer (Layer 2) works with switches, which uses auto sensing and can
provide Gigabit Ethernets as well as VLANs.

QUESTION 160:

Your newly appointed Certkiller trainee wants to know what the primary functions
of the Core Layer in a campus design hierarchy is.
What will your reply be? (Choose all that apply.)

A. High-speed transport
B. Security
C. Manageability
D. Provides WAN connections.
E. Fault tolerance
F. Packet filtering
G. Enforces security policies.

Answer: A, C, E

Explanation:
Core Layer
The core layer provides optimal transport between sites.
The core layer is the high-speed switching backbone of the network, which is crucial to
enable corporate communication. The core layer should have the following
characteristics.
* Offer high reliability
* Provide redundancy
* Provide fault tolerance
* Avoid to changes quickly
* Offer low latency and good manageability
* Avoid slow packet manipulation caused by filters or other processes

* Have a limited and consistent diameter
Reference: Designing Cisco Networks (Ciscopress) page 91

QUESTION 161:

The server farm would usually be connected to which layer in the design hierarchy of a large campus network design?

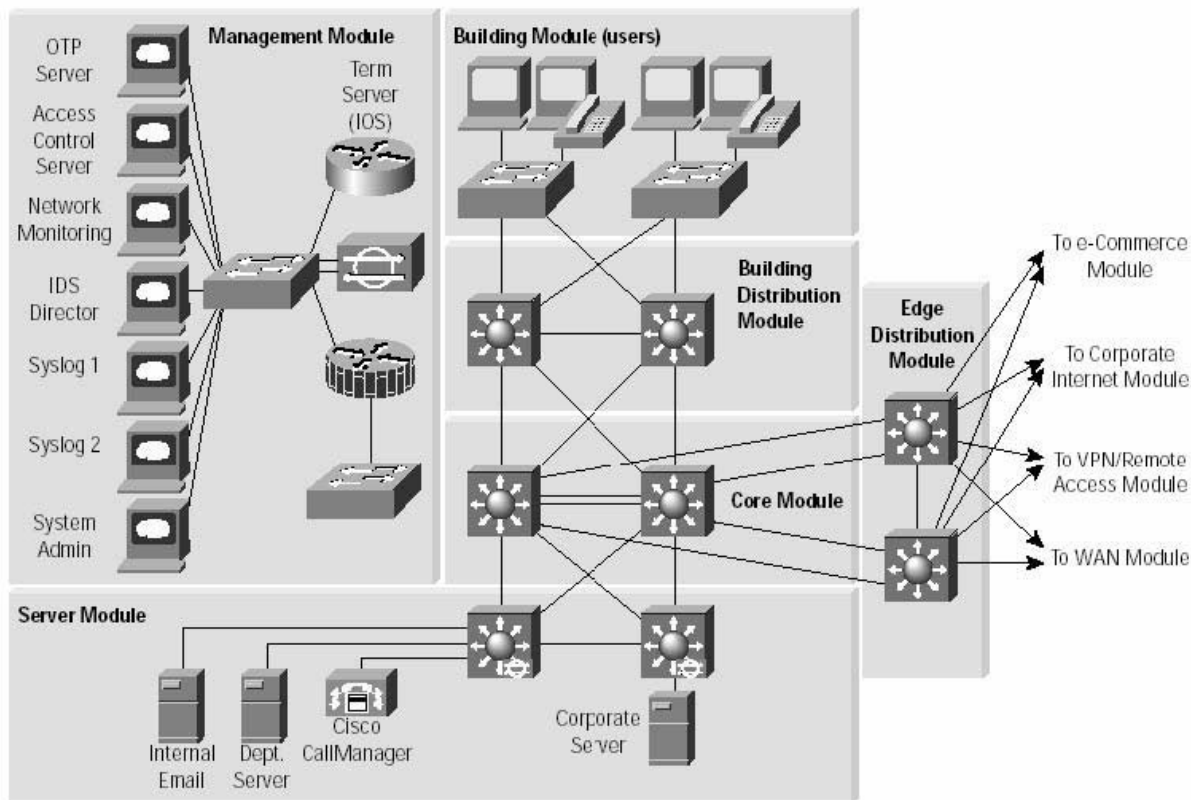A. Distribution
B. Internal
C. Access
D. Core
E. Edge
F. External

Answer: D

Explanation:

Enterprise Campus

The following is a detailed analysis of all the modules contained within the Enterprise Campus.

Figure 3 Enterprise Campus Detail

Reference: SAFE: A Security Blueprint for Enterprise Networks Page 11

QUESTION 162:

Your newly appointed Certkiller trainee wants to know at which layer is most Layer
3 routing features like summarization and redistribution performed when working
within an ideal network design milieu.
What will your reply be?

A. Core
B. Edge
C. Distribution
D. Internal
E. Access
F. External

Answer: C

Explanation:
Distribution Layer
The distribution layer of the network is the demarcation point between the access and
core layers of the network. The distribution layer can have many roles, including
implementing the following functions:
* Policy
* Security
* Address or area aggregation or summarization
* Departmental or workgroup access
* Broadcast/multicast domain definition
* Routing between VLANs
* Media translations
* Redistribution between routing domains
* Demarcation between static and dynamic routing protocols
Several Cisco IOS software features can be used to implement policy at the distribution
layer, including the following.
* Filtering by source or destination address
* Filtering on input or output ports
* Hiding internal network numbers by route filtering
* Static routing
* Quality of service mechanisms
Reference: Designing Cisco Networks (Ciscopress) page 92

QUESTION 163:

You are a network administrator at Certkiller . You are proposing a multi layer
switching solution with multiple paths to replace the current non-redundant
network of routers for the Certkiller network.
When presenting your proposed design to the board of directors, which benefits of
multi layer switching would you emphasize? (Choose all that apply.)

A. Smaller broadcast domains.
B. Increased network availability.
C. Increased network performance.
D. Fast and more reliable convergence.
E. Increased throughput due to multiple paths.
F. Increased network security due to VLAN functionality.

Answer: B, C, E

Explanation:
Multilayer Switching
Multilayer switching combines Layer 2 switching and layer 3 routing functionality.
Multilayer switching moves campus traffic at wire speed while at the same time
satisfying Layer 3 routing requirements. This combination not only solves throughput
problems but also removes the conditions under which layer 3 bottlenecks form.
Multilayer switching is based on the "route once, switch many" model.
Reference: Building Cisco Multilayer Switched Networks (Ciscopress) page 20

QUESTION 164:

DRAG DROP
Two Certkiller users work in separate buildings on a campus network. The one user
sends a packet to the other user with an instant messaging application. Place the
actions that are performed on the packet in the correct order as it travels from the
one user to its destination.

Layer-3 switched across LAN core	place step one here
Layer-2 switched toward the distribution switch	place step two here
Layer-2 switched across access LAN to target host	place step three here
Layer-3 switched through Distribution toward access	place step four here
Layer-3 switched through Distribution toward core	place step five here

Answer:

Explanation:
1)L2 switched toward dist switch
2)L3 switched thru dist towards core
3)L3 switched across LAN core
4)L3 switched thru dist towards access
5)L2 switched across access LAN to target host

Explanation: Typically implementations follow the L2-L3-L2 model in the Cisco
Model. Only w/o budget constraints is the L2-L3-L3 model used to provide extra

features like redundancy in the Core Layer. But in this case, since User A and B are in separate buildings, the L2-L3-L3 implementation is to be used. What happens is that the packet will go from access -> distro -> core -> distro -> access. No way to avoid that.

QUESTION 165:

You are contracted as a network administrator for a small company, Certkiller Inc. The company's network consists of a campus model made up entirely of VLANs attached to layer 2 access switching using C-class networks. The users complained that they get slow responses from the network even though you determined that the core switches show low utilization and after an analysis you found excessive data link layer traffic.
Which of the following network changes can ameliorate this problem? (Choose all that apply.)

A. use NAT wherever possible
B. segment the network into smaller VLANs
C. implement rapid spanning tree protocol (RSTP)
D. reduce size of broadcast domains
E. implement EIGRP at the distribution layer

Answer: B, D

Explanation:
The Core layer is not a problem here hence the problem is on the access layer. There are to many collisions on the access layer. So the broadcasts domains size should be reduced. Both B and D solve this problem.

QUESTION 166:

Which of the following are not primary functions of an Access Layer in a campus design hierarchy? (Choose all that apply.)

A. Provides connectivity to remote offices.
B. Provides policy-based routing services.
C. Connects shared LAN devices.
D. Provides connectivity to end-users.
E. Provides route summarization services.

Answer: B, E

Explanation:
Access Layer
The access layer provides user access to local segments on the network. The access layer is characterized by switched and shared bandwidth LANs in a campus environment.

Microsegmentation, using LAN switches, provides high bandwidth to workgroups by dividing collision domains on Ethernet segments and reducing the number of stations capturing the token on Token Rings LANS. For small office/home office environments, the access layer provides access for remote sites into the corporate networks using WAN technologies such as ISDN, Frame Relay, and leased lines. Features such as dial-on-demand and static routing can be implemented to control costs.
Reference: Designing Cisco Networks (Ciscopress) page 93

QUESTION 167:

You are contracted as a network administrator for a stock brokerage firm, Certkiller Inc. that is opening a new branch in Berlin. The users on the network will consist of a dozen stock traders that need constant data access to exchange continually, fast and uninterrupted all around the world.
Which of the following features will provide this level of connectivity? (Choose all that apply.)

A. CDP
B. QoS
C. IGRP
D. CoS
E. All of the above

Answer: B, D

Explanation:
This document describes Quality of Service (QoS) for Voice over IP (VoIP) in a LAN environment by mapping Type of Service (ToS) to Class of Service (CoS) parameters. Until recently, the general consensus was that QoS would never be an issue in the enterprise side due to the bursty nature of network traffic and the capability of buffer overflow. The reason for QoS on the LAN side is due to buffering, not lack of bandwidth. For this reason, QoS tools are required to manage these buffers to minimize loss, delay, and delay variation. Transmit buffers have a tendency to fill to capacity in high-speed networks due to the bursty nature of data networks combined with the high volume of smaller Transmission Control Protocol (TCP) packets. If an output buffer fills, ingress interfaces are not able to immediately place new flow traffic into the output buffer. Once the ingress buffer fills, which can happen quickly, packet drops occur and this is where voice quality may possibly degrade due to packet loss.
Reference:
http://www.cisco.com/en/US/tech/ CK6 52/ CK6 98/technologies_configuration_example09186a00800a954d.shtml

---

QUESTION 168:

Which of the following design criteria would require the deployment of VLANs in a proposed solution? (Choose all that apply.)

A. Security between departments.
B. Segmenting collision domains.
C. Segmenting broadcast domains.
D. Multicast traffic on the LAN.
E. The use of multivendor equipment.

Answer: A, C

Explanation:
C: When you "segment" a network, you are dividing one network into multiple (smaller) sections. So when you segment something, you are dividing it into smaller sections. Hence, deploying VLANs would be segmenting a broadcast domain. Before the VLANs you had one large broadcast domain. After implementing VLANs, you have multiple, smaller broadcast domains.
Not B: You cannot implement VLANs with hubs, so it has to be assumed that switches are being used. And with switches, each connection to the switch is a collision domain. Deploying VLANs does not "segment collision domains".
Not D, E: Answers D and E are not relevant to VLANs.

QUESTION 169:

When using Ethernet, which frame size will impact on network performance?

A. A frame size (MTU) that is the minimum supported.
B. A frame size (MTU) that is the maximum supported.
C. A frame size (MTU) that uses the largest data block size.
D. A frame size (MTU) that uses the smallest data block size.
E. None of the above.

Answer: B

Explanation:
MTU (Maximum Transmission Unit): The largest packet size, measured in bytes, that an interface can handle.

QUESTION 170:

Which of the following items of information is least relevant when designing a new campus network for a customer who wants to improve the performance of their campus network?

A. Number of users
B. Applications in use
C. Future growth
D. Location of wiring closets

E. Network speed

Answer: D

QUESTION 171:

Which of the following statements regarding network broadcasts are valid? (Choose all that apply.)

A. Broadcasts are restricted to active, end-user device ports.
B. Routers do not forward broadcasts
C. Broadcasts do not happen at Layer 3
D. Broadcasts can be controlled via VLANs

Answer: B, D

Explanation:
You use routers to connect networks and route packets of data from one network to another. Cisco became the de facto standard of routers because of their high-quality router products, their great selection, and their fantastic customer service. Routers, by default, break up a broadcast domain
, which is the set of all the devices on a network segment that hear all the broadcasts sent on that segment. Breaking up a broadcast domain is important because when a host or server sends a network broadcast, every device on the network must read and process that broadcast-that is, unless you've got a router. When the router's interface receives this broadcast, it can respond by basically saying, "Thanks, but no thanks"; it can then discard the broadcast without forwarding it on to other networks. Even though routers are known for breaking up broadcast domains by default, it's important
to remember that they also break up collision domains as well. Here are two ways that using routers in your network can reduce congestion: _
They don't forward broadcasts by default (switches and bridges do)
They can filter the network based on Layer 3 information (that is, based on IP address);
switches and bridges cannot.
VLANsallow a switch to separate different physical ports into different groups so that traffic from devices in one group never gets forwarded to the other group. This allows engineers to build networks that meet their design requirements, without having to buy a different switch for each group. Also, multiple switches can be connected together, with traffic from multiple VLANs crossing the same Ethernet links, using a feature called trunking.

QUESTION 172:

Certkiller .com intends to connect the LANs between the headquarters and the branch office. The headquarters and branch office are located in two separate buildings, and they have line of sight. Which of the following technologies is the most suitable for the task?

A. Broadband wireless access
B. Cellular wireless access
C. Wireless LAN
D. Mobile IP
E. GSM

Answer: A
The Cisco broadband fixed wireless system provides up to 44 Mbps full-duplex data in a
12 MHz RF channel in the Unlicensed National Information Infrastructure (U-NII) band
(5.725 to 5.825 GHz).
Features of the broadband fixed wireless system include:
1. Easy deployment
2. Flexibility-A wide variety of interfaces to the host routers and a wide variety of
network deployments
3. Local access data rates over 44 Mbps
4. End-to-end IP-based technology

QUESTION 173:

A Campus network is made up of VLANs that are attached to Layer-2 access
switches using IP class C address. The campus backbone switches show low
utilization. However, you received reports by users regarding slow network
response. Traffic analyst shows excessive data-link layer traffic in building
distribution layer.
Which two network design changes will you recommend that will have the ability to
improve network response time? (Choose two)

A. Implementing Spanning-Tree Protocol
B. Implementing NAT wherever possible
C. Implement smaller VLANs
D. Implement smaller broadcast domain
E. Implement EIGRP at Distribution layer

Answer: A, C

Explanation: A VLAN is a broadcast domain.
Smaller VLANs equate to smaller broadcast domains.
Answers C and D are redundant.
However, they mention Layer-2 access switches. And they offer "Implementing
Spanning-Tree Protocol" as a possible answer. If the switches were not running STP,
then there would be bridge loops which would cause excessive traffic and slow response
times.

QUESTION 174:

Certkiller requires its network to connect at higher data rate. The Certkiller
networks are located in deferent buildings with clear line of site. Which technology
represents a solution to this need?

A. Cellar Wireless
B. Broadband fixed Wireless
C. Wireless LAN
D. Mobile IP
E. ISDN

Answer: B
The Cisco broadband fixed wireless system provides up to 44 Mbps full-duplex data in a
12 MHz RF channel in the Unlicensed National Information Infrastructure (U-NII) band
(5.725 to 5.825 GHz).
Features of the broadband fixed wireless system include:
1. Easy deployment
2. Flexibility-A wide variety of interfaces to the host routers and a wide variety of
network deployments
3. Local access data rates over 44 Mbps
4. End-to-end IP-based technology

QUESTION 175:

DRAG DROP
Drag the appropriate media to the corresponding media type.

Select from these

Moderate cost

High Cost

Gigabit Ethernet up to 7 KM

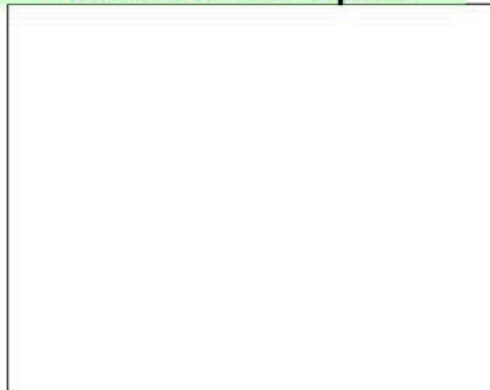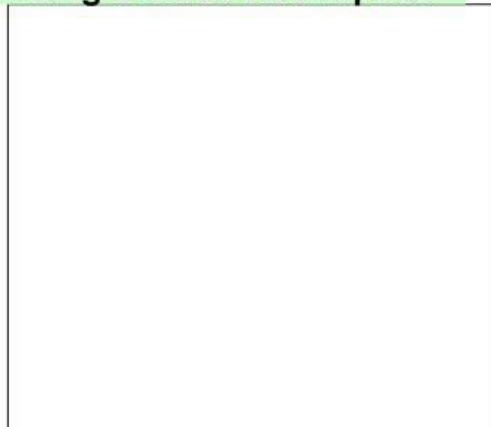Gigabit Ethernet up to 550 KM

Fast Ethernet up to 10 KM

Fast Ethernet up to 2 KM

Place here

Multimode fiber optics

Single mode fiber optics

Answer:

Select from these

Place here

Multimode fiber optics

Moderate cost

Gigabit Ethernet up to 550 KM

Fast Ethernet up to 2 KM

Single mode fiber optics

High Cost

Gigabit Ethernet up to 7 KM

Fast Ethernet up to 10 KM

Explanation:
The cable itself comes in two different styles: single-mode fiber (SMF) and multimode fiber (MMF). The difference between single-mode fibers and multimode fibers is in the number of light rays (and thus the number of signals) they can carry. Generally speaking, multimode fiber is used for shorter-distance applications and single-mode fiber for longer distances.
If you happen to come across a strand of fiber in the field and want to know if it's single mode or multimode, here are some general guidelines. First of all, if it's got a yellow jacket, it's probably single mode. If it's got an orange jacket, it's most likely multimode. Also, check the writing on the cable itself. You'll find a number like 62.5/125. These are the outside diameters of the core and the cladding (respectively). If the first number is a 8, 9, or 10, it is most likely a single mode. On the other hand, if the numbers read as before (62.5/125), it's most likely a multimode strand of fiber. Use these two tips to help you identify that errant strand of fiber. Although fiber-optic cable may sound like the solution to many problems, it has pros and cons just as the other cable types. Here are the pros:
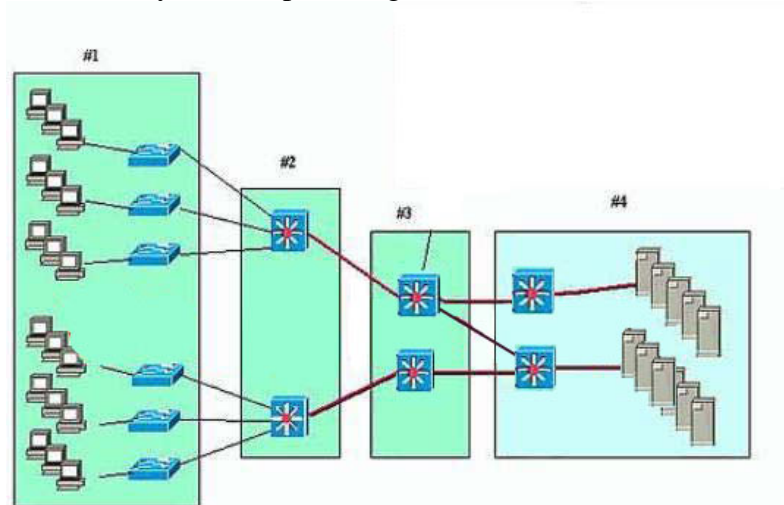1. Is completely immune to EMI or RFI
2. Can transmit up to 40 kilometers (about 25 miles)

3. Here are the cons of fiber-optic cable:
4. _ Is difficult to install
5. Requires a bigger investment in installation and materials

---

QUESTION 176:

The Exhibit below is a diagram of a Certkiller customer's network showing a
standard Layer 2 campus design.

Which numbered box is representative of the Distribution Layer?

A. #1
B. #2
C. #3
D. #4

Answer: B

Explanation:
1. Core Layer
The core layer is literally the core of the network. At the top of the hierarchy, it is
responsible for transporting large amounts of traffic both reliably and quickly. If
there is a failure in the core layer, every single user can be affected. Therefore, fault
tolerance is an issue. The core is likely to see large volumes oftraffic. Speed and
latency are driving concerns here. Given the function of the core, you can now
consider some design specifics. Let's start with some things that you know you don't
want to do at the core:
* Don't do anything to slow down traffic. This includes using access lists, routing
VLANs, packet filtering, any type of packet manipulation, etc.
* Don't support workgroup access.
* Avoid expanding the core when the internetwork grows (i.e., adding routers). If
performance becomes an issue in the core layer, give preference to upgrades over
expansion.

There are a few tasks that you want to make sure to get done as you design the core.
They include
* Design the core layer for high reliability. This means redundancy and fault
tolerance should both be included.
* Design with speed in mind. The core should have very little latency; it should be
fast and efficient.
* Select routing protocols with lower convergence times. Fast and redundant data
link connectivity is no help if your routing tables are shot!
2. Distribution LayerThe distribution layer is where much of the action is. Whereas
in the core the emphasis is speed, at the distribution layer the emphasis is control.
This is theplace to implement policies for the network. Here, you can exercise
considerable flexibility in defining network operation. There are several tasks that
generally should be done at the distribution layer:
* Implementing tools such as access lists, packet filtering, QoS, and queuing
* Implementing security and network policies, including address translation and
firewalls
* Redistribution between routing protocols, including static routing
* Route summarization and route filtering
* Load balancing
* Routing between VLANs, and other workgroup support functions
* Providing redundant connections for access devices
3. Access LayerThe access layer controls user and workgroup access to internetwork
resources. Some of the functions to be included at this layer are
* Continued (from the distribution layer) access control and policies
* Creation of separate collision domains (segmentation)
* Workgroup connectivity into the distribution layer

QUESTION 177:

The newly appointed Certkiller trainee technician wants to know which module
within the Enterprise Campus is connected with redundant link to the Edge
Distribution Module. What will your reply be?

A. Server Farm
B. Campus Backbone
C. Building Distribution
D. Network management

Answer: B

Explanation:
The distribution layer is where much of the action is. Whereas in the core the
emphasis is speed, at the distribution layer the emphasis is control. This is theplace
to implement policies for the network. Here, you can exercise considerable
flexibility in defining network operation. There are several tasks that generally
should be done at the distribution layer:

* Implementing tools such as access lists, packet filtering, QoS, and queuing
* Implementing security and network policies, including address translation and firewalls
* Redistribution between routing protocols, including static routing
* Route summarization and route filtering
* Load balancing
* Routing between VLANs, and other workgroup support functions
* Providing redundant connections for access devices

QUESTION 178:

What are three advantages of multilayer core switch design over a layer 3 core switch design for the network backbone of a large campus environment? (Choose three.)

A. Evenly distributed backbone traffic
B. Large scalability potentials
C. VLan implementation in the backbone
D. Reduced Distribution routes peering
E. Broadcast control in the backbone

Answer: A, C, E

Explanation:
LAN switches have been L2 devices from the beginning. Modern L3 switches provide higher OSI-level functionalities and can replace routers in the LAN switches environment. Your choice of pure L2 or L3 switches inthe enterprise network is no small matter and requires a complete understanding of your network topology and customer needs.
The simple function of an L3 device is to separate network segments. Traditionally, the L3 device was a router. Today, network designers prefer an L3 switches. These two devices differ in the type of information they process to determine the output interface. L2 switches forwards frames based on Data Link switches information (MAC address), while L3 switches forwards frames based on Network switches information (IP address).
A single- or two-L2 broadcast domain backbone isn't a great solution for large enterprise networks. A better choice for the campus backbone is L3 switches due to scalability and flexibility issues. L3- switches campus backbones are preferred over the L2 backbone for many reasons, including:
* Large scalability potential
* Reduced number of connections between L3 switches. Each L3 distribution switches (router) connects to one L3 campus backbone switches. This simplifies any-to-any connectivity between distribution and backbone switches.
* Flexible topology with no spanning-tree loops. There is no L2 switches either in the backbone or on the distribution links to the backbone because all the links are routed. Arbitrary topologies are supported because of the routing protocol used in

the backbone.
* Better support for network services because of L3 support in the backbone switches.
* Multicast and broadcast control. If you have a switches 2 backbone, you have to create multiple VLANs to provide any type of broadcast control.
One of the many things to consider for the L3 backbone switches is the performance of L3 switches. L3 switches require more sophisticated devices for high-speed packet routing. L3 switches support routing in the hardware, although the hardware in your network may not support all its features. If a certain feature is not supported in the hardware, it must be performed in software, which may impinge on data transfer. Other issues surround QoS and access list support. Hardware cannot process QoS tables or security tables if they consist of too many entries. These limitations will degrade the L3 switch's performance. And better performance was your goal for using the L3 switches in the first place! If you're experiencing excessive broadcasts on your corporate LANs, the best solution is to add L3 switches where appropriate and create VLANs.

QUESTION 179:

Why is a top-down network design process preferable to a bottom-up network design?

A. It utilizes previous experience
B. It provides design for current and future development
C. It identifies appropriate technologies first
D. It takes less time to design a network

Answer: B

Explanation:
Top-down means that you begin with abstract concepts and application requirements first before identifying technologies to use. The abstract concepts are the business requirements, the network architecture, and then the network design. The process is often iterative because the design changes as you uncover more information about the needs of the network.
Cisco CCDA self-study v2 (Page 57)

QUESTION 180:

Which of the following statements represents a basic characteristic of Layer 2 switches?

A. Layer 2 switches derive high performance from fast processors.
B. Layer 2 switches are less susceptible to broadcast storms.
C. Layer 2 switches force a network design with smaller subnets.
D. Layer 2 switching is hardware based bridging.

Answer: D

Explanation:
Layer 2 switches are multi-port bridges; therefore, they have all the same
functionality of bridges. There are differences that differentiate a switch from a
bridge. For example, switches utilize hardware or Application-Specific Integrated
Circuit (ASIC) chips to forward frames rather than software. Also, each port of the
switch has a dedicated bandwidth. If the dedicated port on a switch is 10Mbps, the
connected LAN segment has a dedicated bandwidth of 10Mbps. This works in the
same manner for 100Mbps and 1000Mbps dedicated switch ports. This feature also
sets a switch apart from a bridge that has a low port density.

QUESTION 181:

A network designer suggests that the standalone enterprise campus routers be
replaced with paired multilayer switches.
What are the benefits that the designer will emphasize when presenting the
proposed design to the global organization's board of directors? (Choose three)

A. Encryption due to VLAN functionality.
B. Increased throughput due to multiple paths.
C. Remote access connectivity due to access servers.
D. Increased availability due to redundancy.
E. Fast convergence due to OSPF protocol use.
F. Increase network performance

Answer: B, D, F

Explanation:
Enterprise Campus ModulesThe Enterprise Campus functional area contains four major
modules. Itapplies to a single campus and can easily be replicated campus to campus.
The four modules of the Enterprise Campus functional area areas follows:
Campus Infrastructure moduleThe Campus Infrastructure module describes the
infrastructure within a building. It is divided into three sub-modules, which correspond to
the three-layer hierarchy. The Building Access sub-module represents the access layer,
the Building Distribution sub-module represents the distribution layer, and the Campus
Backbone sub- module represents the core. Each building has a separate access layer and
distribution layer sub-module, all interconnected by the Campus Backbone sub-module.
The Campus Infrastructure module handles communications between the other modules
of the Enterprise Campus functional area.
Network Management moduleThe Network Management module represents the
network management function in the campus environment. It includes functions such as
IDS management, syslogging, SNMP management, network monitoring, and out-of-band
management (OBM).
Server Farm module The Server Farm module contains critical servers and connects

them to the Campus Infrastructure Campus Backbone in ahighly available way. These servers include all vital functions such as DNS, DHCP, file and print, e-mail, application, etc.

Edge Distribution moduleThe Edge Distribution module provides distribution layer functions between the Enterprise Campus functional area and the Enterprise Edge functional area (discussed next). The need for a distribution layer between the Campus Backbone and Enterprise Edge modules allows for campus control mechanisms such as access control and security, as well as high-availability and high-capacity communications.

Enterprise Edge ModulesThe Enterprise Edge functional area also includes four modules. Each of these modules is connected to the Edge Distribution module of the Enterprise Campus functional area. This bridges the gap between the campus site and WAN connectivity. Realize that not every enterprise includes every module. The four modules are as follows:

E-Commerce moduleThe E-Commerce module contains servers and applications largely intended for external consumption in for-profit activities. Web servers, application and database servers, firewalls, IDS, Layer 4 switches, and content engines all live here.

Internet Connectivity moduleThe Internet Connectivity module differs from the E-Commerce module in that devices here are supportive of the enterprise not necessarily directly as commerce services. Items such as SMTP mail servers, DNS and public FTP servers, web servers, and firewalls are included in this module.

Remote Access and VPN moduleAs the name implies, the Remote Access and VPN module includes remote access services, as well as VPNaccess devices.

WAN moduleThe WAN module includes the traditional enterprise WAN. Connections from remote offices, external vendors, and SOHO connections are aggregated on a distribution layer device, then handed off through the Edge Distribution module of the Enterprise Campus functional area to the campus backbone.

Service Provider Edge ModulesThe Service Provider Edge functional area includes three modules. These functions are not generally implemented by the enterprise itself; instead, they are purchased services. Nevertheless, they do involve network connectivity. The three modules are as follows:

Internet Service Provider moduleAs the name implies, each ISP is a separate module. They are attached to the Enterprise Edge Internet Connectivity, Remote Access and VPN, and E-Commerce modules. Multiple ISPs can provide higher availability.

PSTN moduleThe PSTN module represents the dial-up components of the enterprise network. ISDN, POTS, and cellular technologies are all included in this module. DDR WAN backup links may also be included.

Frame Relay/ATM moduleThe Frame Relay/ATM module includes all WAN technologies used within the enterprise. Contrary to its name, this module includes more than just Frame Relay and ATM; it also includes SONET, DSL, wireless, leased lines, and any other permanent WAN connections.

QUESTION 182:

Which of the following items of information is least relevant when designing a new campus network for a customer who wants to improve the performance of their

campus network?

A. Number of users
B. Applications in use
C. Future growth
D. Location of wiring closets
E. Network speed

Answer: D

Explanation:
While designing the network, you should think about:
- Number of users in network
- Types of Application in network
- Any plan to growth another networks
- Required Network speed for services

QUESTION 183:

RMON is being used within the Certkiller NOC. In which layer does RMON belong to?

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 4
E. Layer 5
F. Layer 6
G. Layer 7

Answer: B
Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs. RMON works at the MAC sublayer which is part of the Data Link layer (Layer 2).

QUESTION 184:

For the network backbone of a large campus environment, what are three advantages of a multilayer core switch design over a Layer 2 core switch design? (Choose three)

A. Single VLAN implementation in the backbone
B. Reduced distribution router peering
C. Broadcast control in the backbone

D. Evenly distributed backbone traffic
E. Large scalability potential

Answer: B, C, E

Explanation:
Multilayer switching has been described as the next architectural generation of LAN switching. [Communications Week, 1997] Although the definition for multilayer switches is not standardized, they can be described as switches that besides MAC layer routing, have some routing layer functionality like multicast and broadcast containment, some VLAN services (used for broadcast control in the backbone), and Packet filtering and firewalling between two VLANs. They may also support Transmission Control Protocol/Internet Protocol (TCP/IP) and Internetwork Packet Exchange (IPX) routing, allowing for reduced router peering.
One of the most important features would be that it provides gigabit level scaling. This makes it easier and cheaper to upgrade the network in future when the demands on the network increase, increasing scalability.

QUESTION 185:

The logical diagram of two different networks is shown below:
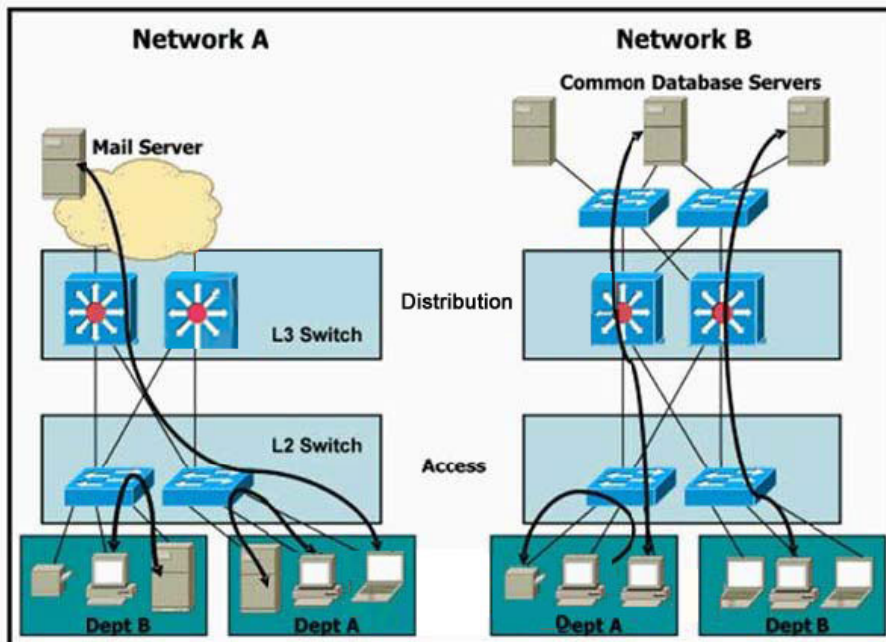
The two networks shown in the diagram have very different traffic patterns, as illustrated by the black arrows. Network A in this diagram has several independent departments, each with its own VLAN in which printers and servers are located. The only common resource is the mail server. Network B also has several departments but they use common server resources. Which network represents 80/20 rule in a campus network?

A. Network A
B. Network B
C. Both networks are needed to achieve an 80/20 rule effect.
D. Neither network represents to 80/20 rule.
E. Both networks combined represents the 80/20 rule.

Answer: A

Explanation:
Virtual LAN support for virtual workgroups is often tied to support of the "80/20 rule,"
that is, 80 percent of the traffic is "local" to the workgroup while 20 percent is remote or
outside of the workgroup. In theory, by properly configuring VLANs to match
workgroups, only the 20 percent of the traffic that is nonlocal will need to pass through a
router and out of the workgroup, improving performance for the 80 percent of the traffic
that is within the workgroup. As shown by the traffic patterns pertaining to these two
networks, only network A correctly represents this 80/20 rule.

QUESTION 186:

You are the network administrator at Certkiller . Certkiller has just hired a new
study guide writer. The study guide writer must be able to communicate with the
Certkiller office in Washington from her home in Lyon. In particular, she must be
able to access the Certkiller web server and send e-mail with attachments
throughout your entire 8-hour workday.
Which technology would be the most cost effective for the new study guide writer to
use?

A. DSL
B. ISDN
C. Satellite
D. Leased Line

Answer: A

Explanation:
With DSL she will able to access web server and email server. This is fixed cost, and
always on.
Reference:
Incorrect Answers
B: ISDN is a costly solution. She may not able to send large attachments.
C: This is also a very costly solution. In addition, the link may fail due to atmospheric
interference such as cloud cover and humidity.
D: Leased line will be for short data transfers.

QUESTION 187:

What does a multi-layer LAN use to switch data outside of the source network?

A. Information stored in RIP tables.
B. Information stored in OSPF tables.
C. Information stored in bridging tables.
D. Information stored in route processors.
E. Information stored on the DNS servers.

Answer: D

Explanation:
Using route processors switch the packets faster than fast switching, because it has an enhanced caching algorithm and switching cache.
Reference:
Incorrect Answers
A, B: RIP and OSPF tables are used on Routers.
C: Bridging tables are used on Bridges
E: This is used to name to IP address resolution.

QUESTION 188:

You are a network engineer at Certkiller . One of your newly appointed Certkiller trainees wants to know why firewalls are necessary.
What will your reply be?

A. It will maintain separate routing information for each protocol.
B. Reduces routing loops by restricting the flow of routing information.
C. It provides a security buffer, protection between a private network and connected public networks.
D. It is responsible for user authentication between a private network and connected public networks.

Answer: C

Explanation:
Firewall Protect network from outside world. It is hardware/software or combination of both, used to block or permit network traffic,
Reference:
Incorrect Answers
A: This is not function of firewall
B: Firewalls not bother about routing loops
D: Firewalls are used to filter packets

QUESTION 189:

You are the technician at Certkiller . Your newly appointed Certkiller trainees wants

to know which mechanisms can be used to provide Virtual Private Networking
(VPN) functionality at Layer 2.
What will your reply be? (Choose all that apply.)

A. Tunnelling/GRE
B. Leased Line
C. Sonet/SDH
D. Frame Relay
E. ATM
F. All of the above.

Answer: D, E

Explanation:
Frame Relay and ATM operates on Layer 2. Using these two mechanisms one can
connect to Internet. Then using VPN remote user can access corporate network using
internet
Incorrect Answers
A, B, C, F: They are not working in Layer 2

QUESTION 190:

At which layers of the OSI reference model do WAN technologies operate? (Choose all
that apply.)

A. Application
B. Presentation
C. Session
D. Transport
E. Network
F. Data Link
G. Physical

Answer: E, F, G

Explanation:
Wan Technologies operate from the Physical layer where it take the bits and turns it into
packets, up to the network layer for routing purposes. Data link layer is responsible for
switching packets.

QUESTION 191:

You are the network administrator at Certkiller . Certkiller has its head office located
in Washington and three branches located in Boston, St Louis and New Orleans.
The company wants connectivity between the branch offices with full redundancy
and high availability.

What topology should you implement?

A. Star hub and spoke
B. Point to point
C. Partial mesh
D. Full mesh
E. Bus

Answer: D

Explanation: Full redundancy requirement indicates a Full mesh topology.

QUESTION 192:

A medium sized accounting firm, Certkiller , has four offices around the country.
There head office is situated in London and the branches are in Manchester,
Liverpool and Newcastle. Certkiller wants to establish connectivity between offices,
but with a limited budget they cannot afford to splash out.
What topology would be suitable for Certkiller ?

A. Partial mesh
B. Token Ring
C. Star hub and spoke
D. Frame Relay
E. Full mesh

Answer: C

Explanation:
For small to medium sized companies, the hierarchical model is often implemented as a
hub and spoke topology.
Reference: Designing Cisco Networks (Ciscopress) page 93

QUESTION 193:

Your newly appointed Certkiller trainee wants to know which of the following
modules are associated with an edge distribution functional area of an enterprise
composite network model.
What will your reply be? (Select two.)

A. Campus infrastructure
B. Internet connectivity
C. Edge security
D. WAN
E. Workgroup Switching
F. None of the above

Answer: B, D

Explanation:
There are 4 modules associated with the Edge Distribution
E-Commerce
Internet Connectivity (B)
Remote Access and VPN
WAN (D)
Note:
The edge distribution module is similar in some respects to the building distribution
module in terms of overall function. Both modules employ access control to filter traffic,
although the edge distribution module can rely somewhat on the entire edge functional
area to perform additional security functions. Both modules use Layer 3 switching to
achieve high performance, but the edge distribution module can add additional security
functions because the performance requirements are not as great. The edge distribution
module provides the last line of defense for all traffic destined to the campus module
from the edge module. This includes mitigation of spoofed packets, erroneous routing
updates, and provisions for network layer access control.
Reference:
http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00800
9

QUESTION 194:

The Certkiller network consists of two locations that are connected via satellite
point-to-point link. The users experience low response time and very low error rates
when employing data communications over this particular link.
Which statement describes the effect of flow control using window size for the
highest end-to-end throughput?

A. A small window size will keep the number of retransmissions to a minimum
B. A large window size reduces the number of acknowledgments
C. A small window size will enhance performance
D. Insufficient information to determine the effect window size
E. none of the above

Answer: B

Explanation:
Some protocols, such as Novell's traditional NetWare Core Protocol (NCP), use a
"ping-pong" approach, where each request generates a reply. This approach is an
inefficient use of bandwidth, but it can be replaced by the burst mode protocol. With
burst mode, a station can send as much data as there is room in the receiver's "receive
window".

In the TCP/IP suit, the TCP supports windowing and flow control.
Reference: Designing Cisco Networks (Ciscopress) page 74

QUESTION 195:

When employing a VPN solution, which types of threats should you be concerned about? (Select all that apply.)

A. Denial of Service (DoS) attacks.
B. Distributed Denial of Service (DDoS) attacks.
C. Data confidentiality.
D. Network mapping.
E. Internet Viruses.
F. IP Spoofing.

Answer: C, F

QUESTION 196:

The Certkiller trainee technician wants to know what the default encapsulation for synchronous serial interfaces on Cisco routers is. What will your reply be?

A. ATM
B. HDLC
C. GRE
D. PPTP
E. Frame Relay
F. All of the above

Answer: B

Explanation:
By default, synchronous serial lines use the High-Level Data Link Control (HDLC) serial encapsulation method, which provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. Synchronous serial interfaces support the following serial encapsulation methods for dial solutions:
* High-Level Data Link Control (HDLC)
* Point-to-Point Protocol (PPP)

QUESTION 197:

Certkiller is a medium sized accounting firm that has four offices around the country. The head office is in Phoenix with branches in Boston, Chicago and Los Angeles. Certkiller wants connectivity between these offices with minimal expense due to a limited budget.
What topology would you recommend for Certkiller ?

A. Partial mesh
B. Ring
C. Star hub and spoke
D. Full mesh

Answer: C

Explanation:
The star topology specifies a core router that serves as the hub for the WAN connections. Designers often refer to this topology as a hub-and-spoke topology. The core router connects to each of the branch offices; in fact, branch offices can only communicate with each other if they pass their communications though the core (hub) router. The star topology features the advantage of simplified and centralized management of the WAN topology.
Reference: Cisco CCDA self-study v2 (Page 195)

QUESTION 198:

The application of which of the technologies listed below over the Internet will permit the retaining of security policies while lowering WAN lease expenses by the organization implementing it.

A. ADSL
B. VPN
C. VLANs
D. ATM

Answer: B

Explanation:
A Virtual Private Network (VPN) is defined as network connectivity deployed on a shared infrastructure with the same policies and security as a private network.
A VPN can be between two end systems, or it can be between two or more networks. A VPN can be built using tunnels and encryption. VPNs can occur at any layer of the OSI protocol stack. A VPN is an alternative WAN infrastructure that replaces or augments existing private networks that use leased-line or enterprise-owned Frame Relay or ATM networks.
VPNsprovide three critical functions:
1. Confidentiality (encryption)- The sender can encrypt the packets before transmitting them across a network. By doing so, no one can access the communication without permission. If intercepted, the communications cannot be read.
2. Data integrity- The receiver can verify that the data was transmitted through the Internet without being altered.
3. Origin authentication- The receiver can authenticate the source of the packet, guaranteeing and certifying the source of the information.

QUESTION 199:

The Certkiller network administrator is contemplating the use of ODR in the Certkiller network. Which network design is most appropriate for On-Demand Routing (ODR)?

A. Stub networks in a hub and spoke topology.
B. Metro optical ring topology.
C. Highly redundant mesh topology.
D. Counter-routing dual ring campus topology.

Answer: A

Explanation:
On-Demand Routing is not a routing protocol. It uses Cisco Discovery Protocol (CDP) to propagate the IP prefix. ODR is a perfect solution for hub and spoke topology when the spoke routers act as stub routers by connecting to no other router other than the hub. If you only use Cisco routers in your network, running Cisco IOS(r) 11.2 or later, you can use ODR. If you are running dynamic protocols (for instance, if you are an ISP), ODR is not suitable for your network environment.
Reference:
http://www.cisco.com/en/US/tech/ CK3 65/technologies_q_and_a_item09186a0080093f1a.shtml

QUESTION 200:

Which kind of address translation is best when the servers on the internal network with private IPv4 addresses must be visible from the public network?

A. Many-to-one translation (PAT)
B. Many-to-one translation (Dynamic NAT)
C. One-to-one translation (Static NAT)
D. One-to-one translation (NAT Traversal)
E. None of the above

Answer: C

Explanation:
Developed by Cisco, Network Address Translation is used by a device (firewall, router or computer) that sits between an internal network and the rest of the world. NAT has many forms and can work in several ways including static NAT described below:
Static NAT - Mapping an unregistered IP address to a registered IP address on a one-to-one basis, which is particularly useful when a device needs to be accessible from outside the network.
In this static NAT example, the computer with the IP address of 192.168.32.10 will always translate to 213.18.123.110:

Static NAT is most often used for Internet facing servers that need to be accessed from outside the internal network, such as FTP and web servers.

QUESTION 201:

An analysis of the 258 kbps wan link for a network shows that the link is not usually congested. However, delay-sensitive applications are often hampered when large packets block access. What is this problem called and what are two possible solutions? (Choose three)

A. Link layer fragmentation and interleaving.
B. Use different VLANs for each application type.
C. Serialization delay.
D. Compressed real-time protocol.
E. Use different subinterfaces for each application type.
F. Packetization delay.

Answer: A, C, D

Explanation:
The problem described in this question is the serialization delay with large packets being transmitted over slow, congested links. This is especially
As shown in Table 1, the amount of serialization delay (the time it takes to actually place the bits onto an interface) introduced on low-speed WAN links can be significant, considering that the target end-to-end one-way delay should not exceed 150ms. (ITU-T G.114 recommendation specifies 150 ms maximum one-way end-to-end.)
Table 1. Serialization Delay for Various Frame Sizes on Low-Speed Links
Serialization Delay = frame size (bits)/link bandwidth (bps)

	1 Byte	64 Bytes	128 Bytes	256 Bytes	512 Bytes	1024 Bytes	1500 Bytes
56 kbps	143 us	9 ms	18 ms	36 ms	72 ms	144 ms	214 ms
64 kbps	125 us	8 ms	16 ms	32 ms	64 ms	126 ms	187 ms
128 kbps	62.5 us	4 ms	8 ms	16 ms	32 ms	64 ms	93 ms
256 kbps	31 us	2 ms	4 ms	8 ms	16 ms	32 ms	46 ms

512 kbps	15.5 us	1 ms	2 ms	4 ms	8 ms	16 ms	32 ms
768 kbps	10 us	640 us	1.28 ms	2.56 ms	5.12 ms	10.24 ms	15 ms
1536 kbps	5 us	320 us	640 us	1.28 ms	2.56 ms	5.12 ms	7.5 ms

Note:
For voice applications, recommended serialization delay (per hop basis) is 10 ms and should not exceed 20 ms.
As a solution to the serialization delay problem, Link Fragmentation and Interleaving as well as the Compressed Real Time Protocol, described below:
Link Fragmentation and Interleaving (LFI): Multilink PPP
While 1500 bytes is a common size for data packets, a typical VoIP packet (carrying G.729 voice frames) can be around 66 bytes (20 bytes voice payload, 6 bytes layer-2 header, 20 bytes RTP & UDP header, and 20 Bytes IP header).
Now, imagine a 56Kbps leased line link where voice and data traffic coexist. If a voice packet is ready to be serialized just when a data packet starts being transmitted over the link, then there is a problem. The delay-sensitive voice packet has to wait 214 msec before being transmitted (it takes 214 msec to serialize a 1500 bytes packet over a 56Kbps link).
As you can see, large data packets can adversely delay delivery of small voice packets, reducing speech quality. Fragmenting these large data packets into smaller ones and interleaving voice packets among the fragments reduces jitter and delay. The Cisco IOS Link Fragmentation and Interleaving (LFI) feature helps satisfy the real-time delivery requirements of VoIP. This image illustrates the operation of LFI:
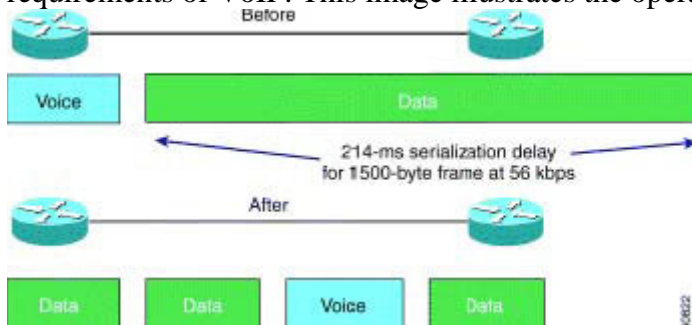
Compressed Real-time Protocol (cRTP)
Note:cRTP is not required to ensure good voice quality. It is a feature that reduces bandwidth consumption. Configure cRTP after all other conditions are met and the voice quality is good. This procedure can save troubleshooting time by isolating potential cRTP issues.
Based on RFC 2508, the RTP header compression feature compresses the IP/UDP/RTP header from 40 Bytes to 2 or 4 bytes, reducing unnecessary bandwidth consumption. It is a hop-by-hop compression scheme; therefore, cRTP must be configured on both ends of the link (unless the passive option is configured).
Reference: http://www.cisco.com/warp/public/788/voice-qos/voip-mlppp.html

QUESTION 202:

Router CK1 has just been configured with IP multicast. If you configure PIM with Sparse Mode in this router connected with a switch, in which interfaces it will be transmitted? (Select two)

A. All interfaces of the router and of the switch
B. Just the interfaces of the switch that request the multicast signal
C. Just the interfaces of the router connected with the switch that requests the signal
D. It won't be propagated by the router

Answer: B, C
PIM Sparse Mode requires devices to request to get the multicasts.
Besides, both answers A and D cannot be correct since they contradict the other choices and you must choose 2.

QUESTION 203:

DRAG DROP
Match the submodules of the Enterprise Composite Network Model with the functions they would perform for a Voice Network design.

Select from these	Place here	Description
Building Access	Place here	fast packet switching
Building Distribution	Place here	concentrates wiring closets
Campus Backbone	Place here	IP phone power
Server farm	Place here	connections to call managers

Answer:

Select from these	Place here	Description
	Campus Backbone	fast packet switching
	Building Distribution	concentrates wiring closets
	Building Access	IP phone power
	Server farm	connections to call managers

Explanation:

The Enterprise Composite Network model is a model that provides a functional modular approach to network design. In addition to a hierarchy, modules organize server farms, network management, and the Enterprise Edge.
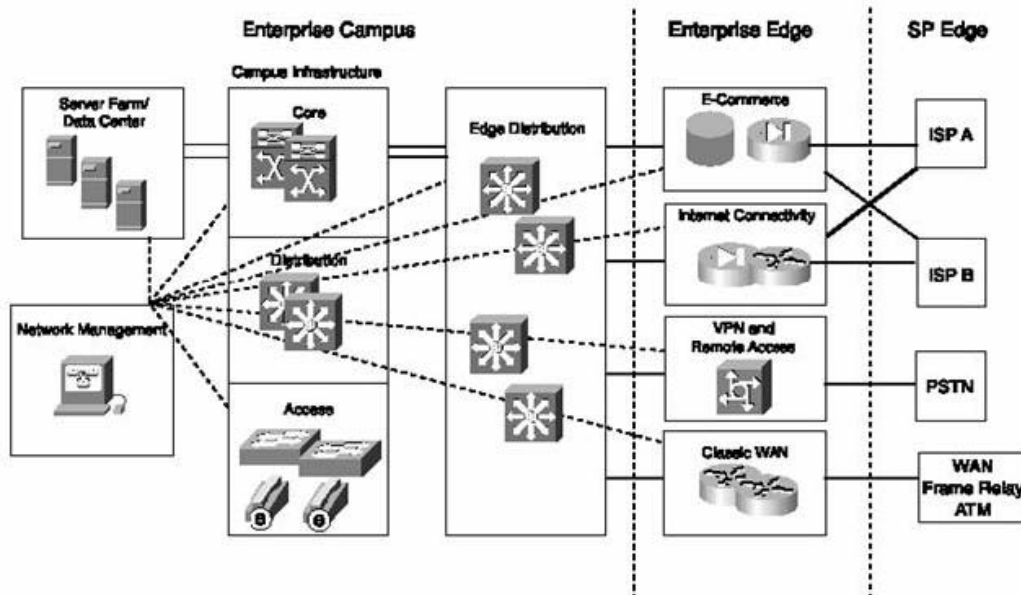
An enterprise-campus infrastructure can apply to small, medium, and large locations. In most instances, large campus locations have a three-tier design with a wiring-closet component (buildingaccess layer), a building-distribution layer, and a campus-core layer. Small campus locations likely have a two-tier design with a wiring-closet component (Ethernet access layer) and a backbone core (collapsed core and distribution layers). It is also possible to configure distribution functions in a multilayer building-access device to maintain the focus of the campus backbone on fast transport. Medium-sized campus network designs sometimes use a three-tier implementation or a two-tier implementation, depending on the number of ports, service requirements, manageability, performance, and availability required.

QUESTION 204:

Your newly appointed Certkiller trainee wants to know which of the following modules form part of the Enterprise Campus functional area of Enterprise Composite Network models.
What will your reply be? (Choose all that apply.)

A. E-Commerce module
B. Server Farm module
C. Network Management module
D. Remote Access module
E. Server Edge moduleF. All of the above

Answer: B, C
Explanation
Enterprise Campus - Campus network with backbone, distribution, and access
infrastructure; also includes server farm and network management.
Source: CCDA Exam Certification Guide Second Edition, Page 624

QUESTION 205:

Your newly appointed Certkiller trainee wants to know which security function is performed in the Server Farm module of the Enterprise Composite Network Model. What will your reply be?

A. port security
B. packet filtering
C. private VLANs
D. AAA controls

Answer: A

Explanation:
Not D: is not the correct answer as AAA control works for routers and switches only, not the servers.

QUESTION 206:

Which of the following phrases are best defined by the PDIOO process?

A. Is the design phase of the network life cycle.
B. Is the network life cycle phase that leverages organizational knowledge.
C. Reflects the life cycle of the network.
D. Reflects the organizational policy structure of the network.

Answer: C

Explanation:
Cisco Advanced Services incorporates a unique three tiered program offering a real world life cycle process to help you achieve your business objectives. Depending on individual operational, maintenance, and network level requirements, each customer has unique support requirements throughout the network life cycle of planning, designing, implementing, operating, and optimizing the network (PDIOO).

QUESTION 207:

What is introduced by the Enterprise Composite Network Model to the network design process?

A. Hierarchical network design
B. Modularity within major functions.
C. The concept of core, distribution, and access layers of a network.
D. Flattening of the network model for simplicity.

Answer: B

Explanation:
The Cisco Enterprise composite Network model facilitates the design of larger, more scaleable network. As networks become more sophisticated, it is necessary to use a more modular approach to design than just WAN and LAN core, distribution and access layers. The model divides the network into functional components, functional areas containing network modules.
Reference: Cisco CCDA self-study v2 (Page 84)

QUESTION 208:

Which of the following are the functional areas of the Enterprise Composite Network Model? (Choose two)

A. enterprise edge
B. enterprise management
C. enterprise campus
D. enterprise commerce
E. enterprise backbone
F. enterprise provider edge

Answer: A, C

Explanation:
The Enterprise Composite Network model divides the network into three major functional components:
1. Enterprise Campus
2. Enterprise Edge
3. SP Edge
Reference: Cisco CCDA self-study v2 (Page 84)

QUESTION 209:

Enterprise Campus Functional Area
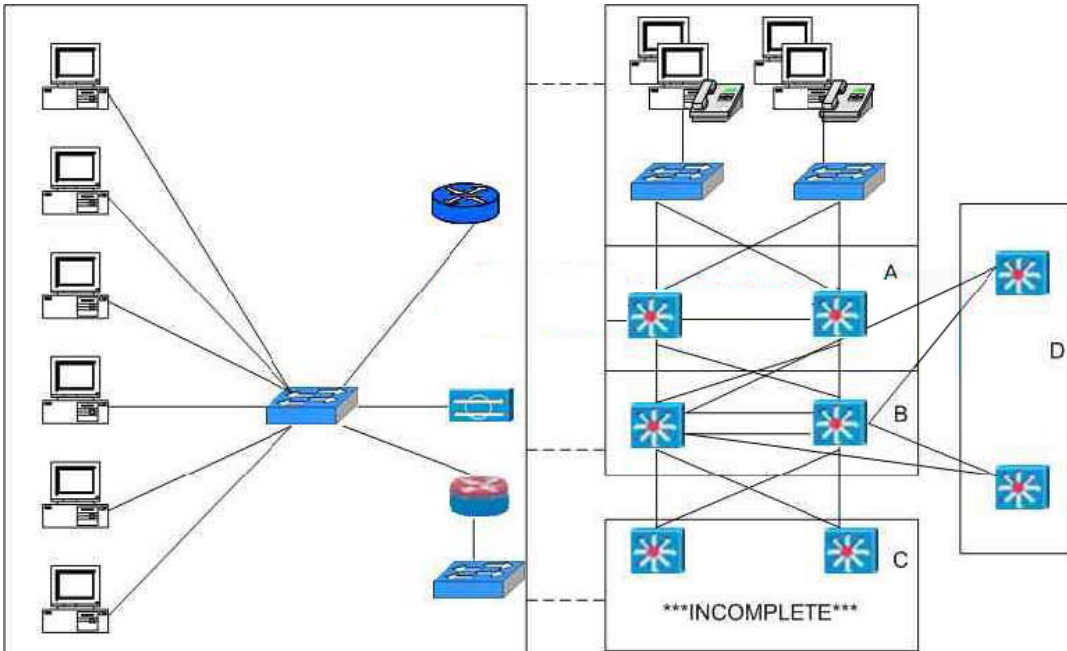
Use the diagram of the Enterprise Composite Network Model; identify the diagram section indicated by the "B".

A. Server Farm module
B. Network Management module
C. Building Access submodule
D. Building Distribution submodule
E. Campus Backbone (core) submodule
F. Edge Distribution module

Answer: E

Explanation:
It is Campus Backbone (core) submodule because:
Part "B" consists from routers which are situated in the middle of the network. The routers and switches from other layers are connected to them with redundant uplinks.
This characterizes the core layer of Cisco model.

QUESTION 210:

The Certkiller logical diagram is displayed below:
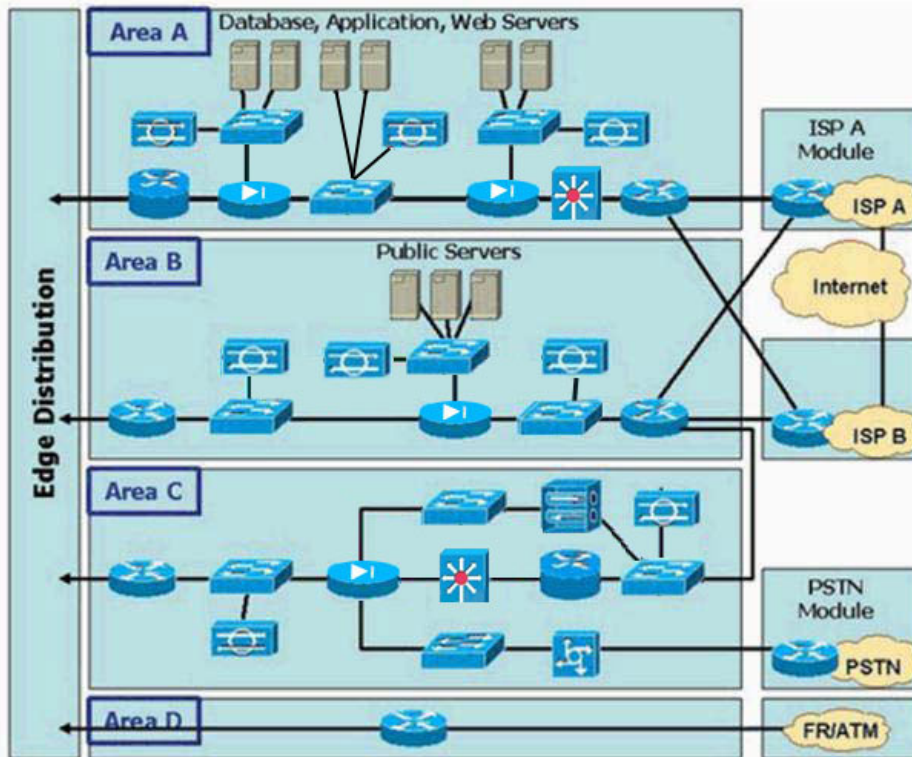
Which three statements accurately reflect this Enterprise Edge functional area diagram? (Choose three)

A. Area B is the Internet Connectivity module.
B. The WAN module is illustrated by Area B.
C. The VPN/Remote Access module is reflected in Area D.
D. The Internet Connectivity module is comprised of the ISP, PSTN, and FR/ATM modules.
E. The WAN module is shown as Area D.
F. Area C represents the VPN/Remote Access module.

Answer: A, E, F

Explanation:
A: Area B shows the public (Internet) facing servers, such as the web, FTP, and email servers. It also directly shows the connection to the ISP.
E: Area D displays the logical layout of the internal WAN, as shown by the connection to the frame relay/ATM network.
F: Area C must be used as the VPN and remote access module, as shown by the connection to the PSTN (telephone) network, which remote users use to dial in to the network or use a VPN.

QUESTION 211:

Which two modules are found in the Enterprise Edge functional area of the

Enterprise Composite Network Model? (Choose two.)

A. Campus Infrastructure
B. Internet Connectivity
C. WAN
D. Edge Security
E. Workgroup Switching

Answer: B, C

Explanation:
EnterpriseEdge Modules
The Enterprise Edge consists of the following modules:
1. E-commerce networks and servers
2. Internet connectivity
3. VPN and remote access
4. Classic WAN
E-Commerce Module
The e-commerce module provides highly available networks for business services. It uses the highavailability designs of the server-farm module with the Internet connectivity of the Internet module. Design techniques are the same as those described for these modules.
Internet Module
Several models connect the enterprise to the Internet. The simplest form is to have a single circuit between the enterprise and the SP.
VPN/Remote Access Module
The VPN/remote access module provides remote-access termination services, including authentication for remote users and sites. If you use a remote-access terminal server, this module connects to the PSTN network. Today's networks often prefer VPNs over remote-access terminal servers and dedicated WAN links. VPNs reduce communication expenses by leveraging the infrastructure of SPs. For critical applications, the cost savings might be offset by a reduction of enterprise control and the loss of deterministic service. Remote offices, mobile users, and home offices access the Internet using the local SP with secured IP Security (IPSec) tunnels to the VPN/remote access module via the Internet module.
WAN Module
The Enterprise Edge includes access to WANs. WAN technologies include the following:
1. Wireless
2. PSTN
3. Leased lines
4. Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH)
5. PPP
6. Frame Relay
7. ATM
8. Cable
9. Digital subscriber line (DSL)

QUESTION 212:

An existing Cisco customer has called for help with designing a new solution for its changing needs. The first issues the customer wants to address are security, logging, and troubleshooting. On which major functional area and which sub-module of the Enterprise Composite Network Model will you be keying your efforts?

A. Enterprise Edge; Internet Connectivity
B. Enterprise Campus; Network Management
C. Service Provider; ISP
D. Campus Infrastructure; Building Access
E. Enterprise Campus; Campus Infrastructure
F. Edge Distribution; Call Detail Log

Answer: B

Explanation:
The Enterprise Campus module - Network Management module supports security, monitoring, logging, troubleshooting, and other common management features from end to end.
Reference: Page 132 in CiscoPress CCDA Self-Study: Designing for Cisco Internetwork Solutions DESGN 640-861. ISBN : 1587051419, Third printing June 2005

QUESTION 213:

During which phase of the PDIOO process should the implementation be planned?

A. Planning
B. Design
C. Implementing
D. Operating
E. Optimizing
F. Instigating

Answer: B

Explanation:
Design is just one component of a network lifecycle. Planning, design, implementation, operation, and optimization (PDIOO) are the different stages of the network lifecycle. Each stage builds on its predecessor, developing a sound network that maintains its effectiveness through changing business needs. You can apply the PDIOO methodology to all echnologies. During this PDIOO process, you define key deliverables and associated actions, with a direct correlation to the added value and benefit for the client's network. For example, understanding business goals, usage characteristics, and network requirements helps you avoid unnecessary upgrades and network redesigns, reducing time for introducing new services in the network. Discussions in this chapter revolve around these five main stages.
After completing the planning stage, you have enough information to develop a network design. If a network is already in place, use this phase to review and validate it. At this stage, you choose products, protocols, and features based on criteria defined in the planning stage. You develop network diagrams to

illustrate what changes will occur in the network to achieve the desired results. The more detailed the network diagram and plan, the better you can anticipate the challenges during the implementation.

QUESTION 214:

You are the network administrator at Certkiller . You have a problem of voice traffic that has been affected by variable delay. Which measures can you deploy at the receiving end of a converged network to help smooth voice traffic?

A. Reducing compression level.
B. Link fragmentation and interleaving.
C. Dejitter buffers.
D. Increasing the compression level.
E. All of the above.

Answer: C

Explanation:
Digital voice circuits use dejitter buffers to change this random variable delay to a more tolerable fixed delay.
Source: CCDA Exam Certification Guide Second Edition, Page 140

QUESTION 215:

What is the recommended maximum network response time to ensure that productivity remains high and the quantity of user complaints remains low?

A. 50 milliseconds
B. 100 milliseconds
C. 150 milliseconds
D. 200 milliseconds

Answer: C

Explanation:
Page 478 of Cisco CCDA Self-Study states "The generally accepted limit for good-quality voice connection delay is 150 milliseconds(ms) one-way."
The ITU describes voice delay in G.114, which states 0-150ms is an acceptable delay.

QUESTION 216:

You are the network administrator at Certkiller . Your newly appointed Certkiller trainee wants to know what a tie trunk (tie line) is used for.
What will your reply be?

A. To interconnect two PBX switches.

B. To interconnect a PBX and a CO switch (exchange).
C. To interconnect a PBX and a remote telephone.
D. To interconnect a CO switch (exchange) and a remote telephone.
E. To interconnect two CO switches.

Answer: A

Explanation:
A trunk (tie-line) is a permanent point-to-point communication line between two voice ports. The connection trunk command creates a permanent Voice over IP (VoIP) call between two VoIP gateways. It simulates a trunk connection by creating virtual trunk tie-lines between two telephony endpoints. To the connected systems, it appears as if a T1 trunk was directly connected between them.
Reference:
http://www.cisco.com/en/US/tech/ CK6 52/ CK7 01/technologies_configuration_example09186a00800afd65.shtml

QUESTION 217:

What is the reason why one cannot use PCM codecs that are meant for use in Europe and parts of Asia in North America or Japan?

A. Echo cancellation
B. Noise suppression
C. Code companding
D. Band limiting
E. None of the above

Answer: C

Explanation:
A-law: An ITU-T companding standard used in the conversion between analog and digital signals in PCM systems. The A-law is used primarily in European telephone networks and is similar to the North American u-law standard.
U-law: A companding technique commonly used in North America. U-law is standardized as a 64-kbps codec in ITU-T G.711.
Source: CCDA Exam Certification Guide Second Edition

QUESTION 218:

A PBX switchboard is connected to a Europe Public service by making use of three ISDN PRI(T1) circuits only. Hence only one signaling channel is being used for all three PRI circuits.
What is the maximum number of bearer channels that can carry voice calls (provided that the traffic offering allows it) in this case?

A. 92
B. 190
C. 72
D. 71
E. 171

Answer: D

Explanation: If anISDN PRI (T1) is 23B +D, then 3 ISDN PRI T1's using only 1
signaling channel (non-facility associated signaling)for all three='s 24 x 3 = 72 - 1=
71.
ISDN Non-Facility Associated Signaling (NFAS) allows a single D channel to control
multiple PRI interfaces. Use of a single D channel to control multiple PRI interfaces frees
one B channel on each interface to carry other traffic.

QUESTION 219:

Certkiller wants to run voice traffic over an existing frame relay network. However,
the company does not want to deploy IP telephones at this point in time.
What networking hardware would Certkiller use to accommodate meet this
objective?

A. CallManager
B. Voice gatekeeper
C. Voice gateway
D. Multi Control Unit (MCU)
E. Frame Relay Access Device (FRAD)

Answer: C
A voice gateway should be used. For example, a voice enabled Cisco router with a FXS
card.
Incorrect
Answer:
A: Call Manager is software. You would use for IP Phones.
B. Voice Gatekeeper - Manages call control for voice gateways
D. Multi Control Unit - Not applicable
E. FRAD - Not Applicable

QUESTION 220:

Your newly appointed Certkiller trainee wants to know how one can associate a
phone number with a physical voice port on a voice-enabled router.
What will your reply be?

A. Configure automatic router selection
B. Configure a dial-peer

C. Enable voice over the voice port
D. Configure the voice port
E. Enable voice over IP

Answer: B

QUESTION 221:

You are the technician at Certkiller and received an instruction to design a
converged network that will be able to carry voice traffic. Which of the following
mechanisms will you use to prioritise different types of traffic?

A. Grade of service (GoS).
B. Quality of service (QoS).
C. Dial peers.
D. Call legs.
E. All of the above.

Answer: B

Explanation:
Increasingly data networks are being called upon to support communications for traffic with
varied delivery requirements. Previously an organization used separate networks for voice, video,
and data traffic. It is now common practice to combine these into a single multiservice network in
which the varied traffic types coexist. There are many circumstances where these Quality of
Service (QoS) requirements have not been met or even addressed at a rudimentary level:
1. The long delay in speech transmission when calling by way of an international satellite link
2. Stop-start and choppy Internet streaming video performance
3. Harsh audio when using an Internet-based IP phone
4. Messenger applications are all examples of inadequate QoS
For many applications such as file and print services, Internet browsing, email and peer-to-peer
messaging products, the "best effort" delivery attempts of the Internet and many corporate
networks may be adequate. However, for organizations seeking to integrate their voice and data
networks using Voice over IP (VoIP), IP telephony or high quality streaming video for corporate
communications, it is essential that QoS be built into the design of the network.
In order to provide QoS within a network it is critical to have an understanding of the network
characteristics that make up quality of service and the QoS requirements of the varied traffic and
applications using the network. Once application and traffic requirements can be stated in QoS
terms, classification techniques are used to identify streams of traffic as having a particular QoS
requirement. For example, a standard access-list could be used to identify a user who requires
priority access to the network resources. Once traffic has been classified into classes of service,
there are many scheduling and congestion management techniques that can be used to provide
the desired service characteristics. The key to effective QoS design is knowing how these
techniques operate and the benefits and limitations of each.
QoS refers to the ability of a network to provide improved service to selected network traffic over
various underlying technologies including Frame Relay, ATM, Ethernet and 802.3 networks,

SONET, and IP-routed networks.
QoS features provide improved and more predictable network service by offering the following
services:
1. Dedicated bandwidth
2. Improved loss characteristics
3. Congestion management and avoidance
4. Traffic shaping
5. Prioritization of traffic

QUESTION 222:

Which of the following codecs does Cisco recommend for WAN links when reducing the required bandwidth
over a converged
network for each voice call?

A. G.711
B. G.723
C. G.728
D. G.729

Answer: D

Explanation:
VoIP calls need to meet bandwidth and delay parameters. The amount of bandwidth required
depends on the codec used, the Layer 2 protocols, and whether VAD is enabled. For the purpose
of call control, you can use the following bandwidth requirements for VoIP design:
1) G.729 calls use 24 Kbps
2) G.723 calls use 24 Kbps
3) G.711 calls use 80 Kbps
G.729 codec uses less bandwidth than others.
Reference: Ciscopress page 448

QUESTION 223:

You are the technician at Certkiller and received an instruction to test a converged
network. Upon doing the verification tests you discover that long distance calls goes
off-net at the local office in stead of going via a remote office. When you try to put a
long distance call through to the remote office, the remote voice gateway sends a
busy-back signal.
Which changes in the design can rectify this situation?

A. Modify the queuing mechanism
B. Add WAN capacity between the local and remote voice gateways
C. Configure more capacity between the remote voice gateway and its PBX
D. Add local PSTN trunk capacity

Answer: B

Explanation:
Cisco built upon the classic hierarchical network model (access, distribution, core) to provide network designers with the Enterprise Composite Network model. The classic hierarchical model always suffered from scalability and manageability weaknesses. Cisco recommends use of the Enterprise Composite Network model to provide the functional components for network design. This model is aligned with the current Cisco "best practice" for building converged networks that provide security and other network services to support the transport of voice, video, and data.

QUESTION 224:

How is grade of service (GoS) put to use when designing a converged network?

A. In reducing the need for QoS
B. To prioritize different types of traffic
C. In planning trunk capacity
D. As a means of calculating dial peers
E. As a mechanism for prioritizing H.323 traffic

Answer: C

Explanation:
Grade of service (GoS) is the probability of a call being blocked when attempting to seize a circuit. If a network defines P.02 GoS, the probability is that two percent of all attempted calls will be blocked.
Reference: Cisco press p. 432

QUESTION 225:

What is used on a router to associate physical voice ports with phone numbers in Cisco VoIP implementation?

A. Automatic route selections
B. Translation patterns
C. IP telephony
D. Dial peers
E. All of the above

Answer: D

Explanation:
POTS dial peers define the phone numbers or prefixes of attached telephony devices, and the VoIP dial peers define the IP address of the remote device (H.323 GW, GK, or endpoint) that is connected to remote phone numbers. POTS dial peers will always point

to a voice port on the router, while the destination of a VoIP dial peer will always be the IP address of a device that can terminate the VoIP call.

QUESTION 226:

A Voice over Frame Relay (VoFR) network is experiencing delay and delay variation due to serialization of packets of varying size. This condition is causing voice quality problems.
Which of the following solutions can be added to the network at the sending end to reduce these problems?

A. hardware digital signal processors
B. link fragmentation and interleaving
C. dejitter buffers
D. coding algorithm

Answer: B

Explanation:
LinkFragm can be used on sendig interface.Dejitterinto receiverinterface

QUESTION 227:

Which two technologies are capable of reducing the amount of VoIP-call generated traffic? (Choose two)

A. grade of service (GoS)
B. quality of service (QoS)
C. voice activation detection (VAD)
D. compressed real-time transport protocol (Crtp)
E. automatic route selection

Answer: C, D

Explanation:
As we listen and pause between sentences, typical voice conversations can contain up to 60 percent silence in each direction. In circuit-switched telephone networks, all voice calls use fixed-bandwidth, 64 Kbps links regardless of how much of the conversation is speec and how much is silence. In multiservice networks, all conversation and silence is packetized. Using VAD, you can suppress packets of silence. Silence suppression at the source IP telephone or VOIP gateway increases the number of calls or data volumes that can be carried over the links, more effectively utilizing network bandwidth.
CRTP compresses the IP/UDP/RTP headers from 40 bytes to 2/4 bytes. It is configured on a link-to-link basis. Cisco recommends using CRTP for links lower than 768 Kbps.
Do not configure CRTP if the router CPU is above 75 percent utilization.
Reference: Designing Cisco Networks (Ciscopress) page 448,451.

QUESTION 228:

What provides reliable connections to Cisco CallManagers in a voice-network design?

A. building access
B. building distribution
C. enterprise edge
D. server farm

Answer: D

Explanation:
The server-farm or data-center module provides high-speed access to servers for the campus networks.
You can attach servers to switches via Fast Ethernet or Gigabit Ethernet. Some campus deployments might need EtherChannel technology to meet traffic requirements.
The server-farm switches connect via redundant uplink ports to the core switches. The largest deployments might find it useful to hierarchically construct service to the data center using access and distribution network devices.

QUESTION 229:

You've designed a converged network to carry voice calls on-net as close as possible to the destination to avoid long distance charges. Which two are reasons that a VoIP call could go off-net earlier than designed? (Choose two)

A. Remote voice gateway sending busy-back signal.
B. Destination routing not configured on local and remote gateways.
C. Call manager server is too busy to process the call.
D. The telephone user dials an access code.

Answer: A, D

Explanation: Off-net happens when the user dials an access code or the On-net resources are not available which can be for 2 reasons; the far end has no available circuit and gives a buy signal back or the near end sees there is not enough bandwidth.
Reference: Page 506 in CiscoPress CCDA Self-Study: Designing for Cisco Internetwork Solutions DESGN 640-861. ISBN : 1587051419, Third printing june 2005

QUESTION 230:

VOIP has been deployed within the Certkiller network. Which IP telephony component controls, processes, and delivers the voice stream?

A. IP telephone
B. Inline power switches
C. Cisco CallManager
D. Voice gateway
E. None of the above

Answer: C

Explanation:
Cisco CallManager is the software-based call-processing component of the Cisco IP
telephony solution. The software extends enterprise telephony features and functions to
packet telephony network devices such as IP phones, media processing devices,
voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and
video services such as unified messaging, multimedia videoconferencing, collaborative
contact centers, and interactive multimedia response systems interact with the IP
telephony solution through Cisco CallManager's open telephony application
programming interface (API).

QUESTION 231:

You are a technician at Certkiller . Your newly appointed Certkiller trainee wants to know
which components are included in the original Cisco SAFE architecture.
What would your reply be? (Choose all that apply.)

A. SP Edge
B. SAFE VPN
C. Enterprise Edge
D. Multicast Router
E. Enterprise Campus

Answer: A, C, E

Explanation:
SAFE architecture blue print includes security in enterprise networks, mid size, remote
access networks, IPSec, SP edge which includes wireless and IP telephony.
Incorrect Answers
B: The SAFE VNP is not in the original Cisco SAFE architecture.
D: The SAFE Architecture does not include hardware such as routers.
Reference:
http://www.cisco.com/global/ME/breakfree/pdfs/SAFE_blueprint.pdf

QUESTION 232:

In the Cisco SAFE Architecture, what does the Enterprise Campus consist of? (Choose
all that apply.)

A. Server
B. WAN
C. Corporate Internet
D. Building Distribution
E. Core

Answer: A, D, E

Explanation:
Server is Required Enterprise networks. Distribution layer is required for Policies; Core
is mainly connected to Service Providers.
Incorrect Answers
B,C: WAN & Corporate Internet are not in the SAFE Architecture

---

QUESTION 233:

Which of the following modules comprise the Enterprise Composite Network Model?
(Choose all that apply.)

A. Enterprise Campus
B. Enterprise Edge
C. Enterprise Server Edge
D. Enterprise Core Backbone
E. Service Provider Edge

Answer: A, B, E

Explanation:
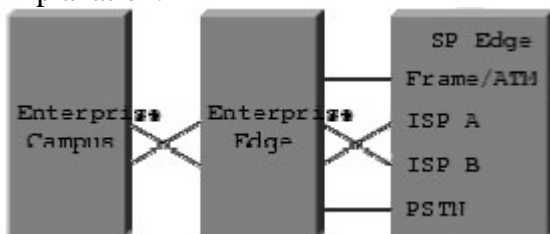
The second layer of modularity, which is illustrated in Figure 2, represents a view of the
modules within each functional area. These modules perform specific roles in the
network and have specific security requirements, but their sizes are not meant to reflect
their scale in a real network. For example, the building module, which represents the
end-user devices, may include 80 percent of the network devices. The security design of
each module is described separately, but is validated as part of the complete enterprise
design.
Reference: SAFE: A Security Blueprint for Enterprise Networks

---

QUESTION 234:

Which of the following steps are involved in a network security design? (Choose all that

apply)

A. Analysis of security risks.
B. Training of users, managers, and technical staff.
C. Identification of network assets.
D. Identification of routing protocol metrics.
E. Analysis of security requirements and tradeoffs.

Answer: A, B, C, E

Explanation:
Identify security requirements of the new network, do the following:
* Appraise security risks and determine how much security will be needed and of what type.
* Determine requirements for outsiders to access data
* Determine the authorization and authentication requirements for corporate branch offices, mobile users, and telecommuters.
* Identify any requirements for authenticating routes received from access routers or other routers.
* Identify any requirements for host security, such as physical security of hosts, user accounts, dated software, access rights on data, and so on.
C should be included in answer because if you have to know what devices you have in your network
Reference: Designing Cisco Networks (Ciscopress) page 70

QUESTION 235:

Your newly appointed Certkiller trainee wants to know which of the following forms part of the Campus function area of the Enterprise Corporate network model.
What will your reply be? (Choose all that apply.)

A. E-commerce module
B. Network Management module
C. Server Farm module
D. Remote Access module
E. All of the above

Answer: B, C

Explanation:
Management Module
The primary goal of the management module is to facilitate the secure management of all devices and hosts within the enterprise SAFE architecture. Logging and reporting information flow from the devices through to the management hosts, while content, configurations, and new software flow to the devices from the management hosts.
Server Module

The server module's primary goal is to provide application services to end users and devices. Traffic flows on the server module are inspected by on-board intrusion detection within the Layer 3 switches.
Reference: SAFE: A Security Blueprint for Enterprise Networks

---

QUESTION 236:

You are a network administrator at Certkiller and have been instructed to design as well as implement a SAFE network. You have done so, but now the users on the network complain that they still encounter some DoS attacks on specific hosts in the E-commerce module. You already patched the operating systems on the servers as well as discontinue all unnecessary services.
What else can you do to ameliorate the effects of these attacks?

A. Block all TCP traffic to these servers at the internet firewall
B. Practice Load-balancing between multiple servers with similar applications
C. Place limitations on the connection rate to the servers at the internet firewall
D. Block all UDP traffic to these servers at the internet firewall

Answer: C

QUESTION 237:

Which of the following recommendations will you make when asked to propose a security option to protect servers in the E-commerce module of a network? (Choose all that apply.)

A. Implement intrusion detection on the E-commerce server farm.
B. Limit the number of incoming connections to reduce the risks.
C. Place application servers and E-commerce servers in separate DMZs.
D. Move the E-commerce application servers to the WAN module where tighter security is used.
E. Implement a private and public key encryption system.

Answer: A, C
A: Intrusion detection on both hosts and network intrusion detection in most segments are used to detect attack attempts and perhaps respond to some of the attack automatically.
C: A good firewall design places both servers in separate DMZ networks with firewalls in between and allows only the necessary e-commerce application connections.
Page 584 - 585 in CiscoPress CCDA Self-Study: Designing for Cisco Internetwork Solutions DESGN 640-861. ISBN : 1587051419, Third printing june 2005

QUESTION 238:

Your newly appointed Certkiller trainee wants to know which of the following can
be associated with remote access and VNP security modules in a SAFE network, as
threats.
What will your reply be? (Choose all that apply.)

A. Data transmission confidentiality
B. DdoS directed at the network resources
C. Snooping
D. Network mapping
E. Identity spoofing
F. DoS directed at exposed hosts
G. None of the above

Answer: A, E

Explanation:
A Virtual Private Network (VPN) is defined as network connectivity deployed on a shared
infrastructure with the same policies and security as a private network.
A VPN can be between two end systems, or it can be between two or more networks. A VPN can
be built using tunnels and encryption. VPNs can occur at any layer of the OSI protocol stack. A
VPN is an alternative WAN infrastructure that replaces or augments existing private networks that
use leased-line or enterprise-owned Frame Relay or ATM networks.
VPNs provide three critical functions:
1. Confidentiality (encryption) - The sender can encrypt the packets before transmitting them
across a network. By doing so, no one can access the communication without permission. If
intercepted, the communications cannot be read.
2. Data integrity - The receiver can verify that the data was transmitted through the Internet
without being altered.
3. Origin authentication - The receiver can authenticate the source of the packet, guaranteeing
and certifying the source of the information.
VPNs offer many advantages over traditional, leased-line networks. The primary benefits include:
1. VPNs offer lower cost than private networks. Total cost of ownership is reduced through
lower-cost transport bandwidth, backbone equipment, and operations. LAN-to-LAN connectivity
costs are typically reduced by 20 to 40 percent over domestic leased-line networks. Cost
reduction for remote access is in the 60 to 80 percent range.
2. VPNs offer flexibility for enabling the Internet economy.VPNs are inherently more flexible and
scalable network architectures than classic WANs. This enables enterprises to quickly and
cost-effectively extend connection or disconnection of remote offices, international locations,
telecommuters, roaming mobile users, and external business partners as business requirements
demand.
3. VPNs offer simplified management burdens compared to owning and operating a private
network infrastructure. Enterprises may outsource some or all of their WAN functions to a service
provider, enabling enterprises to focus on core business objectives, instead of managing a WAN
or dial-access network.
4. VPNs provide tunneled network topologies that reduce management burdens. An IP backbone
eliminates static permanent virtual circuits (PVCs) associated with connection-oriented protocols

such as Frame Relay and ATM. This creates a fully meshed network topology while decreasing network complexity and cost.

Virtual Private Networking enables the benefits of a private network over the larger shared IP infrastructure of the Internet. Benefits include privacy and the use of multiple protocols.

A virtual network is created through the ability to tunnel multiple protocols over a standard IP connection. Generic Routing Encapsulation (GRE) and Layer 2 Tunneling Protocol (L2TP) are two methods of this tunneling and are both configurable on Cisco Routers. The third method, IPSec, is also configurable on Cisco Routers and is the key focus of this VPN module.

A private network is one that ensures Confidentiality, Integrity and Authentication (CIA). Encrypting data and using the IPSec protocol enables data to traverse the Web with the same CIA as with a private network.

QUESTION 239:

The manufacturing company Certkiller has decided to add the web site to enhance sales. The WEB-Servers in the E-commence module must be accessible without compromising network security.
Which two design accommodation these requirement

A. Use intruder detection in the E-Commerce Server farm
B. Limit the number of in coming connection to E-Commerce server module
C. Place the E-Commerce server and Application Server isolated LAN (DMZ)
D. Move E-commerce server to the WAN module to prevent tight security
E. Use Private and Public key encryption

Answer: A, C
A: Intrusion detection on both hosts and network intrusion detection in most segments are used to detect attack attempts and perhaps respond to some of the attack automatically.
C: A good firewall design places both servers in separate DMZ networks with firewalls in between and allows only the necessary e-commerce application connections.
Page 584 - 585 in CiscoPress CCDA Self-Study: Designing for Cisco Internetwork Solutions DESGN 640-861. ISBN : 1587051419, Third printing june 2005

QUESTION 240:

Which technology can ensure data confidentiality, data integrity, and authentication across a public IP network?

A. VLANs
B. VPDN
C. IPSec
D. GRE

Answer: C

Explanation:
IPSec is a framework of open standards developed by the Internet Engineering Task
Force (IETF) that provides security for transmission of sensitive information over
unprotected networks such as the Internet.
IPSec provides a obust security solution and is standards-based. IPSec also provides data
authentication and anti-replay services in addition to data confidentiality services

---

QUESTION 241:

DRAG DROP

Drag the Internet Connectivity module risk to the threat that causes it

| Reconnaissance threats on the Internet |
| Comprmise of exposed host and applications |
| Comprmising a host from other compromised hosts |
| DOS attacks directed at exposed hosts |
| DOS attacks directed at network links |
| Malicious code |

SYN flood sent to the web server	Place here
Multigigabit stream of ICMP messages	Place here
Ping all systems in the enterprise	Place here
Hacker can view or change all enterprise e-mail	Place here
Public web server hacker gets to internal data	Place here
Trojan horse sends passwords fro the attacker	Place here

Answer:

Drag the Internet Connectivity module risk to the threat that causes it

SYN flood sent to the web server	DOS attacks directed at network links
Multigigabit stream of ICMP messages	Malicious code
Ping all systems in the enterprise	DOS attacks directed at exposed hosts
Hacker can view or change all enterprise e-mail	Compromising a host from other compromised hosts
Public web server hacker gets to internal data	Compromise of exposed host and applications
Trojan horse sends passwords fro the attacker	Reconnaissance threats on the Internet

Explanation:
Packet Sniffing
Useful network tools can become threats in the hands of a hacker. A packet sniffer provides an example of
how someone can exploit a tool used to capture all packets on physical wire (promiscuous mode). A
packet-sniffer application is common tool for traffic analysis and troubleshooting by capturing and
decoding packets. You can use packet sniffers to capture and inspect all unencrypted data (clear text),
which can include usernames and passwords or critical information. Hackers can use this information to
attack the network and user applications. Some ways to prevent packet-sniffing attacks include
authentication, cryptography, and network segmenting:
1. Authentication methods such as two-factor authentication (using token cards that generate a random

password, which is used in conjunction with a user password), which uses a one-time password, mitigate subsequent attacks using false credentials for authentication and some replay attacks.

2. Cryptography is the most common and effective method of securing data against sniffers because it scrambles the clear text. IP Security (IPSec), SSH, and SSL are common encryption protocols.

3. Segmenting the network using switches can help to localize the sniffer's activity.

IP Spoofing

IP spoofing is a technique in which the attacker sends packets with the source IP address modified to match that of a trusted host. IP spoofing can also disguise the source of packets launched as part of a DoS attack. Some ways to prevent IP spoofing attacks are authentication and filtering:

1. Authentication prevents access to systems based solely on IP address.

2. With filtering (see RFC 2827), you can prevent a network's users from spoofing other networks from your networks by preventing any outbound traffic on your network that does not have a source address in your organization's own IP range.

DoS

DoS

attacks deny legitimate users access to services. DoS attacks are characterized by disrupting connectivity between devices, preventing access to specific services, halting processes on devices by sending bad packets, and flooding networks.

Some ways to prevent DoS attacks follow:

* Properly configure firewalls and routers to prevent DoS attacks. You can find these configurations on vendor and security websites.

* Prevent spoofing.

* Prevent traffic rates from getting out of control.

QUESTION 242:

Which of the following statements is valid when developing a network design implementation plan?

A. The implementation design plan must be supervised and monitored by the designer to ensure success.
B. Fallback steps are obsolete if a detailed pilot completes successfully.
C. Many implementation steps can be performed simultaneously to limit time wastage.
D. Implementation steps described in detail can be performed by a less-experienced engineer.
E. None of the above.

Answer: D

Explanation:
If you specify the related to functionality, scalability, adaptability, Manageability & cost-effectiveness clearly and elaborately, implementation can be done be less experience engineer
Incorrect Answers
A: Success is measured by customer. The customer measures success from a business standpoint

B: This will not play any role in network design implementation.
C: The steps should be carried in an order.
E: This possibility is negated by option D.

QUESTION 243:

Which three items of information should each set of implementation plans consist of?
(Choose all that apply.)

A. A description of the objective of each step.
B. Detailed implementation guidelines.
C. Reference to a section in the design document.
D. A summary of requirements to be fulfilled by each step.
E. A listing of applicable device configurations.

Answer: A, B, C

Explanation:
Objective of the network have to be clearly defined. Define step by step guide lines of
design goals and reference section in design document is required.
Incorrect Answers
D,E : Summary and Listing of applicable devices are not main items

---

QUESTION 244:

You are a network engineer at Certkiller . Your inexperienced Certkiller trainee is
implementing the design.
Which of the following steps should you consider?

A. Make the design implementation description as detailed as possible.
B. Have the designer carry out the complex implementation steps.
C. Prevent detailed steps that require the involvement of other staff members.
D. Create less detailed implementation steps that exclude the direct involvement of the
designer.

Answer: A

Explanation:
Steps for Determining a Customer's network Requirements
Determining a customer's requirements for a new network design I s one of the most
important tasks in internetwork design. This section provides a step-by-step approach to
determining these requirements. This approach will ensure the network design
specifically meets the needs of the customer. You might want to take a copy of this
outline with you to the customer's site and use it as a checklist when requesting
information.
Step1. Identify business constraints

Step2. Identify security requirements
Step3. Identify manageability requirements
Step4. Determine application requirements
Step5. Characterize new network traffic
Step6. Identify performance requirements
Step7. Create a customer needs specification document
Reference: Designing Cisco Networks (Ciscopress) page 69

QUESTION 245:

You are the network administrator at Certkiller . You want to implements a
three-part firewall system on the Certkiller network as a security measure.
Which of the following components would be included in this solution? (Choose all that
apply.)

A. A router acting as an inside packet filter.
B. An independent WAN.
C. An isolation LAN.
D. A router acting as an outside packet filter.
E. A Web server.

Answer: A, C, D

Explanation:
The classic firewall system, called the three-part firewall system, has the following
three
specialized layers:
* Isolation LAN
* Inside packet filter
* Outside packet filter
Reference: Designing Cisco Networks (Ciscopress) page 103

QUESTION 246:

Your newly appointed Certkiller trainee wants to know what information will have
to be included in implementation to allow for the further gathering of details when
characterizing a current network.
What will your reply be? (Choose all that apply.)

A. Corporate policies regarding protocols and standards.
B. Corporate policies with regard to certain vendors and applications.
C. Reference to design documents.
D. Availability of trained personnel within the organization.
E. Budgetary resource limitations.
F. None of the above.

Answer: C

Explanation:
In Step3 of characterizing a Customer's Current Network, you need a network topology.
Reference: Designing Cisco Networks (Ciscopress) page 55

QUESTION 247:

Which of the following issues can you prepare yourself to face if you use a design
plan that consists of multiple, complex implementation steps.
(Choose all that apply.)

A. budgetary constraints
B. intricate, difficult troubleshooting
C. less time necessary to revert to previous states in case of failure
D. more time necessary to revert to previous states in case of failure
E. corporate policies regarding protocols, standards, vendors, and applications
F. all of the above

Answer: B, D

QUESTION 248:

Which aspect of network design would be of concern if the company involved
consist of a small number of IT staff with minimal networking skills and the only
down time allotted is midnight until 6:00 AM once a week?

A. choice of design model
B. choice of network hierarchy
C. implementation schedule
D. choice of vendors when purchasing switches
E. security considerations

Answer: C

Explanation:
Finally, set up a time and present the pilot to the customer. If you have prepared well,
your confidence level should be high and your presentation should go smoothly. Be
courteous of the customer's time and be prepared to answer any questions the customer
may have after you complete your demonstrations.

QUESTION 249:

Your newly appointed Certkiller trainee wants to know which statement regarding
the steps to an implementation plan would be valid.
What will your reply be?

A. Each step should list prerequisites for that particular step
B. The designer should supervise each step of the implementation
C. Each step should have a number of phases to carry out
D. Each step should detail roll-back guidelines in case of failure

Answer: D
Implementation of the design has several phases. Each phases consists of
several steps. Documentation should contain the following:
A description of the step
Reference to the design document
Detailed implementation guidelines
Detailed roll-back guidelines in case of failure
The estimated time that is necessary for implementation
Page 95 in CiscoPress CCDA Self-Study: Designing for Cisco Internetwork
Solutions DESGN 640-861. ISBN : 1587051419, Third printing june 2005
Not C: Each step should not have several phases as this can cause more extensive
troubleshooting and more time to effect a rollback in case of failure.

QUESTION 250:

Study the Exhibit of a section of an implementation plan carefully:

Certkiller Deploy Step # 3-1 Layer 2 switch configuration at Certkiller headquarters campus

- Refer to Design Document Section 3.1.1.0
- Implementation Guidelines
    - Configure separate VLAN for each wing on each floor.
    - Configure Spanning Tree domain
    - Configure specific port settings
        - Duplex
        - Speed
        - Portfast
    - Security
    - Configure Trunk links
- Old Switches will stay in closets for possible roll-back

You are a network administrator at Certkiller and have been instructed to write an
implementation plan for an intricate network design that is intended for a customer
who is a large financial institution. You have just written the deployment step to
configure the switches that are to be used in the design.
What information is outstanding from the above exhibit?

A. A failsafe mechanism
B. Applicable technical constraints
C. Contingency plan in case this step fails
D. Implementation constraints
E. Applicable timeline for this step

Answer: E

Explanation:
We believe this question refers to the phased implementation idea which involves 5 steps;
1. Description
2. Reference to design sections
3. Detailed implementation guidelines
4. Detailed roll-back guidelines in case of failure
5. Estimated time for implementation
In our opinion what is missing in its entirety is step 5 and somewhat step 4 since all that is mention is that "old switches will stay in closets for possible roll-back". Option D "implementation constraints" is not even a part of the phased implementation. Therefore option E is the correct one.

QUESTION 251:

The large company Certkiller .com has a new network design with many complex implementation steps.
How can troubleshooting efforts are minimize during implementation

A. By utilizing additional staff implementation
B. By implementing each step separately
C. By completing the entire design plan then revert to previous state in case of failure
D. By deferring testing a unit of implementation of all step is complete

Answer: B

QUESTION 252:

DRAG DROP
You are a trainee technician at Certkiller . Your instructor tells you to build a prototype network.
Match the following steps on the left to the correct actions on the right.

Step 1		Determine how much of the network structure must be built to prove that the design meets the customers goals.
Step 2		Gain an understanding of what your competition intends to propose.
Step3		Review extracted new customer requirements.
Step 4		Purchase and configure equipment.
Step 5		Practice demonstrations.
Step 6		Develop a test plan.

Answer:

Step 2	Determine how much of the network structure must be built to prove that the design meets the customers goals.
Step3	Gain an understanding of what your competition intends to propose.
Step1	Review extracted new customer requirements.
Step 5	Purchase and configure equipment.
Step 6	Practice demonstrations
Step 4	Develop a test plan.

Explanation:
Steps of creating prototype
Step 1: Review the requirements. Determine the major goals. Outline the proof required to demonstrate that your design works. Determine possible problem areas that might affect your design.
Step 2: Determine the extent of the prototype. Determine how much of the design must be built into a prototype to be effective. Identify the tools you can use to simplify the prototype.
Step 3: Understand alternative proposals. Work with others to identify the products and designs in alternative proposals. If information is not available, speculate on what competing proposals might use. Research information on alternative products by referencing websites, industry articles, and evaluations.
Step 4: Develop a test plan. Draw a network diagram. List tools for the test. List the plan scheduling, resources, and milestones. Prepare the demonstrations. Determine how each test will prove that the design meets the requirements. Determine how each test will show that the alternative products provide an inferior solution.
Step 5: Purchase and prepare equipment. You must acquire and prepare some or all of the following equipment:
Network-simulation tools

Protocol analyzers
Industry tests
Network hardware and software
Routers
Switches
Network-management tools
End-system hardware and software
Application servers
File servers
Step 6: Practice. Practice your demonstration to include the necessary elements from the
previous step.
Step 7: Conduct final tests and demonstrations. Test your configuration using the
following tools:
Cisco IOS Software commands
Protocol analyzers
Simulation tools

QUESTION 253:

You are contracted as a network administrator for Certkiller Inc. You must produce
evidence to the CEO regarding a proposed new campus network that uses Layer 3
switching. Since the company is still small, it cannot allow you to interrupt work
performance as the network is critical to business.
Which of the following approaches will you take?

A. Pilot network approach
B. Verification design approach
C. Prototype network approach
D. Live network approach

Answer: C

Explanation:
IN this method build smaller representation of network design. In Prototyping situation
be sure to build those segments of the network that had worst MTBF record to test how
your design improves it. Test most critical portions of the network.
Reference:
CCDA Study guide by Damon Merchant. Syngress Press
Incorrect Answers
A: If network is small build pilot network. It will be less expensive than pilot
D: Live network should not demonstrate any new design. This may disturb existing
behavior.
B: Verification design to be performed on Lab network.

QUESTION 254:

You are a network administrator at Certkiller and have been instructed to test a proposed network redesign solution. You successfully tested the proposed redesign solution with a prototype network. But when put into operation in the live network, the network performance is seriously hampered.
What was wrong with the prototype network test?

A. The prototype should have been built on the live network.
B. The prototype design network was configured with different parameters.
C. The prototype failed to test for the proper characteristics.
D. The prototype network was not a proper match for the live network.

Answer: C

Explanation:
Network Health Checklist
Use the following checklist when checking a prototype or pilot for proper network functionality and scalability. This checklist provides guidelines, not rules. As mention in chapter 3, "Characterizing the Existing Network," the correct answer to questions regarding thresholds for network health is usually, "it depends." Thresholds depend on topologies, router configurations, network applications, user requirements, how measurement tools calculate thresholds, and many other factors.
Reference: Designing Cisco Networks (Ciscopress) page 278

A. Provides connectivity to remote offices.
B. Provides policy-based routing services.
C. Connects shared LAN devices.
D. Provides connectivity to end-users.
E. Provides route summarization services.

QUESTION 255:

Which testing techniques can be used as proof of concept of a network design? (Choose all that apply.)

A. A pilot network.
B. A simulation lab.
C. A modular network.
D. A prototype network.
E. A verification network.

Answer: A, D

Explanation:
A prototype of a network is an implementation of a portion of the network to prove that the design meets the requirements. A pilot is simply a scaled-down prototype used to

demonstrate basic functionality.
Reference: Designing Cisco Networks (Ciscopress) page 267

QUESTION 256:

Which of the following serves as rationale for making use of a prototype network
instead of a pilot network when testing a network redesign? (Choose all that apply.)

A. cheaper to implement
B. more flexible test environment
C. more available options to test
D. has no impact on a live network
E. more accurate test results
F. more modeling tools available

Answer: B, E

Explanation:
For larger configurations, a prototype is more feasible. For smaller configurations, a pilot
might be more practical. The decision will probably be made on relative cost; the costs
for prototyping a portion of network will be relatively small for a large network.
Reference: Designing Cisco Networks (Ciscopress) page 267

QUESTION 257:

You are the technician at Certkiller and received an instruction to improve the
Internet performance on the company network. You thus decided to test a proxy
server in the live network so as to generate the appropriate, necessary traffic load.
What is this type of test called?

A. Simulation
B. Blueprinting
C. Pilot
D. Conformance
E. Prototype

Answer: C

Explanation:
pilot or prototype of your proposed internetwork may be necessary to prove that your
design actually meets the customer's requirements. The data produced by a pilot or
prototype can be a powerful tool as you present your design and (hopefully) win the
customer's business. The saying that "talk is cheap" certainly applies here. Anyone can
claim that their design will work; here is where you prove that your design actually
works.
The idea behind a pilot or prototype is that you do not need to build the entire

internetwork to prove that your design works. Many times that simply isn't feasible. Instead, you can select key components of the internetwork, implement them, and then test them under simulated real-world conditions. The difference between a pilot and prototype is largely one of scale. These differences can be summarized as follows:
A pilot is smaller in scale, and thus requires less money and time to implement. It is useful to prove small portions of your design.
A prototype is larger than a pilot in scale, but smaller than the finished internetwork; you don't just order the internetwork and set it up, complete in a warehouse somewhere. A prototype can be used to prove sections or entire modules of your design.
Your customer will likely drive the choice between implementing a pilot or prototype. There are costs involved in completing either one. Your customer should be involved in deciding just how extensive your testing needs to be. The following sections describe the steps you need to take to implement either a pilot or prototype.

QUESTION 258:

DRAG DROP

Drag the prototype system test definition on the top to the test it defines

Quantifies performance from a user's point of view

Calculates the amount of work that an application or applications can do in a given time period

Measures the rate and failures under a mdium to heavy load over a 24 to 72 hour period

Ensures the prototype does not break any working applications.

Availability	Place here
Throughput	Place here
Regression	Place here
Application response time	Place here

Answer:

Drag the prototype system test definition on the top to the test it defines

Availability	Measures the rate and failures under a medium to heavy load over a 24 to 72 hour period
Throughput	Quantifies performance from a user's point of view
Regression	Ensures the prototype does not break any working applications.
Application response time	Calculates the amount of work that an application or applications can do in a given time period

QUESTION 259:

What are three important elements that a good prototype test plan should include?
(Select three)

A. A verification of the behavior of the system
B. The development of test objectives and acceptance criteria
C. The documentation of network equipment and other resources
D. An integration into the existing network ... with off-hour testing
E. Determination of the scope of the prototype
F. The generation of scripts that define initial values

Answer: A, B, E

Explanation:
By exclusion:
C: Not needed since the design plan has all of this already
D: Incorrect since this is a prototype and it does not affect the existing network, time of testing is irrelevant.
F: This isn't mentioned anywhere when talking about pilot/prototypes and the other answers (A,B,E are much better answer choices).

QUESTION 260:

DRAG DROP
You are a trainee technician at Certkiller . Your instructor tells you to build a pilot.
Match the following steps on the left to the correct actions on the right.

Step 1		Investigate the competition.
Step 2		Test the design.
Step 3		Practice the demonstration.
Step 4		Schedule and present the demonstration.
Step 5		Script a demonstration of the test results.

Answer:

Step 2	Investigate the competition.
Step 1	Test the Design.
Step 4	Practice the demonstration.
Step 5	Schedule and present the demonstration.
Step 3	Script a demonstration of the test results.

Explanation:

Steps Required for a Pilot Implementation

As mentioned, a pilot is simply a small test. It is useful for a small network design, or if only a small component of a larger design needs to be demonstrated. At a minimum, Cisco recommends the following steps for implementing a pilot:

Test the design.You should test your design and verify that it will work before proceeding with the pilot. A pilot is not an ad-lib, preliminary test infront of the customer. You do not want any surprises when you go in front of the customer with your pilot, so verify your design with actual testing before proceeding with the pilot. If your design fails at this point, re-evaluate your design and retest it.

Investigate what the competitors will be proposing.Cisco recommends you be aware of what the competition will propose. If you know what the competition is doing, you can prepare to present reasons why your design is superior. You may wish to outline the features of your design that are not supported by other vendors and demonstrate these as part of your pilot. For example, if you are aware of specific IOS features that are useful to the customer, but not available in products proposed by other vendors, use this time to demonstrate those features.

Write a script for the demonstration.

Prepare a script of your presentation before you actually give it. This will keep you focused as you present. Your script should focus on several issues. First and foremost, your test should prove that your design will satisfy the customer's requirements. Your test is also an opportunity to showcase your company's technical expertise and the power and scalability of Cisco's solutions. Don't be afraid to demonstrate any potential problems with the competition's solutions atthis point. As mentioned earlier, talk is cheap.

However, if you script side-by-side comparisons, be able to demonstrate both the acceptability ofyour solution and any problems with the competition's solutions. Practice the demonstration. As mentioned, a pilot is not a first shot. It is ascripted, practiced, real-time demonstration of a solution. Make sure to practice the demonstration ahead of time. Of course, this is no guarantee that nothing will go wrong. However, your confidence level will be significantly higher if you are not wondering how your demonstration will turn out.

Schedule time with the customer and present the pilot.Finally, set up a time and present the pilot to the customer. If you have prepared well, your confidence level should be high and your presentation should go smoothly. Be courteous of the customer's time and be prepared to answer any questions the customer may have after you complete your demonstrations.

QUESTION 261:

Which of the following represents a way to measure the Mean Time Between Failure (MTBF) for an internetwork?

A. Capacity
B. Response time
C. Availability
D. Bandwidth usage
E. Utilization
F. Efficiency

Answer: C

Explanation:
Step6: Characterize the Existing Network Availability
Gather statistics on network downtime and the mean time between failure (MTBF) for the internetwork.
Reference: Designing Cisco Networks (Ciscopress) page 57

QUESTION 262:

You arte a network administrator at Certkiller .com. The company is preparing to do business with partners over the internet. Certkiller will use dialup links for this purpose. You are required to ensure the security these transactions. In particular, you need to ensure both the privacy and integrity of the data being transferred over untrusted networks. You also want to identity the users initiating these transactions. In verification and test plan, how would you verify that privacy requirements have been satisfied?

A. Observer the applications transactions.
B. Capture and analyze packets for cipher text.
C. Compare checksum on send and received packets.

D. Inspect logs for telephone number of dial-back customers.

Answer: B

Explanation:
Testing
You can also use a protocol analyzer to generate traffic when testing a prototype or pilot.
Reference: Designing Cisco Networks (Ciscopress) page 55

QUESTION 263:

Which of the following are methods used on tolls to verify a network design
produced by network modeling tools, decision table, and strategic analysis tools?
(Choose two.)

A. A pilot or prototype network
B. Redesign documentation
C. Simulation and test tool
D. Network management tools

Answer: A, C

Explanation:
A Pilot or Prototype
A pilot or prototype of your proposed internetwork may be necessary to prove that your
design actually meets the customer's requirements. The data produced by a pilot or
prototype can be a powerful tool as you present your design and (hopefully) win the
customer's business. The saying that "talk is cheap" certainly applies here. Anyone can
claim that their design will work; here is where you prove that your design actually
works.
The idea behind a pilot or prototype is that you do not need to build the entire
internetwork to prove that your design works. Many times that simply isn't feasible.
Instead, you can select key components of the internetwork, implement them, and then
test them under simulated real-world conditions. The difference between a pilot and
prototype is largely one of scale. These differences can be summarized as follows:
A pilot is smaller in scale, and thus requires less money and time to implement. It is
useful to prove small portions of your design.
A prototype is larger than a pilot in scale, but smaller than the finished internetwork; you
don't just order the internetwork and set it up, complete in a warehouse somewhere. A
prototype can be used to prove sections or entire modules of your design.
Your customer will likely drive the choice between implementing a pilot or prototype.
There are costs involved in completing either one. Your customer should be involved in
deciding just how extensive your testing needs to be. The following sections describe the
steps you need to take to implement either a pilot or prototype.
Simulation and Test Tool
During the final step, you must present the prototype design for usability testing. Some

common basic tools that can make demonstrations more effective are
1. Protocol analyzers
2. Simulation tools
3. Cisco IOS commands
An insightful design methodology helps the network designer define the network's technical and business requirements and work through all phases of the technology lifecycle of PDIOO. Documenting the gathered information is critical, and a complex network design might require demonstrating that the design meets the project requirements using a network prototype.

QUESTION 264:

Certkiller .com requires that a network designer show proof of concept for a redesigned remote access solution that will be implemented in the Enterprise Edge functional area of an existing network. Budget and time constraints require testing in only a portion of the existing Remote Access module.
Which kind of test will be used to show proof of concept?

A. Pilot
B. Prototype
C. Simulation
D. Isolated
E. None of the above

Answer: A

Explanation:
The last step in creating a successful design solution is demonstrating to the customer how your design solution meets that customer's needs for performance, security, capacity, and scalability.
Often the designs proposed are complex and have many different components that must be brought together to build a complete solution. Usually a more complex design means a greater cost to the customer. Therefore, it is important that the consultant provide sound proof to the customer that the proposed design will meet the customer's needs.
Two methods demonstrate to the customer how the proposed design will solve that customer's network needs. The first method is to build a prototype, which is used for larges scale designs. The second is to construct a pilot, which is a smaller and less complicated version of the prototype that is ideal for smaller designs. In this example, a pilot would be more appropriate.
Reference: CCDA Exam Certification Guide,
A. Anthony Bruno, CCIE #2738, p.282

QUESTION 265:

Which three items are foundational to identifying and validating information about possible problems in an existing network? (Choose three)

A. Customer input
B. Organizational procedures
C. Traffic analysis
D. Top-down network design
E. Draft Design Document
F. Network audit

Answer: A, C, F

Explanation:
Identifying the information regarding the possible problems in an existing network : One of the main source is gathering the information from customer from where you take input and start to find out the possible problems.
During the network-design process, there might be tools available to facilitate some of the activities. Some of the activities supported by tools include network auditing, traffic analysis, and network simulation. The choice of tools is very much determined by the value of the network investment and the consequences of network failure. This section discusses some of the tools and techniques used in today's network-design process for auditing networks and analyzing and simulating network traffic.
Network audit tools will help you generate specific reports on certain parts of your network and analyze how these segments of the network are performing. The network audit process should provide detailed recommendations to address the challenges, opportunities, and problems identified in the audit. The audit will also help the network-engineering team proactively identify and resolve potential network troubles before major problems are encountered.
Following is a list of reports that are often generated as part of a network audit:
1. Performance reports
2. Configuration reports
3. Software reports
4. Hardware reports

QUESTION 266:

A good implementation plan that considers the possibility of failure includes which two related principles? (Choose two)

A. A successful pilot or prototype is the only way to eliminate the possibility of failure.
B. A test should be included at every step.
C. A successful test is the only way to eliminate the possibility of failure.
D. A detailed procedure to revert to the original setup is necessary for each and every implementation step.
E. A good implementation plan must eliminate the possibility of failure.
F. A table of failure points, rollback steps, and estimated rollback times is necessary to eliminate the possibility of failure.

Answer: B, D

Explanation:
Implementation of a network design must consider the possibility of a failure, even after
a successful pilot or prototype test. The plan should therefore include a test at every step
and a procedure to revert to the original setup if there is a problem.
Reference: Page 95 in CiscoPress CCDA Self-Study: Designing for Cisco Internetwork
Solutions DESGN 640-861. ISBN : 1587051419, Third printing June 2005

Case Study 1, Certkiller .com

Certkiller .com is an insurance company that has 350 agent offices around Europe.
Each office has a Frame Relay link to the corporate headquarters in Nice. Because
of Certkiller corporate policy, the bandwidth of the agent links is determined by and
paid for by the agents working in their offices. The agents use the network
connection primarily to access various database systems at Nice headquarters and
also for e-mail and Internet access.
Certkiller .com has budgeted 5 million Euro to upgrade the primarily Token-Ring
and FDDI network infrastructure at headquarters to fully redundant Gigabit and
FastEthernet LAN. The upgrade will reduce long-term network costs and improve
the performance, reliability, compatibility, scalability, and manageability of the
LAN infrastructure. Certkiller .com is starting a recruiting effort that it hopes will
result in the addition of 200 new agent offices in the next three years. Certkiller .com
needs higher capacity to meet the potential demand of the new agents. The project
must be completed in three months because of the anticipated demands of a new
E-commerce system, which will increase revenue, and a new customer service
system, which will improve customer satisfaction.
Although the equipment is from a non-Cisco vendor, the current network is an all Cisco solution WAN
infrastructure.
Certkiller wants the LAN to be a complete Cisco solution as well. IT staff is outsourced by the company with
the result that the
Cisco WAN is managed remotely. The onsite IT staff have limited Cisco networking knowledge. Company
policy dictates that
all company data be physically stored in company facilities resulting in the company's website, although
outsourced, is
maintained by personnel and servers located at the head quarters and connected directly to the LAN.
The web developers make use of Macintosh workstations and a mixture of Macintosh and
Sun Solaris servers. The insurance database systems use an IBM mainframe or Oracle on
HPUX servers with custom-developed client software. The e-mail system is based on
Eudora.

Case Study 1: Certkiller .com (4 Questions)

QUESTION 267:

Which two business constraints imposed by Certkiller .com on this new network
design project?

A. equipment vendor selection
B. the existing FDDI infrastructure
C. the three month time line
D. Macintosh and Solaris servers
E. cost reduction due to Ethernet topology

Answer: C, D
According to Cisco press business constraints are
Budget
Personnel
Policies
Schedule

QUESTION 268:

Which two are technical goals of Certkiller .com with regard to this network design project? Select two.

A. increased performance on the WAN links
B. increased WAN scalability
C. increased performance on the LAN
D. network cost reduction
E. increased LAN availability

Answer: C, E
Since it's technical goals the question is asking for, from the statement
"The upgrade will reduce long-term network costs and improve the performance, reliability, compatibility, scalability and manageability on the LAN infrastructure"
Incorrect answers:
Eliminate A and B because it WAN, not LAN
D is a business goal not a technical goal

QUESTION 269:

Which two are business goals of Certkiller .com that apply to this network design project? Select two.

A. project completion in 3 months
B. 200 new agent offices
C. increased revenue from E-commerce system
D. increased manageability of the network
E. increased network scalability

Answer: B, C
Revenue is a business concept.

Which two are technical constraints imposed by Certkiller .com on this network design project? Select two

A. equipment vendor selection
B. three month deadline
C. sufficient bandwidth to support centralized database application
D. the network must transport custom application protocol
E. Gigabit Ethernet upgrade

Answer: C, D

Case Study 2, Certkiller Video

Certkiller Video operates a chain of 45 video rental stores. They currently have a Point-of-Sale (POS) system in which each store posts its daily sales data and inventory changes to a central database through dial-up communication. There is no interaction between the stores and the central system during business hours. The central site runs on an Ethernet LAN. The only always-on WAN link is an Internet connection using wireless broadband to a local ISP.

Certkiller wants to create a new E-Commerce web site where customers can browse and search a catalog of video titles and select the ones they want to rent. The system will instantly communicate the order to the nearest store where employees pull the order and hold it until the customer picks it up. The service must operate on a 24/7 basis. Certkiller sees this new business strategy as a means to increase revenue and expand the business nationally. They see an opportunity to expand the web site in the future to video, DVD and music sales on a worldwide level.

Certkiller wants all stored to be connected to the central site through WAN links. The company is upgrading the central inventory database so that sales and rentals can be posted immediately in real-time. An Internet-based email and instant-messaging system will be set up for all headquarters employees and store managers to use.

Certkiller also wants to upgrade the local LAN to a Gigabit and Fast Ethernet system to facilitate the demands of the new and upgraded systems. They have budgeted $500,000 for the networking equipment and another $10,000/month for the WAN charges including a faster Internet connection. They believe that 256Kbps speeds will be adequate to the stores. Since they have no staff capable of managing the new network, they hire you to complete the project. The project must be complete in 6 months when the new inventory system goes online.

The IT manager has concerns about the security of the servers and workstations on the network when all stores become connected. He does not want any Internet access to or from the stores. He is depending on you to recommend an effective yet affordable solution that will protect his system from intruders.

Case Study 2: Certkiller Video (9 Questions)

QUESTION 271:

What are three technical goals of Certkiller Video with regard to this network design
project? Select three.

A. 24x7 availability of the E-Commerce web site
B. complete the project in 6 months
C. full-time network communication to all stores
D. keep WAN changes below 10,000 USD/month
E. improve the order fulfilment process
F. improve security

Answer: A, C, F

QUESTION 272:

Which two are business goals of Certkiller Video that apply to this network design
project? Select two.

A. Production deployment in 6 months
B. improvement of the order fulfilment process
C. new messaging systems
D. the hiring of skilled IT staff
E. increase revenue through the E-Commerce site

Answer: B, E

Explanation: Since the company now requires all stores to communicate full-time
to the central site, a much better order fulfillment process can be
achieved.
The company is investing in a new network design in order to
generate more revenue by applying a more hierarchical management
approach.
Incorrect Answers
A is a constraint, not a goal.
C is an improvement.
D is a expenditure concern.

QUESTION 273:

Which of the following are business constraints imposed by Certkiller Video on this new network design
project? Choose two.

A. The $10,000/month WAN budget.
B. The installation of WAN links to all stores.

C. The lack of any existing IT staff.
D. The existing Point-of-Sale (POS) system.
E. Real-time posting of store sales.

Answer: A, C

QUESTION 274:

What of the following are technical goals of Certkiller Video with regard to this network design project? (Choose all that apply.)

A. Sell merchandise through an E-Commerce Web site.
B. Real-time posting of sales to a live database.
C. Network security.
D. Upgrade the local LAN for higher performance.
E. Enhance service offerings.

Answer: B, C, D

Explanation:
Technical goals are better network throughput, efficient routing updates and redundancy.
Real-time posting of sales provide instant observation of the status. Security provides
protect system from intruders. High performance LAN provides better response time
Incorrect Answers
A,E: These are business goals.

QUESTION 275:

What of the following are technical goals of Certkiller Video with regard to this network design project? (Select two.)

A. High availability of the E-Commerce web site.
B. Complete the project in 6 months.
C. Keep WAN chargers below $10,000/month.
D. Full-time network communication to all stores.
E. Improve the order fulfilment process.

Answer: A, D

Explanation: To provide 24/7 availability and full-time communications will require
redundancy configurations which are technical in nature.
Incorrect Answers:
B, C: These are non-technical goals.
E: This is an application layer concern.

QUESTION 276:

Which of the following are technical constraints imposed by Certkiller Video on this network design project? (Choose all that apply.)

A. The Point-of-Sale (POS) system.
B. Improved employee communication through instant messaging.
C. The wireless Internet connection.
D. 24/7 availability of the E-Commerce Web site.
E. The central site Ethernet LAN.

Answer: C, D, E

Explanation:
Wireless internet connection is a constraint because of the limited bandwidth it is able to provide.
To provide 24/7 availability and full-time communications will require redundancy configurations which are technical in nature.
The central site is also a technical constraint because it is a hub-spoke topology where a single point of failure (central) will render the whole network dead.
Incorrect Answers:
A is an application layer concern
B is a business/customer service concern

QUESTION 277:

Which of the following are business constraints imposed by the Certkiller Video on this new network design project? (Select two.)

A. The $500,000 equipment budget.
B. The new Internet-based messaging system.
C. Upgrade to Gigabit Ethernet.
D. The existing Point-of-Sale (POS) system.
E. policy against direct Internet access to stores.

Answer: A, E

Explanation: Budget is an apparent business constraint.
E should be considered a business constraint not a technical constraint because the IT manager was worried about Security so the manager decided not to give Internet access which is made to be a policy therefore a business constraint.

Explanation:
B is not a constraint.
C is a technical issues

QUESTION 278:

Which of the following are technical constraints imposed by Certkiller Video on this network design project? (Select two.)

A. Improved employee communication through instant messaging.
B. The Point-of-Sale (POS) system.
C. The central site Ethernet LAN.
D. 24/7 availability of the E-Commerce Web site.

Answer: C, D
The central site is also a technical constraint because it is a hub-spoke topology where a single point of failure (central) will render the whole network dead.
To provide 24/7 availability and full-time communications will require redundancy configurations which are technical in nature.
Incorrect Answers
A is a business/customer service concern
B is an application layer concern

QUESTION 279:

Which of the following are business constraints imposed by Certkiller Video on this new network design project? Choose two.

A. The $10,000/month WAN budget.
B. The installation of WAN links to all stores.
C. The lack of any existing IT staff.
D. Video sales through the global Internet
E. Real-time posting of store sales.

Answer: A, C

Case Study 3, Certkiller Car, Scenario
Certkiller Car operates a chain of 50 rental stores located in Canada. They currently have a Point-of-Sale (POS) system in which each store posts its daily sales data and inventory changes to a central database through dial-up communication. There is no interaction between the stores and the central system during business hours. The central site runs on an Ethernet LAN. The only always-on WAN link is an Internet connection using cable modems to a local ISP.
Certkiller Car wants to enhance its service offering by creating a new E-Commerce web site where customers can select and reserve auto rentals. They would also like to include a credit payment method. The system will instantly communicate the reservation to the appropriate rental store. The service must operate on a 24x7 basis. Certkiller Car sees this new business strategy as a means to increase revenue and expand the business nationally.
Certkiller Car sees an opportunity to expand the web site in the future to

commercial fleet rental.

Certkiller Car wants all stores to be connected to the central site through WAN links. Certkiller Car is upgrading the central inventory database so that rentals can be posted immediately in real-time. An Internet-based email and instant-messaging system will be set up for all headquarters employees and store managers to use. Certkiller Car believes that networking the stores will improve customer satisfaction and thus boost revenue. It will also help communication with store employees. Certkiller Car wants to upgrade the local LAN to a Gigabit and Fast Ethernet system to facilitate the demands of the new and upgraded systems. They have budgeted $500,000 for the networking equipment and another $10,000/month for the WAN charges including a faster Internet connection. They believe the 256kbps speeds will be adequate to the stores. Since the company has no staff capable of managing the new network, it will hire two engineers that already have the training and experience. The project must be completed in 6 months when the new inventory system goes online.

The IT manager has concerns about the security of the servers and workstations on the network when all the stores become connected. Because of these concerns, none of the stores should have direct access to the Internet. Certkiller Car is depending on you to recommend an effective, yet affordable, solution hat will protect their systems from intruders.

Case Study 3, Certkiller Car (4 Questions)

QUESTION 280:

Which two are business constraints imposed by Certkiller car on this new network design project? (Choose two.)

A. $500,000 equipment budget
B. the new Internet-based messaging system
C. upgrade to Gigabit Ethernet
D. the existing POS system
E. policy against direct Internet access to stores

Answer: A, E

QUESTION 281:

What are two technical constraints imposed by Certkiller Car on this network design project? (Choose two.)

A. improved employee communication through instant messaging
B. the POS system
C. the central site Ethernet LAN
D. 24x7 availability

Answer: B, C

QUESTION 282:

Which two business goals of Certkiller Car that apply to this network design project? (Choose two.)

A. production deployment in 6 months
B. improvement of the order fulfillment process
C. new messaging systems
D. the hiring of skilled IT staff
E. increase revenue through the E-Commerce site

Answer: B, E

QUESTION 283:

What are three technical goals of Certkiller Car with regard to this network design project? (Choose three.)

A. 24x7 availability of the E-Commerce web site
B. complete the project in 6 months
C. full-time network communications to all stores
D. keep WAN charges below $10,000/month
E. improve the order fulfillment process
F. improve security

Answer: A, C, F

Case Study 4, Certkiller Support, Scenario

Certkiller Support is a network support company that is considering converging voice and data onto a single network. Certkiller needs assurance that existing networks can take on the additional load.
Data gathering has discovered the following:
- Broadcast traffic and bandwidth-intensive applications take up to 60 percent of the available bandwidth.
- Switches do not support VLANs or QoS.
- Up to three simultaneous calls will be established over 256-kbps Frame Relay links to satellite offices.
- Call volume is expected to double in the next 12 months.
- VoIP telephone power will be provided using PoE.
Case Study 4, Certkiller Support (4 Questions)

QUESTION 284:

Which bandwidth recommendation is most appropriate for the network?

A. The round-trip delay on the LAN should always be less than 20 ms.
B. Round-trip delays of 10 ms or less should be available on the LAN at least 70 percent of the time.
C. The round-trip delay between any two points (LAN and WAN combined) should be less than 400 ms.
D. Gateway support must be available to ensure that VoIP packets use the correct firewall.

Answer: B

Explanation:

QUESTION 285:

Which two actions can help keep your customer's voice network from being affected by anything happening on the data network, including such security threats as a DoS attack? (Choose two.)

A. Use manageable switches.
B. Deploy switches that support PBX/PSTN as well as the VoIP on your LAN.
C. Create a separate VLAN on the network for voice traffic.
D. Implement security performance analyzers.
E. Replace the PBX and bring in an IP PBX or VoIP gateway for the voice traffic.
F. Use a gatekeeper as well as a gateway to separate data and voice traffic to avoid the security issues.

Answer: A, C

QUESTION 286:

Which two strategies need to be executed to avoid security threats to which this VoIP deployment can be vulnerable? (Choose two.)

A. Deploy servers that will act as the gatekeeper or voice gateways.
B. Run only standard software applications, which are less vulnerable to virus attacks or other security threats.
C. Subject your network to routine maintenance, take regular backups, do security checks, and install antivirus software.
D. Implement VoIP performance analyzers.
E. A regular VoIP network is not under security threats that normally occur on a dta network, so no action is needed.
F. VoIP networks are given high priority due to the nature of the traffic. Security is not an action item *missing*

Answer: C, D

QUESTION 287:

Sample Bandwidth per Voice Call			
Link Type (Sample Time)	G.711 (10ms)	G.711 (20ms)	G.729 (20ms)
802.3 Half-Duplex	220.8 kbps	174.4 kbps	78.4 kbps
802.3 Full-Duplex	110.4 kbps	87.3 kbps	39.2 kbps
Frame-Relay	100.8 kbps	82.4 kbps	26.4 kbps
PPP	102.4 kbps	83.2 kbps	27.2 kbps

Which codec should be used for this VoIP installation?

A. 802.3 with half-duplex will allow the maximum amount of 10-ms calls to fit the bandwidth available.
B. G.729 with PPP will allow the most efficient use of the available bandwidth.
C. G.729 at 26.4 kbps will fulfill the present voice and data requirements. Make sure the customer knows that bandwidth capacity will have to be increased to achieve the stretch goal.
D. G.711 with Point to Point Protocol with full-duplex will allow the maximum amount of 10-ms calls to fit the bandwidth available or shorten others.
E. G.711 with Frame Relay will supply their needs and give the company room to grow in the future with minimal costs.

Answer: C

Mixed Questions (44 Questions)

QUESTION 288:

Certkiller .com operates a chain of 50 video rental stores located in northern Italy. They currently have a Point-of-Sale (POS) system in which each store posts its daily sales data and inventory changes to a central database through dial-up communication. There is no interaction between the stores and the central system during business hours. The central site runs on an Ethernet LAN. The only always-on WAN link is an Internet connection using wireless broadband to a local ISP.
Certkiller .com wants to enhance their service offering by creating a new E-commerce web site where customers can browse and search a catalog of video titles and select the ones they want for rental. The system will instantly communicate the order to the nearest store where employees pull the order and hold it until the customer picks it up. The service must operate on a 24x7 basis.
Certkiller .com sees this new business strategy as a means to increase revenue and expand the business nationally. They see ab opportunity to expand the web site in

the future to video, DVD and music sales on a worldwide level.
The company wants all stores to be connected to the central site through WAN
links. The company is upgrading the central inventory database so that sales and
rental can be posted immediately in real-time. An Internet-based email and
instant-messaging system will be set up for all headquarters employees and store
managers to use. Certkiller .com believes that networking the stores will improve
order fulfillment processes which will improve customer satisfaction and thus, boost
revenue. It will also help communication with store employees.
Certkiller .com wants to upgrade the local LAN to a Gigabit and Fast Ethernet
system to facilitate the demands of the new and upgraded systems. They have a
budgeted $500,000 for the networking equipment and another $10,000/month for
the WAN charges including a faster Internet connection. They believe the 256Kbps
speed will be adequate to the stores. Since they have no staff capable of managing
the new network, they will hire two engineers that already have the training and
experience. The project must be completed in 6 months when the new inventory
system goes online.
The IT manager has concerns about the security of the servers and workstations on
the network when all stores become connected. He doesn't want any Internet access
to or from the stores. He is depending on you to recommend an effective yet
affordable solution thet will protect his system from intruders.
What are the business goals of Certkiller .com video that will apply to this network
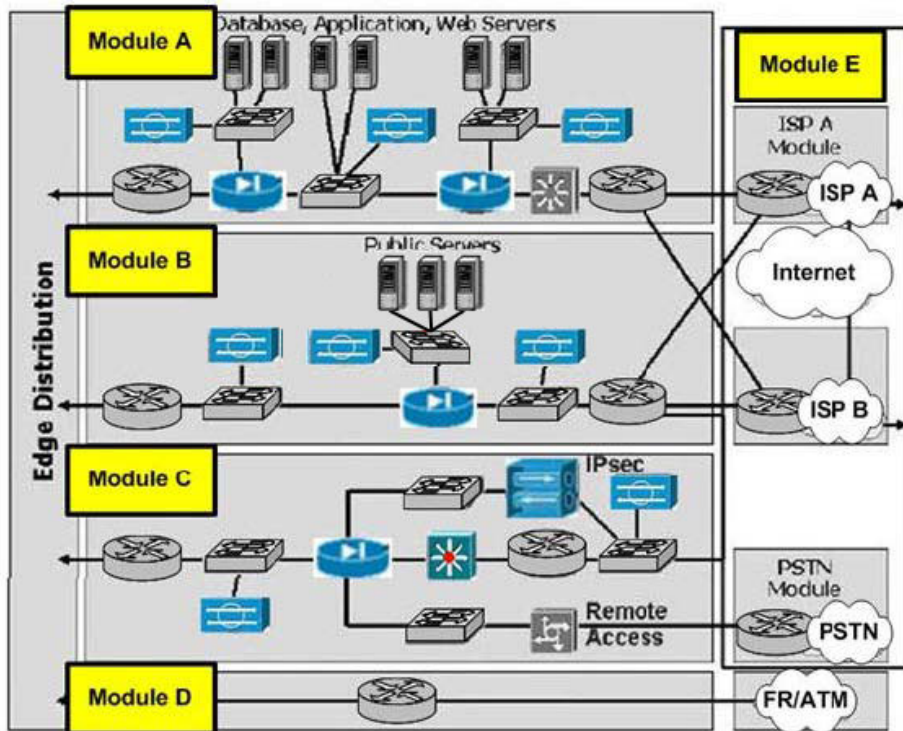design project? Choose two.

A. boost customer satisfaction
B. improve employee communication
C. increase network security
D. upgrading the existing POS system
E. install the network in 6 months

Answer: A, B

QUESTION 289:

Exhibit:

Which module in this figure of the Enterprise Edge functional area deploy
e-commerce and provide connectivity between remote sites and the central site?
(Choose two.)

A. Module A
B. Module B
C. Module C
D. Module D
E. Module E

Answer: A, D

Explanation:
E-Commerce Module
The e-commerce module provides highly available networks for business services. It uses
the highavailability designs of the server-farm module with the Internet connectivity of
the Internet module. Design techniques are the same as those described for these
modules.
VPN/Remote Access Module
The VPN/remote access module provides remote-access termination services, including
authentication for remote users and sites. If you use a remote-access terminal server, this
module connects to the PSTN network. Today's networks often prefer VPNs over
remote-access terminal servers and dedicated WAN links. VPNs reduce communication
expenses by leveraging the infrastructure of SPs. For critical applications, the cost
savings might be offset by a reduction of enterprise control and the loss of deterministic
service. Remote offices, mobile users, and home offices access the Internet using the

local SP with secured IP Security (IPSec) tunnels to the VPN/remote access module via the Internet module.

QUESTION 290:

DRAG DROP
Drag the definition that relates to the Draft Design Document on the left to the term it describes on the right.

The list of procedures that allow the network equipment to function properly		Logical Topology Map
Location of all of the devices in the network		Physical Topology Map
A Network layer representation of all of the modules		Network Device Configuration

Answer:

A Network layer representation of all of the modules

Location of all of the devices in the Network

The list of procedures that allow the network equipment to function properly

Explanation:

A Network layer representation of all of the modules

Location of all of the devices in the network

The list of procedures that allow the network equipment to function properly

---

QUESTION 291:

The Certkiller .com company is concerned that the network management strategy is not as current as it should be. Certkiller .com is specifically interested in improving the ability to provide usage information about network resources and would also like to improve inventory management. Which two functional areas of ISO Network Management will you focus on in your recommendations? (Choose two.)

A. Fault
B. Configuration
C. Accounting
D. Production
E. Security
F. FCAPS

Answer: B, C

QUESTION 292:

DRAG DROP
Drag the routing protocol on the left to the metric it uses on the right.

OSPF		Hop Count
BGP		
EIGRP		Bandwidth, Dealy, reliability, Loading, MTU
RIP		
IS-IS		
RIPv2		Cost
IGRP		
		AS path or manually configured path attributes or both

Answer:
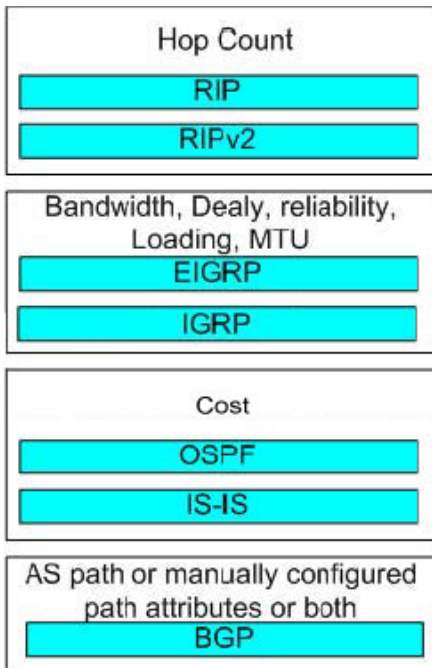
Explanation:

Routing protocols use a metric to determine best routes to a destination. Some routing protocols use a combination of metrics to build a composite metric for best path selection.

1. Hop count
2. Bandwidth
3. Cost
4. Load
5. Delay
6. Reliability
7. Maximum transmission unit (MTU)

1. Hop Count

The hop-count parameter counts the number of links between routers the packet must traverse to reach a destination. The RIP routing protocols use hop count as the metric for route selection. If all links were the same bandwidth, this metric would work well.

2. Bandwidth

The bandwidth parameter uses the interface bandwidth to determine a best path to a destination network. When bandwidth is the metric, the router prefers the path with the highest bandwidth to a destination.

3. Cost

Cost is the name of the metric used by OSPF and IS-IS. In OSPF on a Cisco router, the default cost of a link is derived from the bandwidth of the interface. IS-IS assigns a default cost of 10 for all interfaces. The formula to calculate cost in OSPF is 108/BW where BW is the default or configured bandwidth of the interface.

For Ethernet, cost is calculated as follows:

BW = 10 Mbps = 10 x 106 = 10,000,000 = 107

Cost (Ethernet) = 108 / 107 = 10

The sum of all the costs to reach a destination is the metric for that route. The lowest cost

is the preferred path.

4. Load

The load parameter refers to the degree to which the interface link is busy. The router keeps track of interface utilization; routing protocols can use this metric in the calculation of a best route. Load is one of the five parameters included in the definition of the IGRP and EIGRP metric. By default, it is not used in the calculation of the composite metric. If you have 512 kbps and 256 kbps links to reach a destination, but the 512 Kbps circuit is 99 percent busy and the 256 kbps is only 5 percent busy, the 256 kbps link would be the preferred path. On Cisco routers, the percentage of load is shown as a fraction over 255. Utilization at 100 percent is shown as 255/255 and utilization at 0 percent is shown as 0/255.

5. Delay

The delay parameter refers to the length in time to move a packet to the destination. Delay depends on many factors, such as link bandwidth, utilization, port queues, and physical distance traveled. Total delay is one of the five parameters included in the definition of the IGRP and EIGRP composite metric. By default, it is used in the calculation of the composite metric. You can configure the delay of an interface with the delay tens-of-microseconds command, where tens-of-microseconds specifies the delay in tens of microseconds for an interface or network segment.

6. Reliability

The reliability parameter is the dependability of a network link. Some WAN links tend to go up and down throughout the day. These links get a small reliability rating. Reliability is measured by factors such as the expected received keepalives of a link and the number of packet drops and interface resets. If the ratio is high, the line is reliable. The best rating is 255/255, which is 100 percent reliability. Reliability is one of the five parameters included in the definition of the IGRP and EIGRP metric. By default, it is not used in the calculation of the composite metric.

7. Maximum Transform Unit

The MTU parameter is simply the maximum size of bytes a unit can have on an interface. If the outgoing packet is larger than the MTU, the IP protocol might need to fragment it. If a packet larger that the MTU has the "do not fragment" flag set, the packet is dropped.

QUESTION 293:

DRAG DROP
Drag the prototype system test definitions on the left to the test it defines on the right.

quantifies performance from a user's point of view	availability
calculates the amount of work that an application or applications can do in a given time period	throughput
measures the rate and failures under a medium to heavy load over a 24 to 72 hour time period	regression
Ensures the prototype installation does not break any working applications	application respoonse time

Answer:

measures the rate and failures
under a medium to heavy load over
a 24 to 72 hour time period

calculates the amount of work that
an application or applications can do
in a given time period

quantifies performance from a
user's point of view

Ensures the prototype installation
does not break any working
applications

QUESTION 294:

Which two guidelines are indicative that network utilization has reached an
unhealthy saturation level? (Choose two.)

A. shared Ethernet segments with more than 40 percent
B. WAN links with more than 50 percent
C. shared Token Ring segments with more than 40 percent
D. WAN links with more than 70 percent
E. shared Ethernet segments with more than 50 percent
F. shared Token Ring segments with more than 50 percent

Answer: A, D

Explanation:
When highest percent of available bandwidth utilizing, there is a chances of dropping
packets. We can identify congestion is occurred or not in interface. Shared Ethernet

segments with more than 40 percent is called reached in unhealthy saturation and 70 percent of WAN link is called reached in unhealthy saturation.

QUESTION 295:

Which two routing protocols should be used given these requirements? (Choose two.)
Within the Enterprise network:
1. All routers are Cisco 3600 Series routers running the latest Cisco IOS release.
2. The fastest convergence time possible is required.
3. Unequal cost load-balancing is required.
For Internet connections:
1. A single link is used to connect to a single ISP.

A. Use OSPF as the IGP within the Enterprise.
B. Use EIGRP as the IGP within the Enterprise.
C. Use Internal BGP as the IGP within the Enterprise.
D. Use External BGP between the Enterprise and the ISP.
E. Use EIGRP between the Enterprise and the ISP.
F. Use Static/Default routing between the Enterprise and the ISP.

Answer: B, F

Explanation:
IGP
Interior Gateway Protocol: Any protocol used by the Internet to exchange routing data within an independent system
EIGRP (Enhanced IGRP)
Enhanced IGRP (EIGRP) was created to resolve some of the problems with IGRP. One problem is that the entire route table is sent when changes are made in the network; another problem is the lack of formal neighbor relationships with connected routers. EIGRP is a hybrid of both link-state and distance-vector routing algorithms, which brings the best of both worlds together.
EIGRP allows for equal-cost load balancing, incremental routing updates, and formal neighbor relationships, overcoming the limitations of IGRP. This enhanced version uses the same distance-vector information as IGRP, yet with a different algorithm. EIGRP uses DUAL (diffusing update algorithm) for metric calculation. EIGRP is used within the Enterprise Network.
Static Route
Static routes are manually configured on a router. They do not react to network outages. The one exception is when the static route specifies the outbound interface: If the interface goes down, the static route is removed from the routing table. Because static routes are unidirectional, they must be configured for each outgoing interface the router will use. The size of today's networks makes it impossible to manually configure and maintain all the routes in all the routers in a timely manner.
The main benefit of static routing is that a router generates no routing protocol overhead.

Because no routing protocol is enabled, no bandwidth is consumed by route advertisements between network devices. Static routing is recommended for hub-and-spoke topologies with a low-speed remote connection. A default static route is configured at each remote site because the hub is the only route used to reach all other sites.

QUESTION 296:

Certkiller is an online fitness organization that specializes in creating fitness plans for senior citizens. They recently added a health-products retail inventory to the offerings. Which E-Commerce module device will be used for customers to interface with the company so that they can by the products that they need?

A. NIDS appliances
B. SMTP mail servers
C. Database servers
D. Application servers
E. Web servers
F. Public servers

Answer: E

Explanation:
The e-commerce module provides highly available networks for business services. It uses the highavailability designs of the server-farm module with the Internet connectivity of the Internet module. Design techniques are the same as those described for these modules. Web Server provides the web services.

QUESTION 297:

DRAG DROP
Drag the component on the top to the Enterprise Edge functional area it belongs to at the bottom.

SMTP mail servers

Dial-in access concentrators

DNS servers

IPSec tunnel termination

Web servers

Firewall using IPSec tunnels

Application servers

Edge routers for basic filtering and Layer 3 connectivity

Layer 3 switch with IDS modules for traffic transport

E-Commerce module

Internet Connectivity module

VPN/Remote Access module

Answer:

E-Commerce module

Web servers

Application servers

Layer 3 switch with IDS modules for traffic transport

Internet Connectivity module

SMTP mail servers

DNS servers

Edge routers for basic filtering and Layer 3 connectivity

VPN/Remote Access module

Dial-in access concentrators

IPSec tunnel termination

Firewall using IPSec tunnels

QUESTION 298:

Multicast Traffic

Internet

The graphic represents a common multicast situation. The switch is a Layer 2
switch. Which three considerations are important in designing a solution? (Choose
three.)

A. The problem is that the default behavior for the router forwards the multicast traffic
through every interface.
B. The problem that needs to be overcome is the flooding on the Layer 2 switch.
C. A solution may be deployed to allow the switch to find out from the router which
users are part of the multicast group.
D. The key is to deploy a solution that suppresses incoming traffic by bandwidth rather
than by packets per second.
E. A solution may be deployed to allow the examination of the IGMP data to determine
which switch ports need to participate in a multicast group.
F. Static entries that specify which ports should receive broadcast traffic must be
eliminated and replaced by GVRP.

Answer: B, C, E

Explanation:

Layer 2 Multicasting
The concept of forming a multicast group is the basis for IP multicast. This means that any group or collection of receivers can indicate interest in receiving a particular stream of data. The group itself isn't limited by physical or departmental boundaries, and the hosts can be located anywhere on the network as well. Hosts join the group by using the Internet Group Management Protocol (IGMP) in order to receive data going to that group.
Multicast routing protocols such as Protocol Independent Multicast (PIM) guide the delivery of traffic through multicast-enabled routers. The router to the switch port forwards the incoming multicast stream.
One problem is that the default for an L2 switch is to forward all multicast traffic to every port that belongs to the same VLAN on the switch. Talk about a monkey wrench in the works. This activity defeats the very purpose of the switch, which is to send traffic only to the ports that need to receive the data. Bummer!
The good news is that there are several ways Cisco switches can circumvent this little problem. Ones commonly used include:
Cisco Group Management Protocol (CGMP) A Cisco proprietary solution found on all Cisco LAN switches. The multicast receiver registration (using the IGMP) is accepted by the router and communicated by CGMP to the switch; the switch updates its forwarding table with that information.
IGMP snoopingThe switch intercepts multicast receiver registrations and updates the forwarding table with that information. The IGMP snooping means that the switch is aware of L3 because IGMP is a Network layer protocol. Typically, the IGPM packet recognition is hardware assisted.

QUESTION 299:

DRAG DROP
Drag the definition on the left to the IP telephony architectural component it describes on the right.

Layer 2 and Layer 3 switches and voice-enabled routers interconnect with the IP and PSTN networks, using 10/100 Ethernet ports.	call processing
Software provides a scalable, distributable and highly available enterprise IP telephony solution.	infrastructure
Cisco and third party companies develop software that interoperates with Cisco call control and processing solutions	client devices
IP telephones and software applications allow communications across the IP network.	applications

Answer:

> Software provides a scalable, distributable and highly available enterprise IP telephony solution.

> Layer 2 and Layer 3 switches and voice-enabled routers interconnect with the IP and PSTN networks, using 10/100 Ethernet ports.

> IP telephones and software applications allow communications across the IP network.

> Cisco and third party companies develop software that interoperates with Cisco call control and processing solutions

QUESTION 300:

Analysis and recommendations in a Draft Design Document are based on which two features? (Choose two.)

A. logical topology map
B. collected information
C. physical topology map
D. hardware platform
E. design requirements
F. software versions

Answer: B, E

Explanation:
Analysis and recommendations in Draft Design Document are based on collected information and requirements to design.

QUESTION 301:

For which scenario would static IP addressing be most appropriate?

A. when a given number of IP addresses are expected to change
B. when a variable number of IP addresses are required per subnet
C. when a given number of IP addresses need to be reserved for distribution to dial-in clients
D. when it is desirable to administratively track a given number of IP addresses

Answer: D

Explanation:

IP Address assign into host in two ways, one is static and another automatically from DHCP server. In static you need to enter manually every information into host but automatically from DHCP will assign from DHCP server.

QUESTION 302:

Which three principles should be included in a good implementation plan? (Choose three.)

A. A less-knowledgeable network engineer should be able to implement the design.
B. A good implementation design is composed of multiple small, complex implementation steps.
C. A good implementation plan will not have many problematic incremental implementation steps.
D. When planning for implementation, try to reduce the number of steps in order to avoid complexity.
E. A good implementation plan avoids being too complex.
F. Good implementation plans must consider the possibility of failure.

Answer: A, E, F

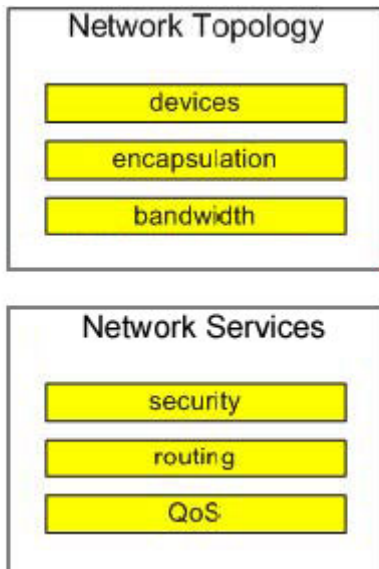## QUESTION 303:

DRAG DROP
Two important aspects of information about an existing network are network topology and network services. Drag the item on the left to the infrastructure category that it belongs to on the right.

devices

encapsulation

security

bandwidth

routing

QoS

Network Topology

Network Services

Answer:

Network Topology

- devices
- encapsulation
- bandwidth

Network Services

- security
- routing
- QoS

QUESTION 304:

DRAG DROP
When evaluating a current voice network you may run into several different legacy technologies. Drag the technology description on the left to the correct technology name on the right.

Description	Technology
Permits modern consumer telephone services in PSTN	Centrax
Measures probability of attemted calls being blocked	ACD
The CO that acts as a voice switch, appearing as a PBX	SS7
Provides recorded announcements and key prompts	IVR
Distribution system that routes calls to agents	GoS

Answer:

The CO that acts as a voice switch, appearing as a PBX

Distribution system that routes calls to agents

Permits modern consumer telephone services in PSTN

Provides recorded announcements and key prompts

Measures probability of attemted calls being blocked

QUESTION 305:

Which three pieces of information should be documented in each phase of a design implementation plan? (Choose three.)

A. simple implementation guidelines
B. step description
C. design document references
D. easy guidelines in case of failure
E. estimated rollback time in case of failure
F. estimated implementation time

Answer: B, C, F

Explanation:
Network Documentation
After completing a design, the next step is to document it so that you can properly communicate your solution. The documentation can be in the form of a response to a Request for Proposal (RFP) or a design document, also referred to as a proposal. The following are the minimum recommended sections of the design document, all of which are described in detail in the sections that follow:
1. Executive summary
2. Design requirements
3. Design solution
4. Summary and appendixes
Executive Summary
The first section is an executive summary, which is typically one page in length. The executive summary
describes the network requirements and how the proposed design meets those requirements.
The audience for the executive summary is the decision makers for the project. The

following is a list of suggested topics:
1. State the goals of the project and how it relates to the business needs.
2. Describe how your solution addresses these business needs. Outline the network-design
strategy.
1. Describe the implementation concerns such as integration issues, training, support, and transition issues.
1. Outline the benefits of the solution.
It is important that you write the executive summary clearly and concisely. Remember that the audience needs to understand the project based on this one- or two-page description.
Design Requirements
This section describes the results of investigating the organization's business and technical needs. Some of the methods for understanding the design requirements can include characterizing the existing network and the logical network requirements, such as performance, scalability, capacity, security, and traffic needs. It is helpful in this section to organize the design requirements to be easily understandable. Remember to refer back to the business needs as appropriate.
Design Solution
Present the recommended solution in this section based on the priority of the organization. This section should include a network diagram of the proposed solution. The network diagram should contain addressing and naming conventions. Also included are listings of the hardware and software recommendations for the LAN and WAN and the recommended protocols for routing and application. Finally, with any implementation, you should write a section addressing how the network will be managed after it is installed.

QUESTION 306:

Which three actions are made possible by the summary report recommendations?
(Choose three.)

A. classification of new network features
B. Design Document conclusions
C. network health description
D. proposed upgrades to hardware and software
E. required feature support
F. customer requirement modification

Answer: D, E, F

Explanation:
Reports are the lifeblood of any well-maintained network management scheme. Using data gathered from the network management solution, network managers can compose reports that provide as detailed a summary as needed of network performance. These reports should be weighed against the stated performance goals, and the collection of

information used in network reports should certainly reflect the metrics that define the design goals. In other words, knowing what tolook for can eliminate sifting through mounds of unneeded data.

QUESTION 307:

	Routing Protocol				
	A	B	C	D	E
Convergence Time	slow	fast	slow	fast	fast
VLSM	no	yes	no	yes	yes
Bandwidth Consumption	high	low	high	low	medium
Multi-path Support	no usually	yes	yes	yes	yes
Scales Well	no	yes	yes	yes	yes
Proprietary	no	no	yes	yes	no
Routes Non-IP protocols	no	no	no	yes	yes

Each column in the table represents characteristics of a routing protocol. Choose one protocol that matches column B and one protocol that matches column E. (Choose two.)

A. OSPF
B. BGP
C. EIGRP
D. IS-IS
E. RIPv2

Answer: A, D

Explanation:
OSPF
RFC 2328 defines OSPF, a link-state routing protocol that uses Dijkstra's shortest-path first (SPF) algorithm to calculate paths to destinations. In OSPF, each router sends link-state advertisements about itself and its links to all other routers in the area. Note that it does not send routing tables but link-state information about its interfaces. Then, each router individually calculates the best routes to the destination by running the SPF algorithm. Each OSPF router in an area maintains an identical database describing the area's topology. The routing table at each router is individually constructed using the local copy of this database to construct a hortest-path tree. OSPF is a classless routing protocol that permits the use of VLSMs and classless interdomain
routing (CIDR). With Cisco routers, OSPF also supports equal-cost multipath load balancing and neighbor authentication. OSPF uses multicast addresses to communicate between routers. OSPF uses IP protocol 89.
IS-IS
IS-IS is an International Organization for Standardization (ISO) dynamic routing

specification. IS-IS is described in ISO/IEC 10589, reprinted by the Internet Engineering Task Force (IETF) as RFC 1142. IS-IS is a link-state routing protocol that floods link-state information throughout the network to build a picture of network topology. IS-IS was primarily intended for routing OSI Connectionless Network Protocol (CNLP) packets but has the capability to route IP packets. IP packet routing uses Integrated IS-IS, which provides the ability to route protocols such as IP. IS-IS is a common alternative to other powerful routing protocols such as OSPF and EIGRP in large networks. Although not seen much in enterprise networks, IS-IS is commonly used for internal routing in large ISP networks.

IS-IS creates two levels of hierarchy with Level 1 for intra-area and Level 2 for interarea routing. IS-IS distinguishes between Level 1 and Level 2 intermediate systems (ISs). Level 1 ISs communicate with other Level 1 ISs in the same area. Level 2 ISs route between Level 1 areas and form an intradomain routing backbone. Hierarchical routing simplifies backbone design because Level 1 ISs only need to know how to get to the nearest Level 2 IS.

QUESTION 308:

Network enhancements my be possible when buffer misses per hour exceed which concentration?

A. 10
B. 25
C. 40
D. 50
E. 75
F. 100

Answer: B

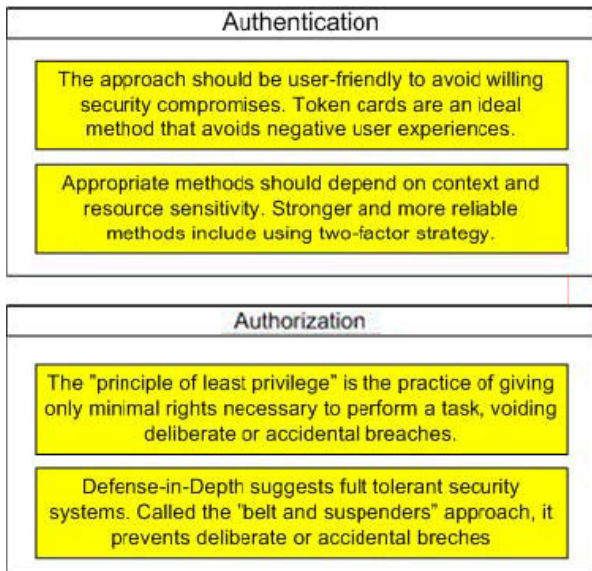## QUESTION 309:

DRAG DROP
Drag the security guideline to the left to the correct network access control mechanism. Not all guidelines apply.

	Authentication
The "principle of least privilege" is the practice of giving only minimal rights necessary to perform a task, voiding deliberate or accidental breaches.	
The client should push security settings to the server to provide filtering that prevents connection to the client and confines attackers via a firewall break-in.	
The approach should be user-friendly to avoid willing security compromises. Token cards are an ideal method that avoids negative user experiences.	Authorization
Appropriate methods should depend on context and resource sensitivity. Stronger and more reliable methods include using two-factor strategy.	
Defense-in-Depth suggests fult tolerant security systems. Called the "belt and suspenders" approach, it prevents deliberate or accidental breches	

Answer:

Authentication
The approach should be user-friendly to avoid willing security compromises. Token cards are an ideal method that avoids negative user experiences.
Appropriate methods should depend on context and resource sensitivity. Stronger and more reliable methods include using two-factor strategy.

Authorization
The "principle of least privilege" is the practice of giving only minimal rights necessary to perform a task, voiding deliberate or accidental breaches.
Defense-in-Depth suggests fult tolerant security systems. Called the 'belt and suspenders" approach, it prevents deliberate or accidental breches

QUESTION 310:

Which two results of segment analysis are approximate thresholds that indicate network enhancement is desired? (Choose two.)

A. 25 percent broadcasts/multicasts
B. 30 percent broadcasts/multicasts
C. 1 CRC error per one million bytes
D. 1 CRC error per 100,000 bytes
E. 20 percent broadcasts/multicasts
F. 1 CRC error per 1000 bytes

Answer: C, E

QUESTION 311:

When you have completed a study of Ethernet segments, what is the guideline ceiling for packet collision, stated as a percentage?

A. 0.001
B. 0.01
C. 0.1
D. 0.15
E. 0.25
F. 1

Answer: C

Explanation:

The most significant design rule for Ethernet is that the round-trip propagation delay in one collision domain must not exceed 512 bit times, which is a requirement for collision detection to work correctly. This rule means that the maximum round-trip delay for a 10-Mbps Ethernet network is 51.2 microseconds. The maximum round-trip delay for a 100-Mbps Ethernet network is only 5.12 microseconds because the bit time on a 100-Mbps Ethernet network is 0.01 microseconds as opposed to 0.1 microseconds on a 10-Mbps Ethernet network.

QUESTION 312:

Which three routing protocols usually converge most quickly? (Choose three.)

A. RIPv2
B. IS-IS
C. BGP
D. EIGRP
E. OSPF
F. IGRP

Answer: B, D, E

Explanation:
EIGRP
Cisco Systems released EIGRP in the early 1990s as an evolution of IGRP toward a more scalable routing protocol for large internetworks. EIGRP is a classless protocol that permits the use of VLSMs and that supports CIDR for the scalable allocation of IP addresses. EIGRP does not send routing updates periodically, as does IGRP. EIGRP allows for authentication with simple passwords or with MD5. EIGRP autosummarizes networks at network borders and can load-balance over unequal-cost paths. Packets using EIGRP use IP protocol 88. Only Cisco routers can use EIGRP.
EIGRP is an advanced distance-vector protocol that implements some characteristics similar to those of link-state protocols. Some Cisco documentation refers to EIGRP as a hybrid protocol.
EIGRP advertises its routing table to its neighbors as distance-vector protocols do, but it uses hellos and forms neighbor relationships as link-state protocols do. EIGRP sends partial updates when a metric or the topology changes on the network. It does not send full routing-table updates in periodic fashion as do distance-vector protocols. EIGRP uses DUAL to determine loop-free paths to destinations. This section discusses DUAL.
EIGRP Components
EIGRP has four components that characterize it:
1. Protocol-dependent modules
2. Neighbor discovery and recovery
3. Reliable Transport Protocol (RTP)
4. DUAL
OSPF
RFC 2328 defines OSPF, a link-state routing protocol that uses Dijkstra's shortest-path

first (SPF) algorithm to calculate paths to destinations. In OSPF, each router sends link-state advertisements about itself and its links to all other routers in the area. Note that it does not send routing tables but link-state information about its interfaces. Then, each router individually calculates the best routes to the destination by running the SPF algorithm. Each OSPF router in an area maintains an identical database describing the area's topology. The routing table at each router is individually constructed using the local copy of this database to construct a hortest-path tree. OSPF is a classless routing protocol that permits the use of VLSMs and classless interdomain routing (CIDR). With Cisco routers, OSPF also supports equal-cost multipath load balancing and neighbor authentication. OSPF uses multicast addresses to communicate between routers. OSPF uses IP protocol 89.

IS-IS

IS-IS is an International Organization for Standardization (ISO) dynamic routing specification. IS-IS is described in ISO/IEC 10589, reprinted by the Internet Engineering Task Force (IETF) as RFC 1142. IS-IS is a link-state routing protocol that floods link-state information throughout the network to build a picture of network topology. IS-IS was primarily intended for routing OSI Connectionless Network Protocol (CNLP) packets but has the capability to route IP packets. IP packet routing uses Integrated IS-IS, which provides the ability to route protocols such as IP. IS-IS is a common alternative to other powerful routing protocols such as OSPF and EIGRP in large networks. Although not seen much in enterprise networks, IS-IS is commonly used for internal routing in large ISP networks.

IS-IS creates two levels of hierarchy with Level 1 for intra-area and Level 2 for interarea routing. IS-IS distinguishes between Level 1 and Level 2 intermediate systems (ISs). Level 1 ISs communicate with other Level 1 ISs in the same area. Level 2 ISs route between Level 1 areas and form an intradomain routing backbone. Hierarchical routing simplifies backbone design because Level 1 ISs only need to know how to get to the nearest Level 2 IS.

QUESTION 313:

A network summary report is a valuable tool in gathering information. Which information should it identify?

A. new network features
B. infrastructure shortcomings
C. actions needed to support the existing network features
D. actions needed to support the existing network
E. customer requirements
F. customer requirement modifications

Answer: B

Explanation:
After completing a design, the next step is to document it so that you can properly communicate your solution. The documentation can be in the form of a response to a

Request for Proposal (RFP) or a design document, also referred to as a proposal. The following are the minimum recommended sections of the design document, all of which are described in detail in the sections that follow:
1. Executive summary
2. Design requirements
3. Design solution
4. Summary and appendixes
Executive Summary
The first section is an executive summary, which is typically one page in length. The executive summary
describes the network requirements and how the proposed design meets those requirements. The audience for the executive summary is the decision makers for the project. The following is a list of suggested topics:
1. State the goals of the project and how it relates to the business needs.
2. Describe how your solution addresses these business needs. Outline the network-design strategy.
3. Describe the implementation concerns such as integration issues, training, support, and transition issues.
4. Outline the benefits of the solution.

QUESTION 314:

	Routing Protocol				
	A	B	C	D	E
Convergence Time	slow	fast	slow	fast	fast
VLSM	no	yes	no	yes	yes
Bandwidth Consumption	high	low	high	low	medium
Multi-path Support	no usually	yes	yes	yes	yes
Scales Well	no	yes	yes	yes	yes
Proprietary	no	no	yes	yes	no
Routes Non-IP protocols	no	no	no	yes	yes

Each column in the table represents characteristics of a routing protocol. Choose one protocol that matches column A and one protocol that matches column D. (Choose two.)

A. OSPF
B. RIP
C. ODR
D. EIGRP
E. IS-IS
F. BGP

Answer: B, D

Explanation:
RIP
RFC 1058 from June 1988 defines RIPv1. RIP is a distance-vector routing protocol that uses router hop count as the metric. RIP is a classful routing protocol that does not support VLSMs or CIDR. There is no method for authenticating route updates. A RIP router sends a copy of its routing table to its neighbors every 30 seconds. RIP uses split horizon with poison reverse; therefore, route updates are sent out an interface with an infinite metric for routes learned (received) from the same interface.
The RIP standard was based on the popular routed program used in UNIX systems since the 1980s. The Cisco implementation of RIP adds support for load balancing. RIP will load-balance traffic if there are several paths with the same metric (equal-cost load balancing) to a destination. Also, RIP sends triggered updates when the metric of a route changes. Triggered updates can help the network converge faster rather than wait for the periodic update. RIP has an administrative distance of 120. Chapter 11, "Routing Protocol Selection Criteria," covers administrative distance. RIP summarizes to IP network values at network boundaries. A network boundary occurs at a router that has one or more interfaces that do not participate in the specified IP network. The IP address assigned to the interface determines participation. IP class determines the network value. For example, an IP network that uses 24-bit subnetworks from 180.100.50.0/24 to 180.100.120.0/24 is summarized to 180.100.0.0/16 at a network boundary.
EIGRP
Cisco Systems released EIGRP in the early 1990s as an evolution of IGRP toward a more scalable routing protocol for large internetworks. EIGRP is a classless protocol that permits the use of VLSMs and that supports CIDR for the scalable allocation of IP addresses. EIGRP does not send routing updates periodically, as does IGRP. EIGRP allows for authentication with simple passwords or with MD5. EIGRP autosummarizes networks at network borders and can load-balance over unequal-cost paths. Packets using EIGRP use IP protocol 88. Only Cisco routers can use EIGRP.
EIGRP is an advanced distance-vector protocol that implements some characteristics similar to those of link-state protocols. Some Cisco documentation refers to EIGRP as a hybrid protocol.
EIGRP advertises its routing table to its neighbors as distance-vector protocols do, but it uses hellos and forms neighbor relationships as link-state protocols do. EIGRP sends partial updates when a metric or the topology changes on the network. It does not send full routing-table updates in periodic fashion as do distance-vector protocols. EIGRP uses DUAL to determine loop-free paths to destinations. This section discusses DUAL.
EIGRP Components
EIGRP has four components that characterize it:
1. Protocol-dependent modules
2. Neighbor discovery and recovery
3. Reliable Transport Protocol (RTP)
4. DUAL

QUESTION 315:

When you have completed a study of Ethernet segments, what is the guideline ceiling for packet collision, stated as a percentage?

A. 0.001
B. 0.01
C. 0.1
D. 0.15
E. 0.25
F. 1

Answer: C

Explanation:
The most significant design rule for Ethernet is that the round-trip propagation delay in one collision domain must not exceed 512 bit times, which is a requirement for collision detection to work correctly. This rule means that the maximum round-trip delay for a 10-Mbps Ethernet network is 51.2 microseconds. The maximum round-trip delay for a 100-Mbps Ethernet network is only 5.12 microseconds because the bit time on a 100-Mbps Ethernet network is 0.01 microseconds as opposed to 0.1 microseconds on a 10-Mbps Ethernet network.

QUESTION 316:

What is the benefit of VLSM?

A. reduces configuration complexity by using the same subnet mask length
B. reduces the routing table size by using automatic summarization
C. allows the advertisement of the subnet mask along with the classful routing updates
D. conserves IP addresses by using different subnet mask length
E. secures the hosts on a subnet by using RFC 1918 addresses
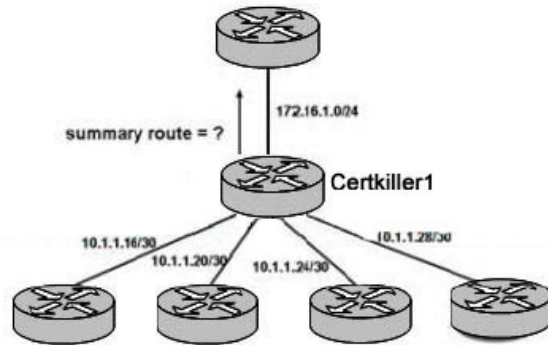
Answer: D

Explanation:
VLSMs divide a network into subnets of various sizes to prevent wasting IP addresses. If a Class C network uses 255.255.255.240 as a subnet mask, there will be 16 subnets, each with 14 IP addresses. If there is a point-to-point link that needs only two IP addresses, 12 IP addresses are wasted. This problem scales further with Class B and Class A address space. With VLSMs, small LANs can use /28 subnets with 14 hosts, and larger LANs can use /23 or /22 masks with 510 and 1022 hosts. Point to point networks use a /30 mask, which supports two hosts.

QUESTION 317:

Exhibit:

Refer to the exhibit. What should Certkiller 1 announce as the summarized address towards its upstream router?

A. 10.1.0.0/24
B. 10.1.1.16/24
C. 10.1.1.16/26
D. 10.1.1.16/28
E. 10.1.1.16/30
F. 10.1.1.16/32

Answer: D

Explanation:
On very large networks, there may be hundreds or even thousands of individual networks and subnetworks being advertised. All these routes can be very taxing on a router's memory and processor. For example, routers on the Internet were starting to be overwhelmed with a couple of hundred thousand routes. After summarizing routes and using CIDR, the number of routes has been dramatically reduced.

Summary Example	
IP Network Address	**Binary Equivalent**
172.16.100.0	**10101100.0001000.01100**100.0
172.16.101.0	**10101100.0001000.01100**101.0
172.16.102.0	**10101100.0001000.01100**110.0
172.16.103.0	**10101100.0001000.01100**111.0
172.16.104.0	**10101100.0001000.0110**1000.0
172.16.105.0	**10101100.0001000.0110**1001.0
172.16.106.0	**10101100.0001000.0110**1010.0

Examine the table to determine the maximum number of bits (starting from the left) that all of the addresses have in common. (Where they are lined up, we boldfaced them to make them easier for you to see.) The number of common bits is the prefix length for the

summarized address (/20).
In this example, we can see from the table that all of the addresses have the first 20 bits in common. The decimal equivalent of these first 20 bits is 172.16.96.0. So, we can write our new summarized address as 172.16.96.0/20. If we were to later add a network 172.16.98.0, it would need to be behind the router summarizing this address space. If we didn't, it could cause problems.

QUESTION 318:

Which three security measures can be used to DoS attacks that are directed at exposed hosts within the E-Commerce module? (Choose three.)

A. Place the exposed hosts on isolated LANs.
B. Use Firewalls to block all unnecessary connections to the exposed hosts.
C. Use LAN switch access-control mechanisms, such as VTP pruning, to separate hosts on the same segment.
D. Use NIDSs and HIDSs to monitor individual hosts and subnets to detect signs of attack and to identify potentially successful breaches.
E. Use VPN concentrator (IPSec) to protect and verify each connection to the exposed host or hosts.

Answer: A, B, D

Explanation:
DoS
DoS attacks deny legitimate users access to services. DoS attacks are characterized by disrupting connectivity between devices, preventing access to specific services, halting processes on devices by sending bad packets, and flooding networks.
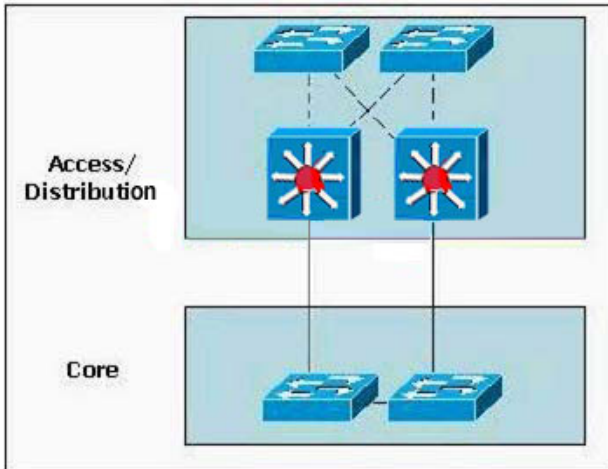Some ways to prevent DoS attacks follow:
1. Properly configure firewalls and routers to prevent DoS attacks. You can find these
2. configurations on vendor and security websites.
3. Prevent spoofing.
4. Prevent traffic rates from getting out of control.

QUESTION 319:

Exhibit:

Refer to the exhibit. Which Campus Backbone Design does this most likely represent?

A. Single VLAN Layer 2
B. Split VLAN Layer 2
C. Layer 3 VLAN
D. Dual Path Layer 3 VLAN

Answer: A

Explanation:
A virtual LAN (VLAN) is a broadcast domain created by one or more switches. The switch creates a VLAN simply by putting some interfaces in one VLAN and some in another. So, instead of all ports on a switch forming a single broadcast domain, the switch separates them into many, based on configuration.

QUESTION 320:

Western Associated News Agency recently acquired a large news organization with several sites, which will allow it to expand to worldwide markets. The new acquisition brings with it a multitude of connectivity technologies, including Frame Relay, ATM, SONET, cable, DSL, and wireless. Which Enterprise Edge module will receive the most attention from a Layer 1 viewpoint?

A. ISP
B. PSTN
C. Internet Connectivity
D. WAN
E. E-Commerce
F. Edge Distribution

Answer: D

Explanation:
As the name implies, WANs encompass broad geographical areas. Unlike with LANs, private organizations that need the WAN services do not typically own the WAN. In most cases, the costs involved are too high, and sharing WAN resources across multiple organizations lessens the need to support multiple parallel private infrastructures, which reduces right-of-way issues and conflicts. Network providers most often supply connections through their systems and can even provide portions of the hardware required. These network providers charge fees, or tariffs, for use of the WAN. Often set by governmental regulation, these fees can be a fixed periodic amount independent of distance, duration of activity, or metered data volumes, as is typical of small office/home office (SOHO) Internet connectivity. These fees are also typically based on permanent or virtual circuits and some defined relationship for guaranteed access bandwidth, as is common for packet-switched networks. Circuit-switched environments often use time of active connection. Leased-line environments frequently use an amount that considers access bandwidth and distance. As you will learn, it is important to consider all the aspects of these tariffs as you design appropriate WAN solutions.

QUESTION 321:

FloCzar Boats is a marine transportation company that has undergone a period of rapid growth in the past year. The company has some issues with the Network Management design, and would like to enhance the information that is available about the devices. It seems that only static information can be obtained, and FloCzar would like to be able to get information that will help to perform long-term trend analysis. The company is specifically concerned with Layer 4. Which management protocol will best meet the goals?

A. RMON
B. SNMP
C. NetFlow
D. CDP
E. RMON2

Answer: E

Explanation:
Remote Monitoring (RMON)Like SNMP, RMON (Remote Monitoring) was developed by the IETF. Originally proposed in 1992, RMON was officially adopted as a draft standard in 1995, as RFC 1757. At its core, RMON is an SNMP MIB, which defines a set of objects available to an RMON probe.
RMON works on a manager/agent basis, but while SNMP retrieves information about a specific network device's status, RMON polls probes for information about network segments. One of the biggest advantages of RMON probes is what is referred to as offline operation, whereby a probe can continuously monitor a network segment in lieu of the RMON console device. This is especially beneficial when the segment is not in continual contact with the console device, such as when a link on the network has failed.

This also can substantially reduce overhead CPU usage for the NMS itself, because the probe can handle the segment-specific monitoring duties.

GroupsRMON defines a number of statistics (referred to as groups), each of which delivers specific sets of data. Each group is optional, and vendors can support as many or as few of the groups as they like. Currently, there are two versions of RMON defined by the IETF: RMON1 and RMON2. RMON1 includes 10 groups, and RMON2 adds 9 more. RMON2 does not replace RMON1; instead, it adds onto it. RMON1 is limited to data-link visibility, that is, it only sees Layers 1 and 2 of the OSI model. RMON2 gives visibility into upper layer protocols for better visibility in application and protocol-monitoring situations.

Let's take a look at the RMON1 and RMON2 groups.

A. RMON1RMON1 contains the following groups:

StatisticsThe Statistics group contains statistics measured by the probe for each monitored interface on the network, for example, broadcast packets, multicast packets, CRC errors, etc.

HistoryThe History group records periodic statistical samples and stores them for later analysis.

AlarmThe Alarm group periodically collects statistical samples from variables in the probe and compares them with previously configured thresholds. If these variables cross a threshold, an event is generated. (See also the description of the Events group.)

HostThe Host group collects information about each host on the network, for example, host MAC address, packets received and transmitted, etc.

HostTopNThe HostTopN group is used to prepare reports that describe the hosts that top a list ordered by one of their statistics.

MatrixThe Matrix group stores statistics for conversations between sets of two addresses. As the probe detects new conversations, new table entries are created.

Filters The Filters group allows packets to be matched by a filter equation. These matched packets from a data stream may be captured for later analysis, or they may generate events. Associated with each filter is a channel, a specific path along which data flows.

Packet CaptureThe Packet Capture group allows packets to be captured after they flow through a channel.

EventsThe Events group controls the generation and notification of events from the probe. An event can generate an SNMP trap, or generate a log entry, or both.

Token RingThe Token Ring group contains Token Ring extensions, including ring station, ring station order, and source routing information.

B. RMON2RMON2 contains the following groups:

Protocol DirectoryThe Protocol Directory group provides a list of protocols supported by the RMON device.

Protocol DistributionThe Protocol Distribution group contains the traffic statistics for each Layer 3 and above supported protocol.

Address MappingThis group contains the mappings of Network layer addresses to Layer 2 or MAC addresses.

Network Layer HostThe Network Layer Host group contains information on Network layer traffic to and from individual hosts.

Network Layer MatrixThis group contains statistics for Network layer conversations

between pairs of hosts.
Application Layer HostThe Application Layer Host group contains statistics on the
Application layer traffic to or from individual hosts.
Application Layer MatrixThe Application Layer Matrix group contains statistics for
Application layer conversations between pairs of hosts.
User History CollectionThis group contains periodic samples of user-specified
variables.
Probe ConfigurationThis group allows for probe configuration issues, such as trap
destinations or OBM (out-of-band management).

QUESTION 322:

Exhibit:

During which stage of the PDIOO process are implementation procedures prepared
in advance to expedite and clarify the actual implementation?

A. PLAN
B. DESIGN
C. IMPLEMENT
D. OPERATE
E. OPTIMIZE
F. RETIREMENT

Answer: B

Explanation:
PDIOO
The network lifecycle is a simple process of planning, designing, implementing,
operating, and optimizing. Whether you face a simple design change or a new network,
the five steps are applicable. If you begin with proper planning, you can ensure a
smoother implementation. Each stage of the lifecycle, although described in one word,
represents a complex grouping of tasks. Those tasks change depending on the project at
hand. However, creating clear and realistic objectives for each stage is the key to
developing subsequent tasks. Treat each stage as if it were its own project, with the same

level of concentration and completeness.
Network Documentation
After completing a network design, you must present it in a manner that is concise and accurate.
Cisco recommends that the network documentation have the following five components:
1. Executive summary
2. Design requirements
3. Design solution
4. Summary
5. Appendix

QUESTION 323:

When validating gathered information, the summary report recommendations correlate which two items? (Choose two.)

A. existing network
B. summary report conclusions
C. customer requirements
D. infrastructure shortcomings
E. actions needed
F. new features

Answer: A,C

Explanation:
While gathering information to create the summary report of existing network, and requirements of customer to create report.

QUESTION 324:

Which value is the most commonly accepted threshhold of acceptable network response time.

A. 1 millisecond
B. 4 milliseconds
C. 10 milliseconds
D. 40 milliseconds
E. 100 milliseconds
F. 400 milliseconds

Answer: E

QUESTION 325:

What is part of the network auditing step when characterizing an existing

enterprise network?

A. customer input on the network topology
B. detail from the NetFlow Collector analysis
C. subdetail of NBAR reports
D. third-party sniffer recommendations
E. show tech-support; show processes cpu commands

Answer: E

Explanation:
show tech-support : To displays system and configuration information. By default
this command displays the output for technical-support-related show commands.
Use keywords to specify the type of information to be displayed.
Show processes cpu : Shows CPU utilization averaged over the past five seconds,
one minute and five minutes. CPU utilization numbers do not provide a true linear
indication of the utilization with respect to the offered load.

QUESTION 326:

DataQuirk is a medical transcription company for exotic-animal veterinarians. The
company recently added a third ISP for international business and is organizing the
enterprise network into a fully operational Enterprise Edge. To which two modules
will the three ISPs be directly related? (Choose two.)

A. Edge Distribution
B. WAN
C. VPN/Remote Access
D. Internet Connectivity
E. E-Commerce
F. PSTN

Answer: D,E,F

Explanation:
Service Provider (SP) Edge
The SP Edge consists of edge services such as the following:
1. Internet services
2. PSTN services
3. WAN services
Enterprises use SPs to acquire network services. ISPs offer enterprises access to the
Internet. ISP have the ability to route the enterprise's networks to their network and to
upstream and peer Internet providers. Some SPs can provide Internet services with DSL
access. For voice services, PSTN providers offer access to the global public voice
network. WAN SPs offer Frame Relay, ATM, and other WAN services for Enterprise
site-to-site connectivity. The SP Edge is not a test topic. For the test, focus on the

Enterprise Campus and Enterprise Edge modules of the Enterprise Composite Network model.

QUESTION 327:

Voice-to-IP encoding and compression take place in which module?

A. Cisco CallManager
B. Voice gateway
C. Gatekeeper
D. Layer 3 switches between the IP phones and the voice gateway

Answer: B

Explanation:
The cisco telephone solution is part of CISCO AVVID (Architecture for Voice, Video and integrated data) and provides a full-featured telephony system running on a IP network. Avaialbe on either the Digital T1/E1 Packet Voice Trunk Network Module or HDV transcoding/Conference DSP Fram And Operating on teh CISCO 2600, 3600, 3700 and Cisco VG200 Gateway product lines, the Cisco Conferencinf and Transcoding for Voice Gateway Routers feature preserves all the WAN, public switched telehpone network (PSTN) and private-branch-exchange (PBX) acccess capabilities provided on these platforms while adding conference and transcode functions. As an integrated solution with Cisco CallManager,feature such as Cisco CallManager failover, reporting and management are all provided.
Voice Gateway relays high quality voice and fax traffic across an IP Netowork. When equiped with digital T1/E1 packet voice trunk network modules and voice-enabled Cisco IOS software the Cisco 3660 supports carrier-class Voice over IP and fax over IP services.
Reference:www.cisco.com

QUESTION 328:

A lightweight access point is added to a working network. Which sequence will it use to associate itself with a wireless LAN controller?

A. master, primary, secondary, tertiary, greatest AP capacity
B. primary, secondary, tertiary, greatest AP capacity, master
C. primary, secondary, tertiary, master, greatest AP capacity
D. greatest AP capacity, primary, secondary, tertiary, master

Answer: C

QUESTION 329:

Given a VoIP network with these attributes:

Codec: G.711
WAN bandwidth: 768Kbps
Packet Header: 6 bytes
Payload: 160 bytes
CRTP: No
How many calls can be made?

A. 8 calls
B. 11 calls
C. 7 calls
D. 9 calls
E. 13 calls

Answer: D

QUESTION 330:

For which technology is IPsec required for a site-to-site enterprise WAN/MAN architecture?

A. Frame Relay
B. SP MPLS VPN
C. ISP Service
D. ATM
E. self-deployed MPLS

Answer: C

QUESTION 331:

Which Cisco security solution offers protection against "day zero" attacks?

A. Cisco IOS Firewall
B. Cisco Security Agent
C. Cisco Traffic Anomaly Detector
D. Cisco Adaptive Security Appliance
E. Cisco IOS IPS

Answer: B