

Cisco.ActualTests.640-864.2012-05-19.257q.by.LLcoolJ

Number: 640-864
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



<http://www.gratisexam.com/>

Cisco 640-864



Designing for Cisco Internetwork Solutions Exam

(DESGN) v2.1

Version: 9.1
Cisco 640-864 Exam

Topic 1, Main Questions

Exam A

QUESTION 1

Which consideration is the most important for the network designer when considering IP routing?

- A. convergence
- B. scalability
- C. on-demand routing
- D. redistribution

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Convergence is most important because with delayed convergence outage recovery will be delayed as well.

Link: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/routed-ex.html#wp998414>

QUESTION 2

You want to gather as much detail as possible during a network audit, to include data time stamping across a large number of interfaces, customized according to interface, with a minimal impact on the network devices themselves. Which tool would you use to meet these requirements?

- A. RMON
- B. SNMPV3
- C. NetFlow
- D. Cisco Discovery Protocol

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

NetFlow provides extremely granular and accurate traffic measurements and a high-level collection of aggregated traffic. The output of netflow information is displayed via the show ip cache flow command on routers. The Table shows a description of the fields for NetFlow output.

Table. Netflow Output escription

Field	Description
Bytes	Number of bytes of memory that are used by the NetFlow cache
Active	Number of active flows
Inactive	Number of flow buffers that are allocated in the Netflow cache
Added	Number of flows that have been created since the start of the summary
Exporting flows	IP address and UDP port number of the workstation to which flows are exported
Flows exported	Total number of flows export and the total number of UDP datagrams
Protocol	IP protocol and well-known port number
Total Flows	Number of flows for this protocol since the last time that statistics were cleared
Flows/sec	Average number of flows this protocol per second
Packets/flow	Average number of packets per flow per second
Bytes/pkt	Average number of bytes for this protocol
Packets/sec	Average number of packets for this protocol per second

QUESTION 3

DataQuirk is a web-based medical transcription company for exotic-animal veterinarians. The company recently added a third ISP for international business. They are organizing the enterprise network into a fully operational Enterprise Edge.

To which two modules will the three ISPs be directly related? (Choose two)

- A. PSTN
- B. E- Commerce
- C. WAN/MAN
- D. Edge Distribution
- E. Internet Connectivity
- F. Remote Access VPN

Correct Answer: BE

Section: (none)

Explanation

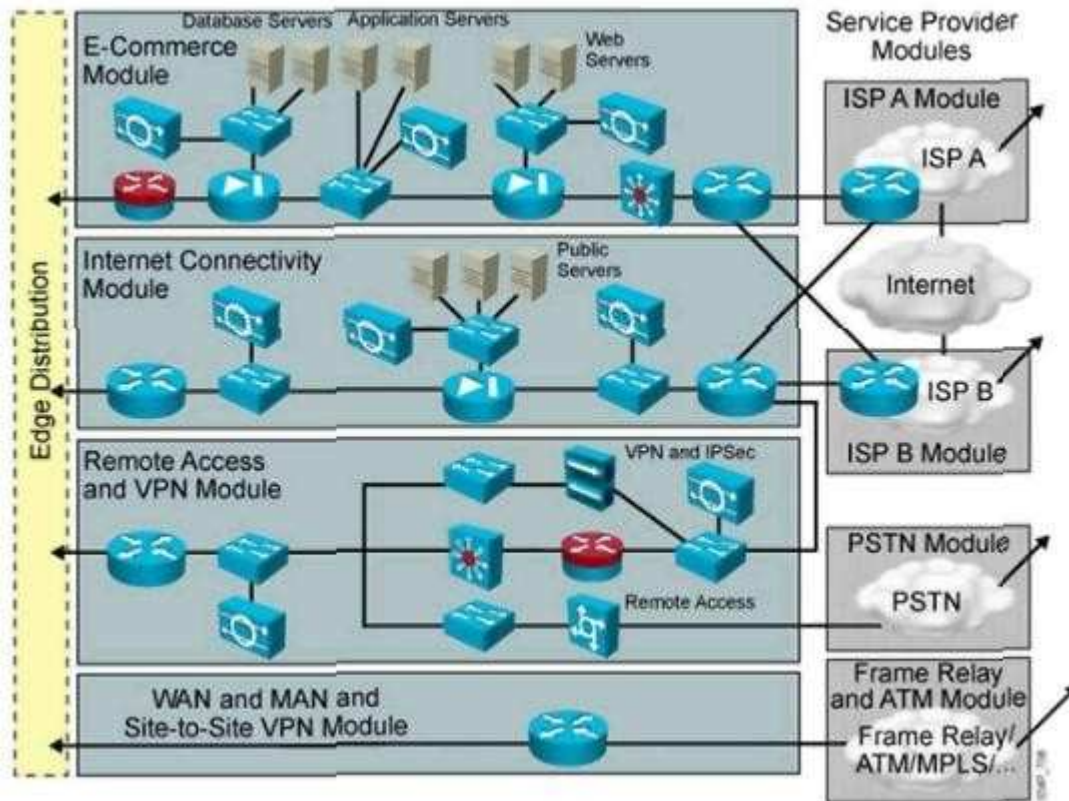
Explanation/Reference:

Explanation: The purpose of ISP link is for serving customers & it is also providing internet connectivity to internal & external users, thus it falls into above 2 categories.

Explanation

The Enterprise Edge Module consists of the following modules:

+ E-commerce module: includes the devices and services necessary for an organization to provide e-commerce applications.
+ Internet connectivity module: provides enterprise users with Internet access.
+ VPN and remote access module: terminates VPN traf and dial-in connections from external users.
+ WAN/ MAN and site-to-site module: provides connectivity between remote sites and the central site over various WAN technologies. In these modules, only E-Commerce and Internet Connectivity modules will be directly related to the three ISPs.



Link: http://leaman.org/ccna4/Chap_1.pdf

QUESTION 4

Which two of these practices are considered to be best practices when designing the access layer for the enterprise campus? (Choose two)

- A. Implement all of the services (QoS, security, STP, and so on) in the access layer, offloading the work from the distribution and core layers.
- B. Always use a Spanning Tree Protocol; preferred is Rapid PVST+.
- C. Use automatic VLAN pruning to prune unused VLANs from trunked interface to avoid broadcast propagation.
- D. Avoid wasted processing by disabling STP where loops are not possible.
- E. Use VTP transparent mode to decrease the potential for operational error

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When designing the building access layer, you must consider the number of users or ports required to size up the LAN switch. Connectivity speed for each host should also be considered. Hosts might be connected using various technologies such as Fast Ethernet, Gigabit Ethernet, or port channels. The planned VLANs enter into the design.

Performance in the access layer is also important. Redundancy and QoS features should be considered. The following are recommended best practices for the building access layer:

- Limit VLANs to a single closet when possible to provide the most deterministic and highly available topology.

- Use Rapid Per-VLAN Spanning Tree Plus (RPVST+) if STP is required. It provides the faster convergence than traditional 802.1d default timers.
 - Set trunks to ON and ON with no-negotiate.
 - Manually prune unused VLANs to avoid broadcast propagation (commonly done on the distribution switch).
 - Use VLAN Trunking Protocol (VTP) Transparent mode, because there is little need for a common VLAN database in hierarchical networks.
 - Disable trunking on host ports, because it is not necessary. Doing so provides more security and speeds up PortFast.
 - Consider implementing routing in the access layer to provide fast convergence and Layer 3 load balancing.
 - Use the switchport host commands on server and end-user ports to enable PortFast and disable channeling on these ports.
 - Use Cisco STP Toolkit, which provides
 - PortFast: Bypass listening-learning phase for access ports
 - Loop Guard: Prevents alternate or root port from becoming designated in absence of bridge protocol data units (BPDU)
 - Root Guard: Prevents external switches from becoming root
 - BPDU Guard: Disables PortFast-enabled port if a BPDU is received
- Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 3, Page 85

QUESTION 5

With deterministic Wireless LAN Controller redundancy design, the different options available to the designer have their own strengths. Which one of these statements is an example of such a strength?

- Dynamic load balancing, or salt-and-pepper access point design, avoids the potential impact of oversubscription on aggregate network performance.
- N+N redundancy configuration allows logically grouping access points on controllers to minimize intercontroller roaming events.
- N+N+1 redundancy configuration has the least impact to system management because all of the controllers are collocated in an NOC or data center
- N+1 redundancy configuration uses Layer 3 intercontroller roaming, maintaining traffic on the same subnet for more efficiency.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: With such an arrangement there is no complex mesh of access points & controllers. Link: <http://www.cisco.com/web/learning/le31/le46/cln/qlm/CCDA/design/understanding-wireless-network-controller-technology-3/player.html>

QUESTION 6

Which of these statements is true concerning the data center access layer design?

- The access layer in the data center is typically built at Layer 3, which allows for better shaping of services across multiple servers.
- With Layer 2 access, the default gateway for the servers can be configured at the access or aggregation layer.
- A dual-homing NIC requires a VLAN or trunk between the two access switches to support the dual IP address on the two server links to two separate switches.
- The access layer is normally not required, as dual homing is standard from the servers to the aggregation layer.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: With Layer 2 / 3, capabilities in-built access layer switches can have data & voice VLANs with interfaces; this is helpful in improving routing convergence.

Link:

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a00805fcc bf.pdf

QUESTION 7

Which one of these statements should the designer keep in mind when considering the advanced routing features?

- A. one-way router redistribution avoids the requirement for state or default routes.
- B. Redistribution, summarization, and filtering are most often applied between the campus core and enterprise edge.
- C. Filtering only occurs on the routing domain boundary using redistribution.
- D. Summarize routes at the core toward the distribution layer.
- E. The hierarchical flexibility of IPv6 addressing avoids the requirement for routing traffic reduction using aggregation.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 8

Which two statements about designing the Data Center Access layer are correct? (Choose two)



<http://www.gratisexam.com/>

- A. Multiport NIC servers should each have their own IP address
- B. Layer 3 connectivity should never be used in the access layer
- C. Layer 2 connectivity is primarily implemented in the access layer
- D. Multiport NIC servers should never be used in the access layer
- E. Layer 2 clustering implementation requires servers to be Layer 2 adjacent

Correct Answer: CE

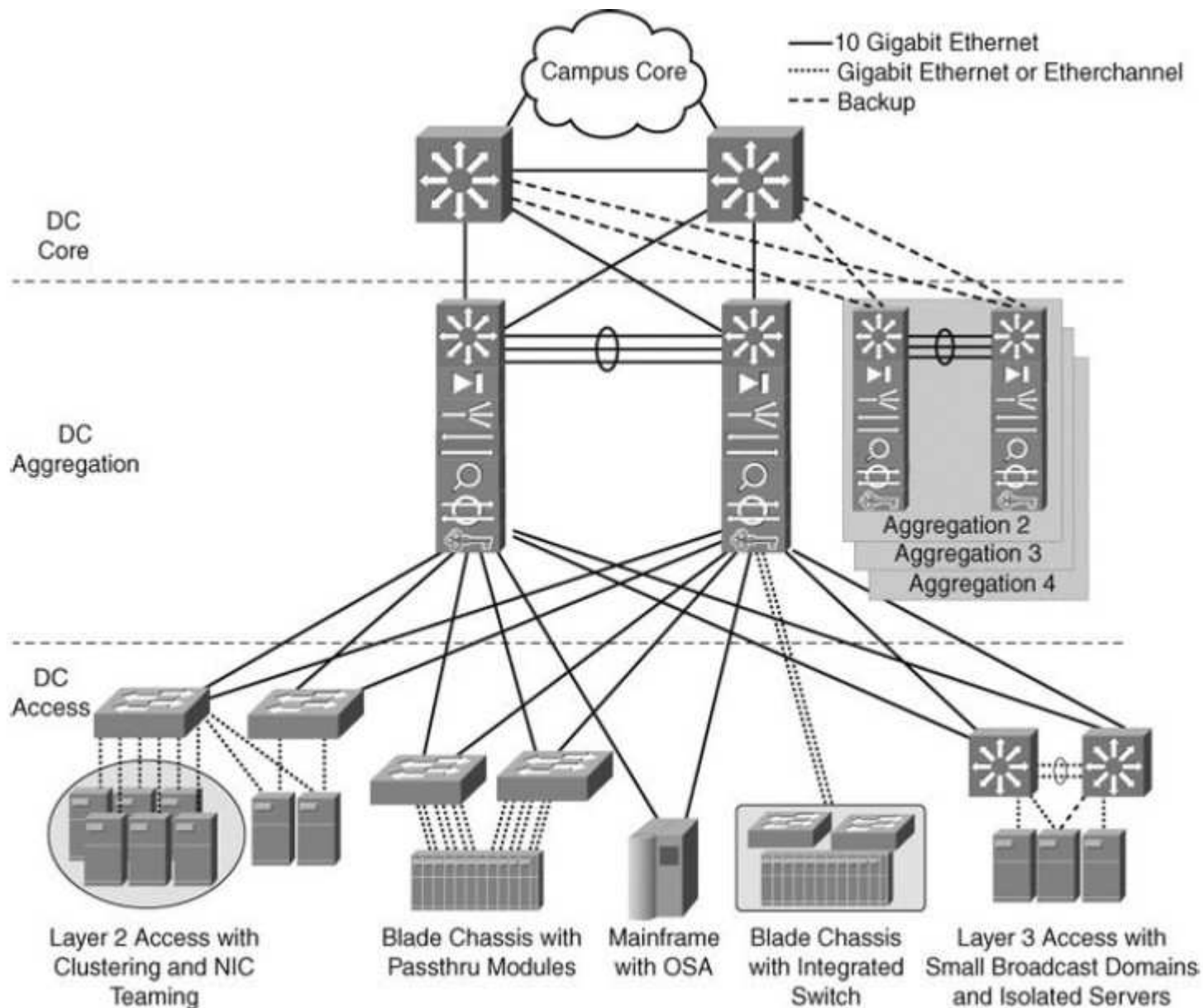
Section: (none)

Explanation

Explanation/Reference:

Explanation:

User access is primarily layer 2 in nature, layer 2 clustering is possible only in layer 2 Here is the explanation from the Cisco press CCDA certification guide Figure 4-8. Enterprise Data Center Infrastructure Overview



Defining the DC Access Layer

The data center access layer's main purpose is to provide Layer 2 and Layer 3 physical port density for various servers in the data center. In addition, data center access layer switches provide high-performance, low-latency switching and can support a mix of oversubscription requirements. Both Layer 2 and Layer 3 access (also called routed access) designs are available, but most data center access layers are built using Layer 2 connectivity. The Layer 2 access design uses VLAN trunks upstream, which allows data center aggregation services to be shared across the same VLAN and across multiple switches. Other advantages of Layer 2 access are support for NIC teaming and server clustering that requires network connections to be Layer 2 adjacent or on the same VLAN with one another.

CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 4

QUESTION 9

Which IPv6 feature enables routing to distribute connection requests to the nearest content server?

- A. Link-local
- B. Site-local

- C. Anycast
- D. Multicast
- E. Global aggregatable

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Anycast is a network addressing and routing methodology in which datagrams from a single sender are routed to the topologically nearest node in a group of potential receivers all identified by the same destination address.

Link: <http://en.wikipedia.org/wiki/Anycast>

QUESTION 10

Which one of these statements is true about addressing redundancy within the WAN environment?

- A. The reliability and speed of DSL allow for cost savings by not including redundant links.
- B. CAMDM and dark fiber offer advanced redundancy features such as automatic backup and repair mechanism to cope system faults.
- C. An SLA is one way to eliminate the need for redundancy.
- D. The failure of a single SONET/SDH link or network element does not lead to failure of the entire network.

Correct Answer: D

Section: (none)

Explanation

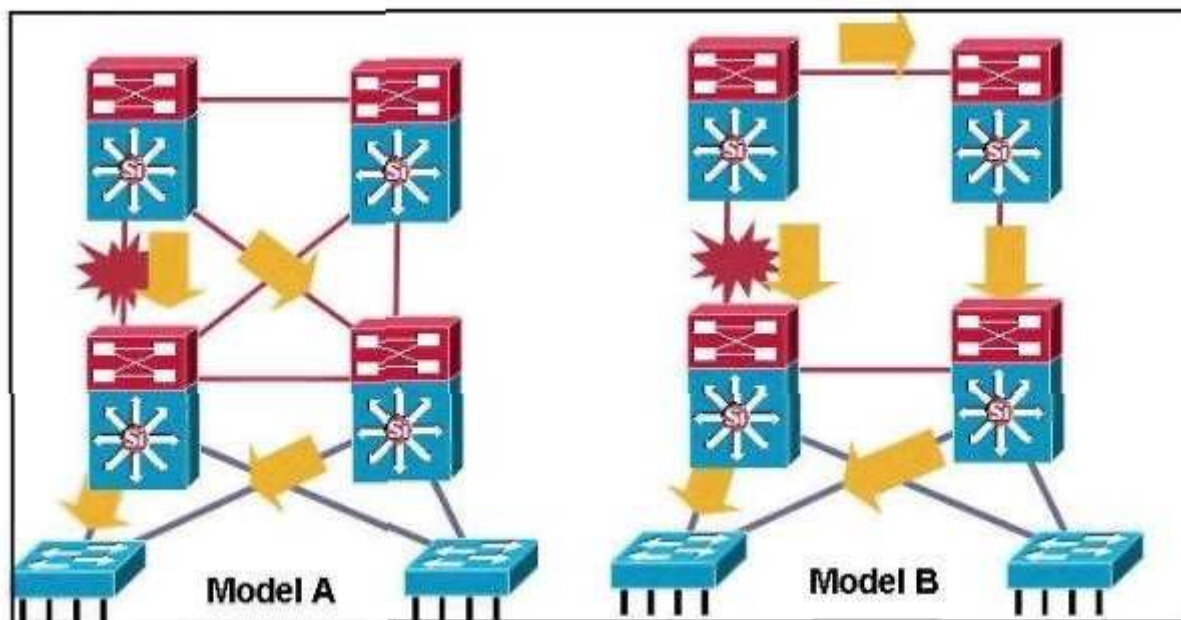
Explanation/Reference:

Explanation: Dual-Ring topologies are being used in WAN environment.

Link: http://en.wikipedia.org/wiki/Ring_network

QUESTION 11

Refer to the exhibit.



Model A is the recommended design for routing between Building Distribution switches and Campus Core

switches. Which two statements describe the reasons? (Choose two)

- A. Model A uses timer-based non-deterministic convergence.
- B. Mode A uses timer-based, providing fast convergence to the remaining path.
- C. In Model A, a link or box failure does not require routing protocol convergence.
- D. In Model A, the Layer 3 redundant equal cost links support fast convergence.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation: Due to redundant links in place the routing protocols can select multiple equal cost paths and installs them as soon as one of the links goes down, such topology also can support load-balancing.

Link:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html

QUESTION 12

Which one of these statements is true concerning the enterprise data center?

- A. It can be located either at the enterprise campus or at a remote branch.
- B. Remote data center connectivity requirements align with the small office design.
- C. The data center designs will differ substantially depending on whether the location is on campus or remote.
- D. A remote branch with a data center becomes the enterprise campus.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: If data center is at enterprise campus there will be no need for installing high capacity WAN links, just an upgrade if existing WAN infrastructure can accommodate increased traffic demands. There are many more such considerations while designing data centers.

Link:

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns994/landing_dc_infrastructure.html

QUESTION 13

Which Cisco security management solution provides the means to identify, isolate, and counter security threats to the network?

- A. Adaptive Security Device Manager
- B. Intrusion Prevention Device Manager
- C. Security Device Manager
- D. Cisco Security Manager
- E. Cisco Security Monitoring, Analysis, and Response System

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation: Cisco Security MARS is a security threat mitigation (STM) system. It delivers a range of information about your networks' health as reported by devices in your network.

Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) is an appliance-based

solution for network security administrators to monitor, identify, isolate, and respond to security threats. MARS understands the network topology and device configurations from routers, switches, firewalls, and IPS devices. MARS also can model packet flows on the network.

Note:

Cisco has a variety of security management products and technologies that allow scalable administration and enforcement of security policy for the Cisco SCF architecture. These solutions reduce the operational management and automate many of the common tasks, including configuration, analysis, incident response, and reporting. Security management platforms include the following:

- Cisco Security Manager (CSM) is an integrated solution for GUI configuration management of firewall, VPN, and IPS policies on Cisco security appliances, firewalls, routers, and switch modules. CSM has capabilities for security policies to be deployed by device, by group, or globally for all devices.
- Cisco Secure Access Control Server (ACS) provides centralized control for administrative access to Cisco devices and security applications. ACS provides for AAA security services and supports routers, switches, VPN services, ASAs, and Cisco NAC clients. In addition, Cisco ACS also supports back-end directory integration with Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory (AD) for authentication services.
- Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) is an appliance-based solution for network security administrators to monitor, identify, isolate, and respond to security threats. MARS understands the network topology and device configurations from routers, switches, firewalls, and IPS devices. MARS also can model packet flows on the network.
- Cisco NAC Manager is an appliance that manages the Cisco NAC servers. NAC Manager has a web-based interface for managing security policies and online users that are part of the NAC infrastructure. Cisco NAC Manager acts as an authentication proxy using Cisco ACS or Microsoft AD.
- System Administration Host provides a centralized host used to stage configuration, software images, and implement network changes.
- Network Time Protocol (NTP) server provides time synchronization to NTP clients such as routers and switches. Time synchronization is crucial in the analysis of event correlations

QUESTION 14

A global corporation has an internal network with the following characteristics:

- 2,000,000+ hosts
- 10,000 + routers
- Internal connectivity
- high traffic volumes with business partners and customers

Which statement best describes what a flexible IPv6 strategy would look like for this corporation?

- A. Both hosts and routers would run dual stack
- B. Hosts would run IPv4 and routers would run native IPv6
- C. Hosts would run dual stack and routers would run IPv4 only
- D. Hosts would run IPv6 and routers would run native IPv6

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Dual-stack is the preferred, most versatile way to deploy IPv6 in existing IPv4 environments. IPv6 can be enabled wherever IPv4 is enabled along with the associated features required to make IPv6 routable, highly available, and secure. In some cases, IPv6 is not enabled on a specific interface or device because of the presence of legacy applications or hosts for which IPv6 is not supported. Inversely, IPv6 may be enabled on interfaces and devices for which IPv4 support is no longer needed.

Link: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/CampIPv6.html#wp389920>

QUESTION 15

Which of these is the best routing deployment for a single dedicated link to an ISP for Internet access?

- A. EIGRP

- B. RIP
- C. BGP
- D. Static
- E. OSPF

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Static routing reduces the complexity and is best way of routing when there are no redundant paths to be maintained.

Link: <http://oreilly.com/catalog/cisco/chapter/ch05.html>

QUESTION 16

In terms of remote office design, which one of these statements is a characteristics only of a small remote office (up to 50 user), and not of medium or remote offices?

- A. Link redundancy to access layer switches is not possible with an integrated design.
- B. A collapsed access and distribution layer is required.
- C. There are no loops in the network design.
- D. Layer 3 services such as DHCP, firewall, and NAT are provided by enterprise campus.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 17

Which two statements about the data Center Aggregation layer are correct? (Choose two)

- A. Layer 4 through layer 7 services are provided in that layer
- B. STP should never be supported in that layer
- C. That layer is the critical point for control and application services
- D. Layer 2 connectivity is provided in that layer from the data center to the core

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation: Data Center aggregation layer connects various network modules together. Link: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html>

QUESTION 18

According to Cisco, which four improvements are the main benefits of the PPDIOO lifecycle approach to network design? (Choose four)

- A. faster ROI
- B. improved business agility
- C. increased network availability
- D. faster access to applications and services
- E. lower total cost of network ownership

F. better implementation team engagement

Correct Answer: BCDE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The PPDIOO life cycle provides four main benefits:

+ It improves business agility by establishing business requirements and technology strategies. + It increases network availability by producing a sound network design and validating the network operation.

+ It speeds access to applications and services by improving availability, reliability, security, scalability, and performance.

+ It lowers the total cost of ownership by validating technology requirements and planning for infrastructure changes and resource requirements.

(Reference: Cisco CCDA Official Exam Certification Guide, 3rd Edition) described in the link below.

Link: <http://www.ciscopress.com/articles/article.asp?p=1608131&seqNum=3>

QUESTION 19

With respect to IPv6 addressing, from a design perspective, which of these statements is it important to keep in mind?

A. IPv6 addressing provides convenience of anycast addressing without any configuration requirements.

B. IPv6 does not use multicast addressing.

C. An IPv6 router will not forward packets from one link to other links if the packet has either a link-local source or a link-local destination address.

D. Dynamic address assignment requires DHCPv6.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Link local addresses are local to the LAN only, they are not communicated across LAN boundaries.

Link: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/CampIPv6.html>

QUESTION 20

When designing the infrastructure protection portion for the enterprise edge, which of these solutions would be the most appropriate solution to consider?

A. 802.1X

B. ACLs in the core layer

C. Cisco Security MARS

D. AAA

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Security in the Enterprise Edge

Cisco Security Category	Security Solutions
Identity and access control	Firewalls, IPsec, SSL VPN, and ACLs
Threat detection and mitigation	NetFlow, syslog, SNMP, RMON, IDS modules, CS-MARS, and NIPS
Infrastructure protection	AAA, CoPP, TACACS, RADIUS, SSH, SNMP v3, IGP/EGP MD5, RFC 2827 ingress filtering and Layer 2 security features
Security management	CSM, CS-MARS, and ACS

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 13

QUESTION 21

What is primary consideration when choosing a routed network design over a traditional campus network design?

- A. Layer 3 service support at the network edge
- B. the routing protocol choice: open (OSPF) or proprietary (EIGRP)
- C. the routing abilities of the host devices
- D. the need to control the broadcast domains within the campus core

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

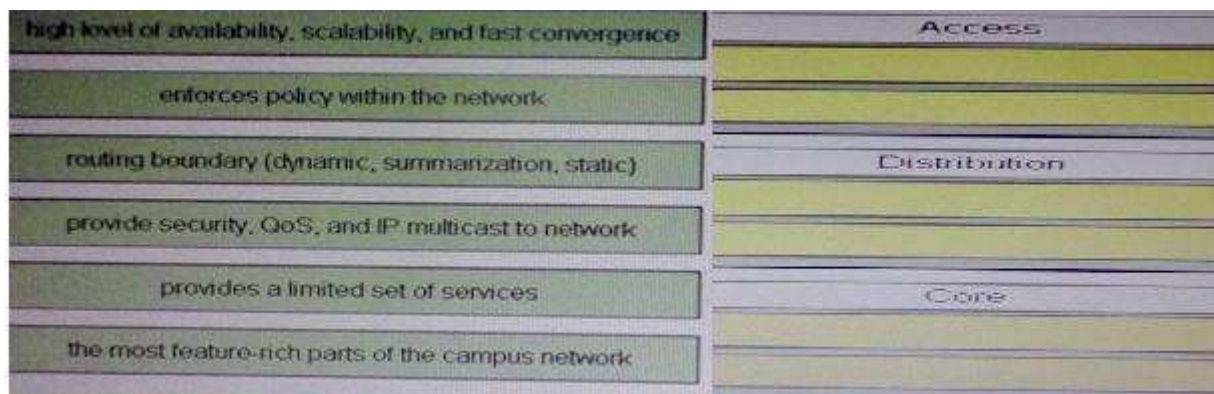
Explanation: Layer 3 ability at network edge should be available to leverage the benefits of routed network design.

Link: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html>

QUESTION 22

DRAG DROP

Drag the characteristics of the traditional campus network on the left to the most appropriate hierarchical network layer on the right.



- A.
- B.

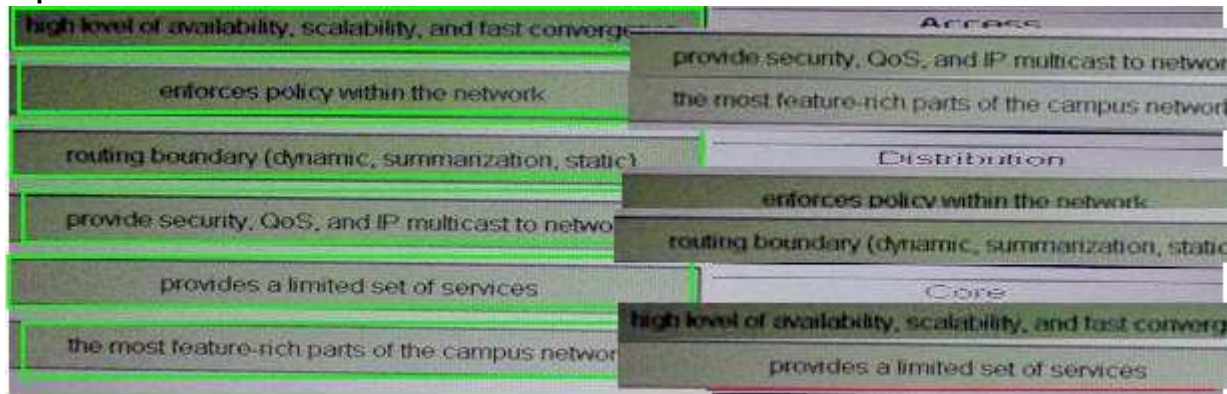
- C.
- D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:



Explanation:

Access

Distribution

Core

Large-Building LANs

Large-building LANs are segmented by floors or departments. The building-access component serves one or more departments or floors. The building-distribution component serves one or more building-access components. Campus and building backbone devices connect the data center, building-distribution components, and the enterprise edge-distribution component. The access layer typically uses Layer 2 switches to contain costs, with more expensive Layer 3 switches in the distribution layer to provide policy enforcement. Current best practice is to also deploy multilayer switches in the campus and building backbone.

Cisco Enterprise Architecture Model

Core

Distribution

Access

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 3

QUESTION 23

Which two statements best describe an OSPF deployment? (Choose two)

- A. ABR provides automatic classful network boundary summarization.
- B. ABR requires manual configuration for classful network summarization
- C. External routes are propagated into the autonomous system from stub areas via ASBR.
- D. External routes are propagated into the autonomous system from regular areas or NSSA via ASBR.
- E. External routes are propagated into the autonomous system from regular areas or NSSA via ABR.

Correct Answer: BD

Section: (none)

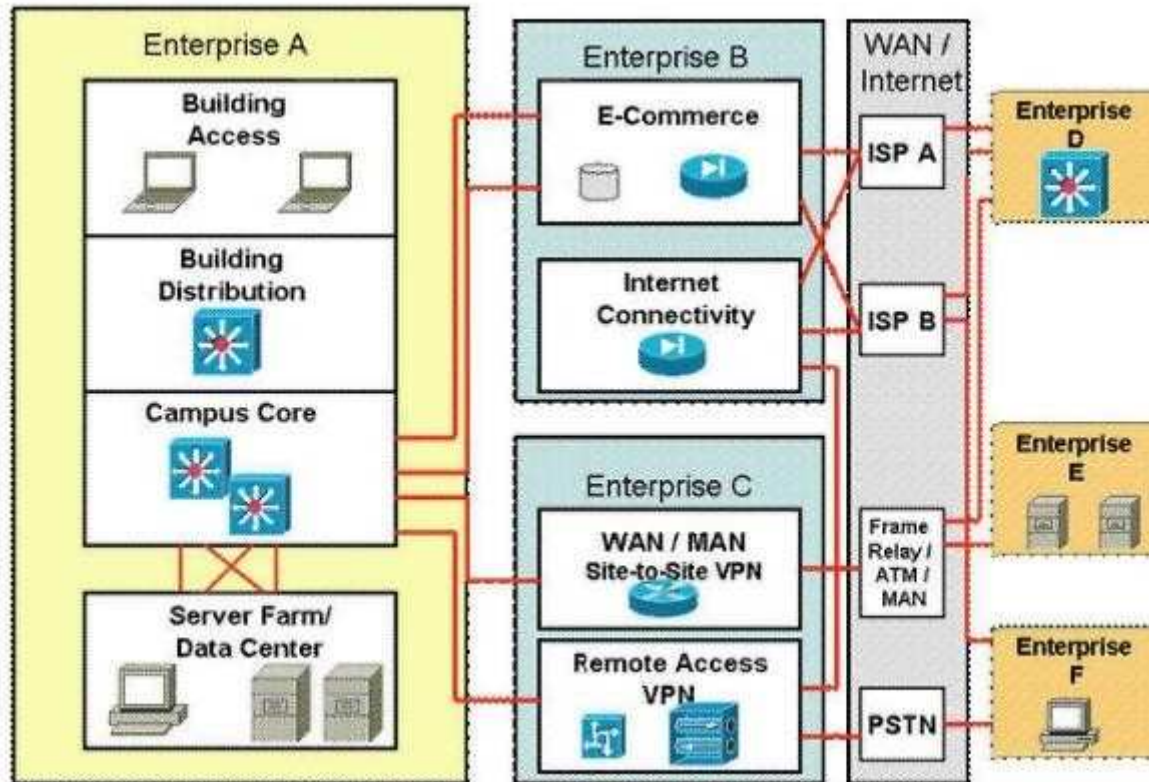
Explanation

Explanation/Reference:

Explanation: Refer to the link below, the protocol is designed to function that way. Link: http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.shtml

QUESTION 24

Refer to the exhibit.



Which module is the Enterprise WAN module?

- A. Enterprise A
- B. Enterprise B
- C. Enterprise C
- D. Enterprise D
- E. Enterprise E
- F. Enterprise F

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: WAN module consists of WAN link terminal devices, routers, firewalls, remote access services. Link: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html#wp708780>

QUESTION 25

A large enterprise requires sensitive information be transmitted over a public infrastructure. It requires confidentiality, integrity, and authenticity. Which security solution best meets these requirements?

- A. Cisco IOS Firewall
- B. Intrusion Prevention
- C. IPSEC
- D. AAA
- E. Traffic Guard Protector
- F. SECURE CONECTIVITY

Correct Answer: C

Section: (none)

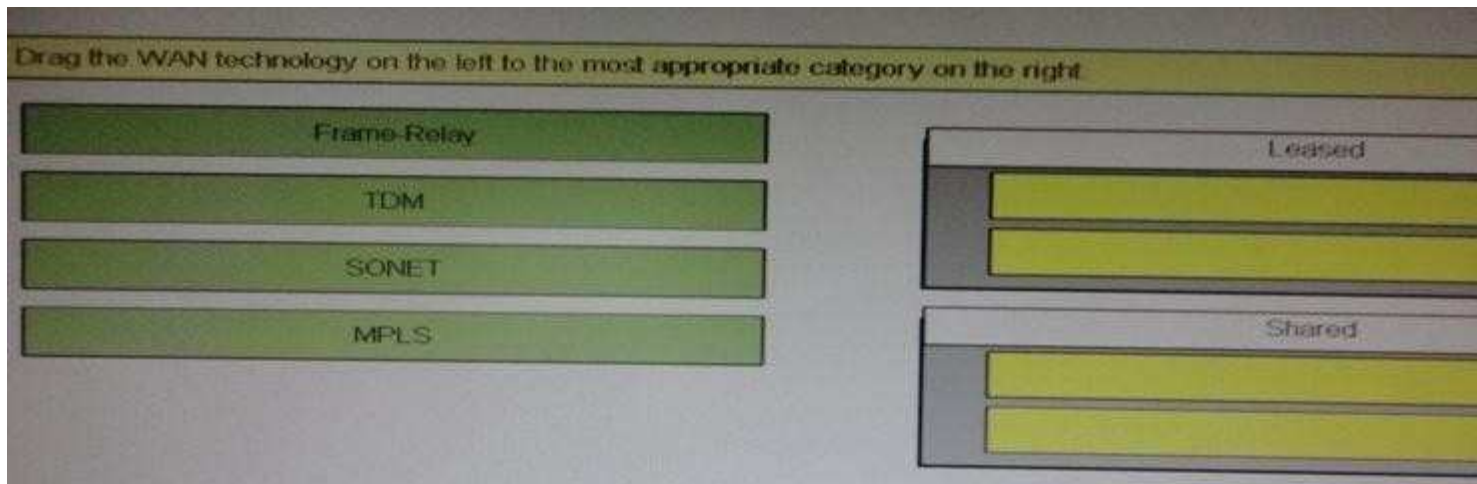
Explanation

Explanation/Reference:

Explanation: IPSec provides CIA (Confidentiality, Integrity & Authencity) Link: <http://nl.wikipedia.org/wiki/IPsec>

QUESTION 26

DRAG DROP



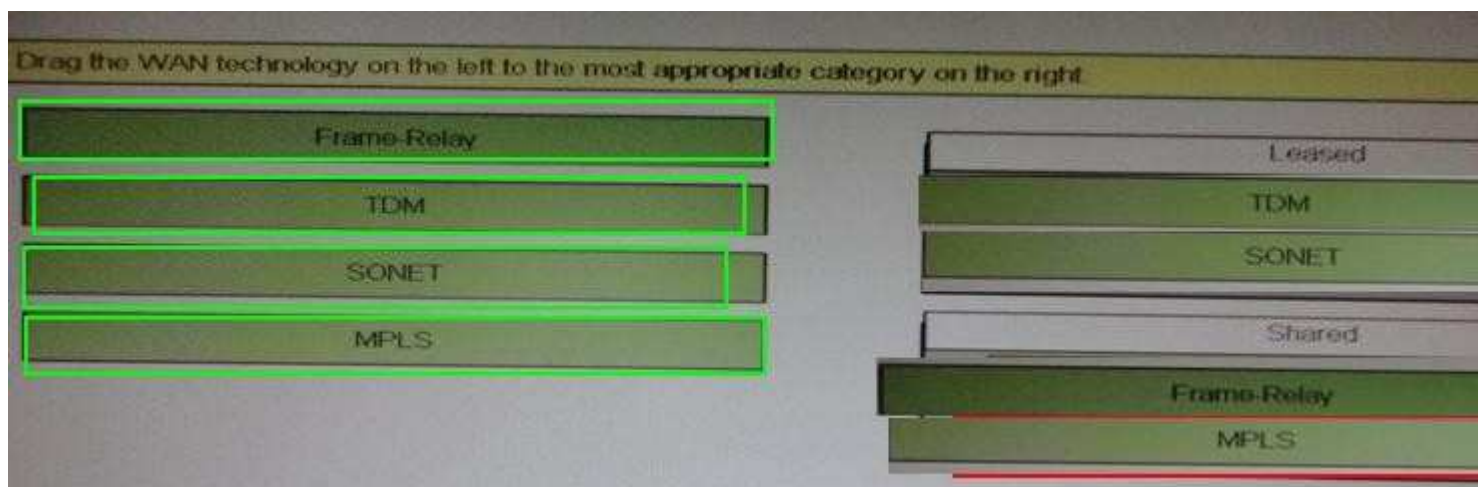
- A.
- B.
- C.
- D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:



Explanation:

Leased

SHARED

WAN Link characteristics				
	Use	Cost	Advantages	Examples
Private	WAN to connect distant LANs	Owner must buy and configure network Expensive to maintain	High security Transmission quality	Metro Ethernet using Dark Fiber
Leased	WAN to connect distant LANs	High cost Equipment is leased or private	Provider is responsible for maintenance Dedicated bandwidth	TDM, SONET
Shared	Shared circuit or packet switched WAN	Cost is fair Bandwidth is leased Equipment is leased or private	Provider is responsible for maintenance Shared network for multiple sites	MPLS or FR

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 6

QUESTION 27

There are a number of advantages to using virtualization within the data center module. Which the following two are samples of these advantages?

- A. Virtualization consolidates many low-performance devices into a few high-performance devices, providing a more efficient utilization of hardware and increasing the price/performance ratio.
- B. Virtualization compartmentalizes a single device into a few high-performance devices, providing a more efficient utilization of hardware and increasing the price/performance ratio.
- C. Dynamic forcibility eliminates the need to add, reassign, or repurpose resources in the system.
- D. Virtualization separates user via different physical networks into groups with visibility into only their logical network.

E. Virtualization provides distinct security policies per physical device.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 28

DRAG DROP

Drag the data center property on the left to the design aspect on the right it is most apt to

variability of computing load, computing power and memory requirements	
disasters, fire suppression and alarm systems	
abundant, variable, well organized and easy to maintain	
amount of racks, equipment, cabling, people	
arranging equipment racks face-to-face or back-to-back	
rack servers vs blade servers	

A.

B.

C.

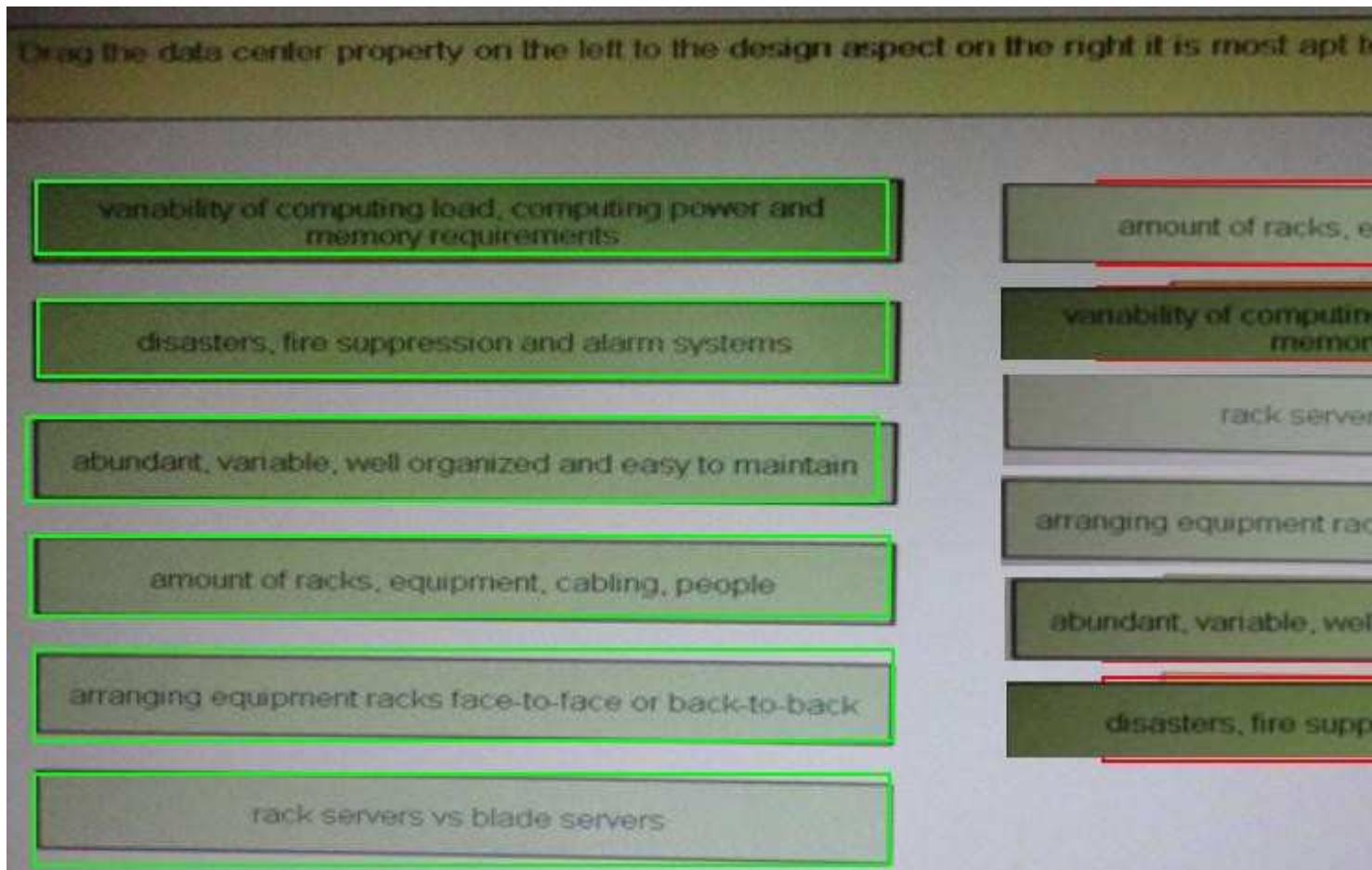
D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:



Explanation: 1 Weight Load

2 Security

3 Cabling

4 Space

5 Cooling

6 Power

please refer to the link below.

Link:

http://www.cisco.com/application/pdf/en/us/guest/netso/ns107/c649/ccmigration_09186a008073377d.pdf

QUESTION 29

When selecting which hardware switches to use throughout an enterprise campus switched network, which consideration is not relevant?

- A. whether data link layer switching based the MAC address is required
- B. the number of shared media segments
- C. which infrastructure service capabilities are required
- D. whether to support Layer 3 services at the network edge.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Shared media are not used in modern networks; all links are operating full-duplex Link: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html>

QUESTION 30

Layer 2 switching is exclusively used in which Enterprise Campus Module layer?

- A. Server Farm
- B. Campus Core
- C. Building Access
- D. Building Distribution
- E. Internet Connectivity

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Access layer provides network connectivity to end users which is layer 2 in nature. Link: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html#wp708780>

QUESTION 31

Which one of these statements describes why, from a design perspective, a managed VPN approach for enterprise teleworkers is a most effective?

- A. A managed VPN solution uses a cost effective, on-demand VPN tunnel back to the enterprise
- B. This solution supports all teleworkers who do not require voice or video
- C. This architecture provides centralized management where the enterprise can apply security policies and push configurations.
- D. It provides complete flexibility for remote access through a wireless hotspot or a guest network at a host, in addition to a home office.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Here is the answer from the Cisco Certification guide.

Enterprise Teleworker Design

Enterprise teleworkers need to be differentiated from the occasional remote worker. The full-time enterprise teleworker has more extensive application access and requirements than the occasional remote worker.

Occasionally, remote users connect to the corporate network at a hotspot, but generally they do not have the same application demands of an enterprise teleworker. Generally, enterprise teleworkers connect to a local ISP through a cable or DSL connection in their residence.'

The Cisco Virtual Office Solution for the Enterprise Teleworker is implemented using the Cisco 800 series ISRs. Each ISR has integrated switch ports that then connect to the user's broadband connection. The solution uses a permanent always-on IPsec VPN tunnel back to the corporate network. This architecture provides for centralized IT security management, corporate-pushed security policies, and integrated identity services. In addition, this solution supports the enterprise teleworker needs through advanced applications such as voice and video. For example, the enterprise teleworker can take advantage of toll bypass, voicemail, and advanced IP phone features not available in the PSTN.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 7

QUESTION 32

Which one of these statements is true when considering the design of voice and video services for the enterprise campus network?

- A. Access layer switches should support 802.1Q trunking and 802.1p for Layer 2 CoS packet marking on Layer 2 ports with IP phones connected.
- B. Combining voice and data and a single VLAN simplifies QoS trust boundaries, VLAN access control, and ease of management.
- C. Data devices will also require access to priority queues via packet tagging.
- D. Fixed network delays (serialization, propagation, and so on) are generally unpredictable and more difficult to calculate than variable network delays.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

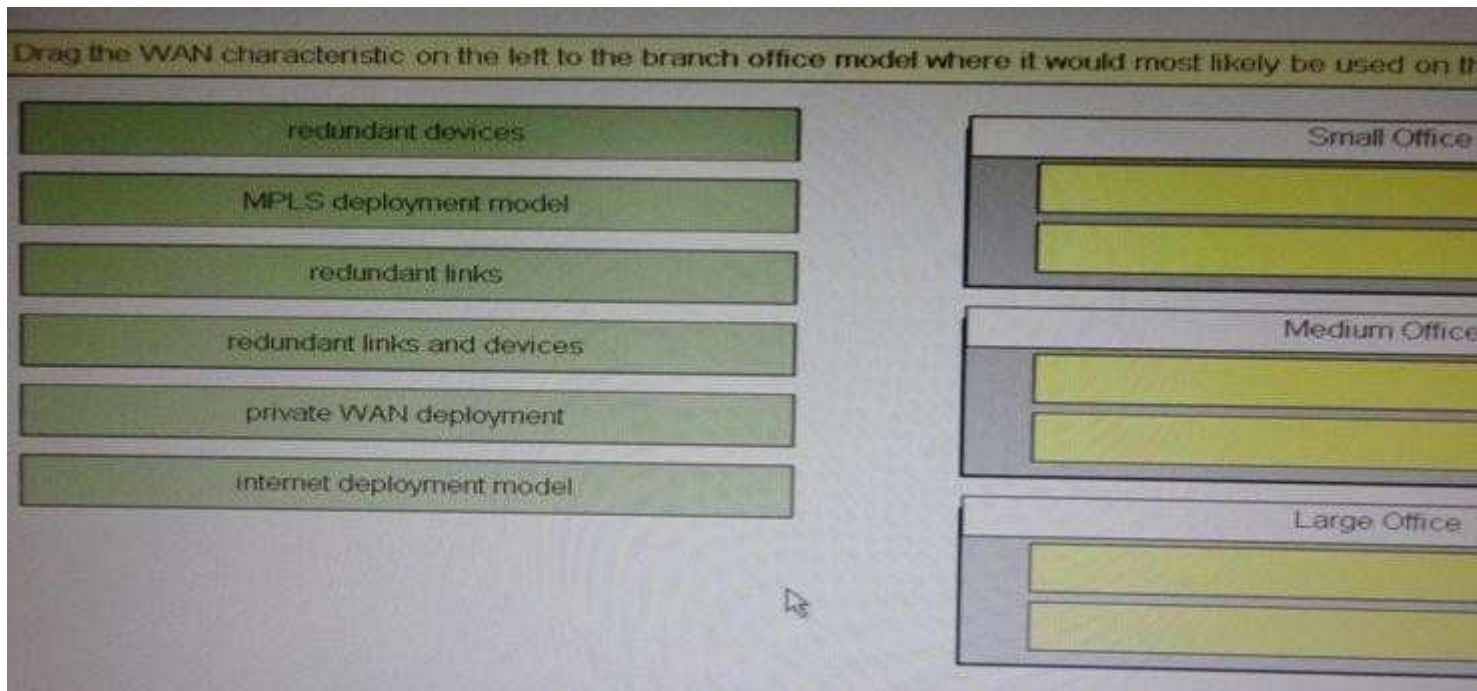
Explanation: 802.1Q & 802.1P are required for Vlan tagging & prioritizing voice frames.

Link:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_sec/configuration/guide/swvoip.html

QUESTION 33

DRAG DROP



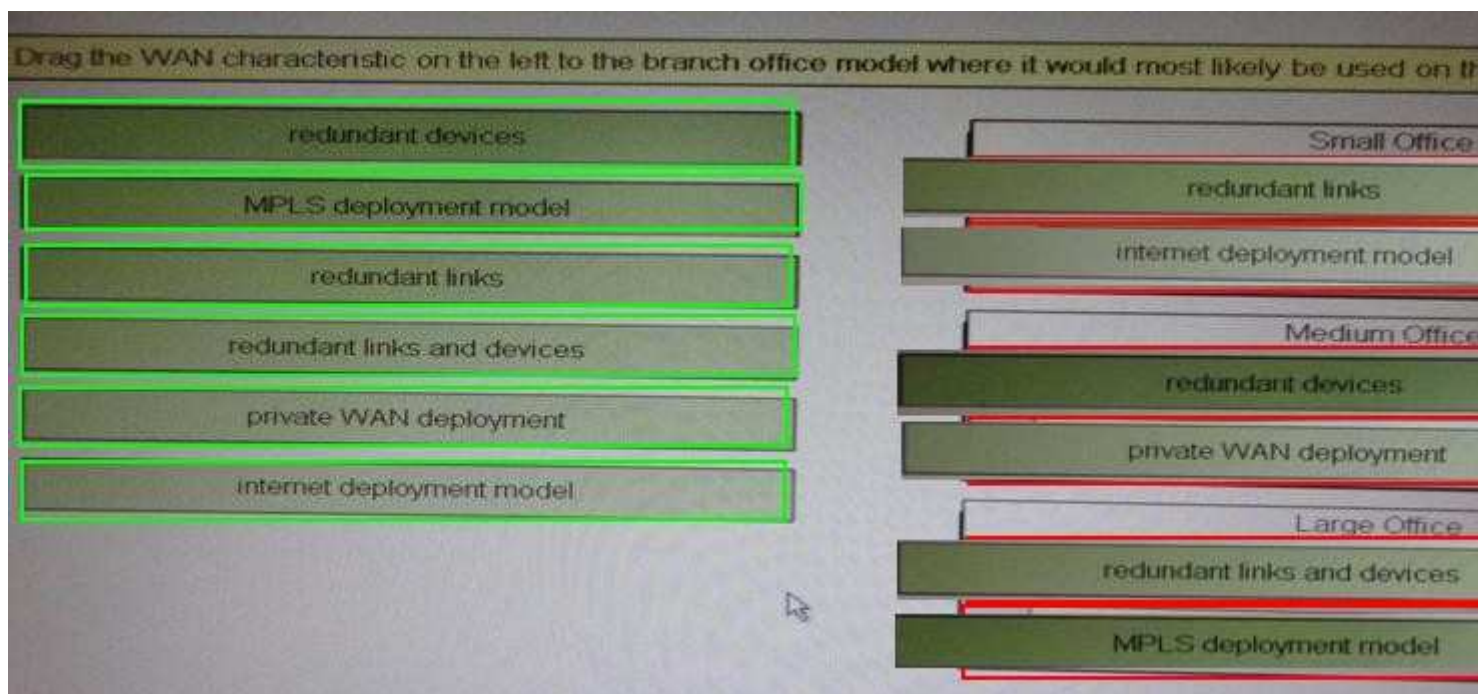
- A.
- B.
- C.
- D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:



Explanation: Explanation

Small Office

- Redundant Links

- Internet Deployment Model

Medium Office

- Redundant devices

- Private WAN deployment

Large Office

- Redundant Links and Devices

- MPLS Deployment model

Small Branch Design

The small branch design is recommended for branch offices that do not require hardware redundancy and that have a small user base supporting up to 50 users. This profile consists of an access router providing WAN services and connections for the LAN services.

The Layer 3 WAN services are based on the WAN and Internet deployment model. A T1 is used for the primary link, and an ADSL secondary link is used for backup. Other network fundamentals are supported, such as EIGRP, floating static routes, and QoS for bandwidth protection.

Medium Branch Design

The medium branch design is recommended for branch offices of 50 to 100 users, which is similar to the small branch but with an additional access router in the WAN edge (slightly larger) allowing for redundancy services.

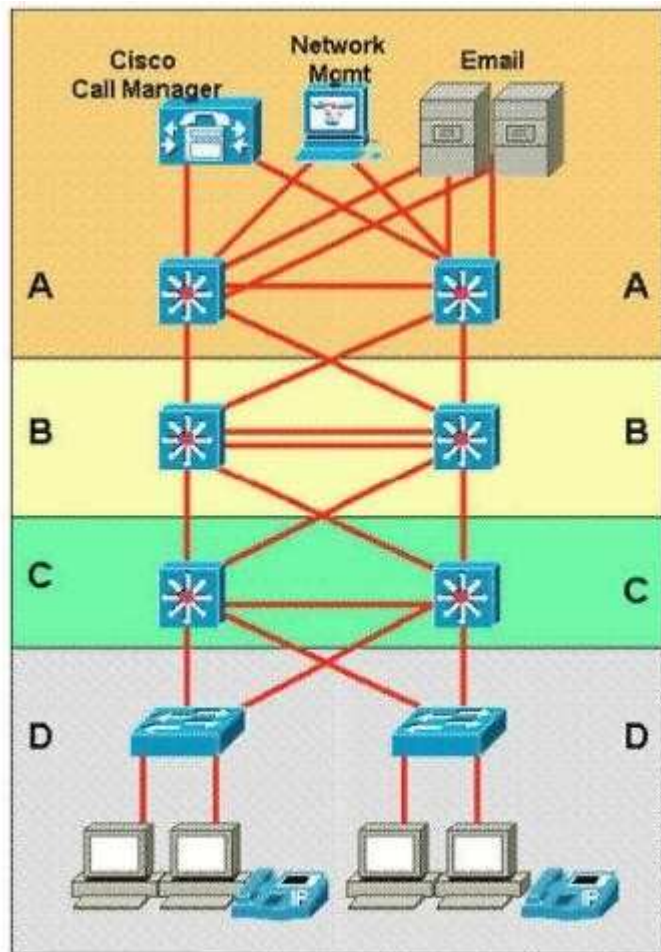
Large Branch Design

The large branch design is the largest of the branch profiles, supporting between 100 and 1000 users. This design profile is similar to the medium branch design in that it also provides dual access routers in the WAN edge. In addition, dual Adaptive Security Appliances (ASA) are used for stateful firewall filtering, and dual distribution switches provide the multilayer switching component. The WAN services use an MPLS deployment model with dual WAN links into the WAN cloud.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 7

QUESTION 34

Refer to the exhibit.



Which two statements correctly identify the layers of the Enterprise Campus module?

(Choose two)

- A. A is the Data Center Module and C is the Campus Core layer
- B. A is the Data Center Module and D is the Building Access layer
- C. B is the Campus Core layer and C is the Building Distribution layer
- D. B is the Building Distribution layer and C is the Campus Core layer
- E. A is the Internet Connectivity layer and B is the Campus Core layer
- F. B is the Building Distribution layer and D is the Building Access layer

Correct Answer: BC

Section: (none)

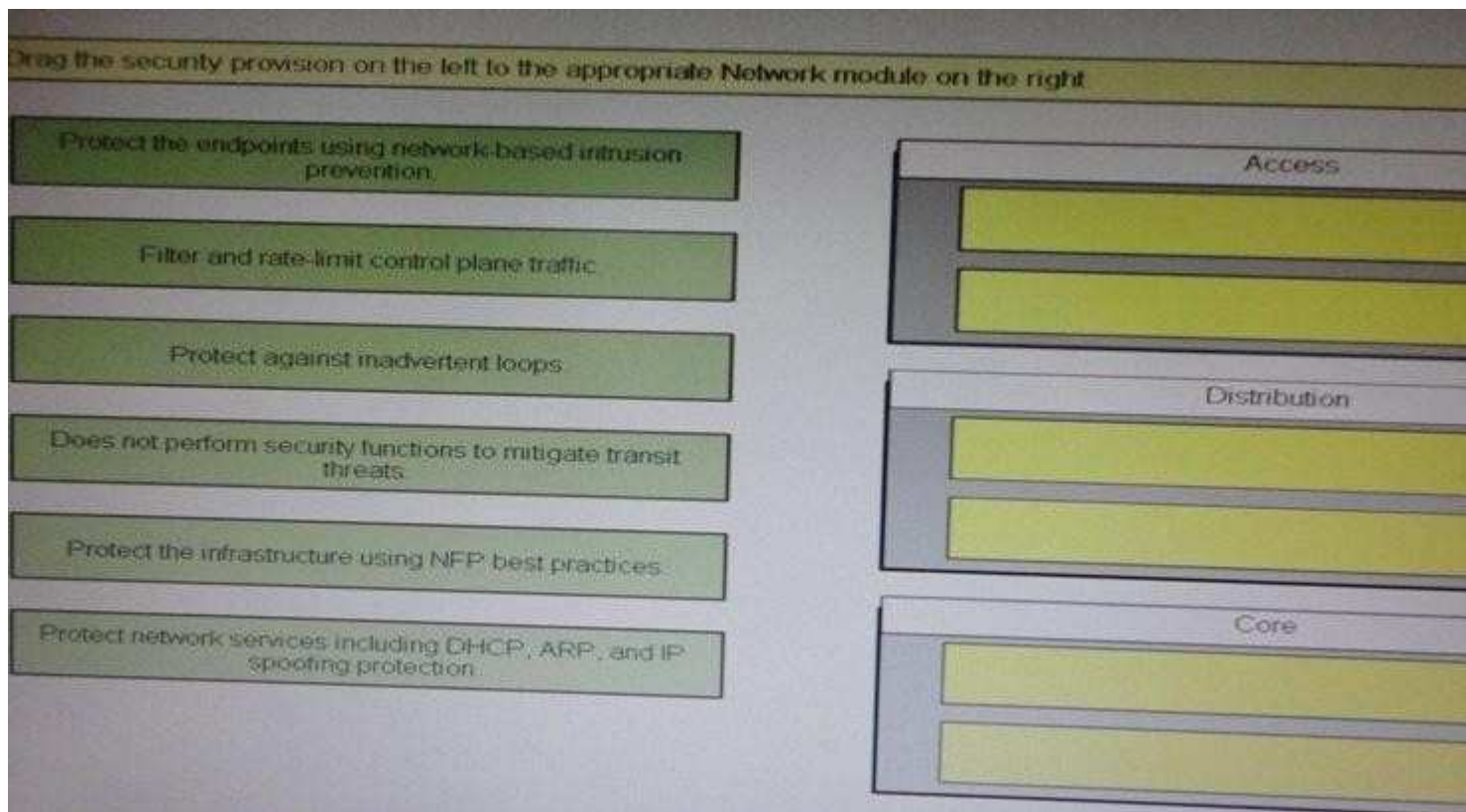
Explanation

Explanation/Reference:

Explanation: Module characteristics show to which category the blocks belong to. Link: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html#wp708780>

QUESTION 35

DRAG DROP



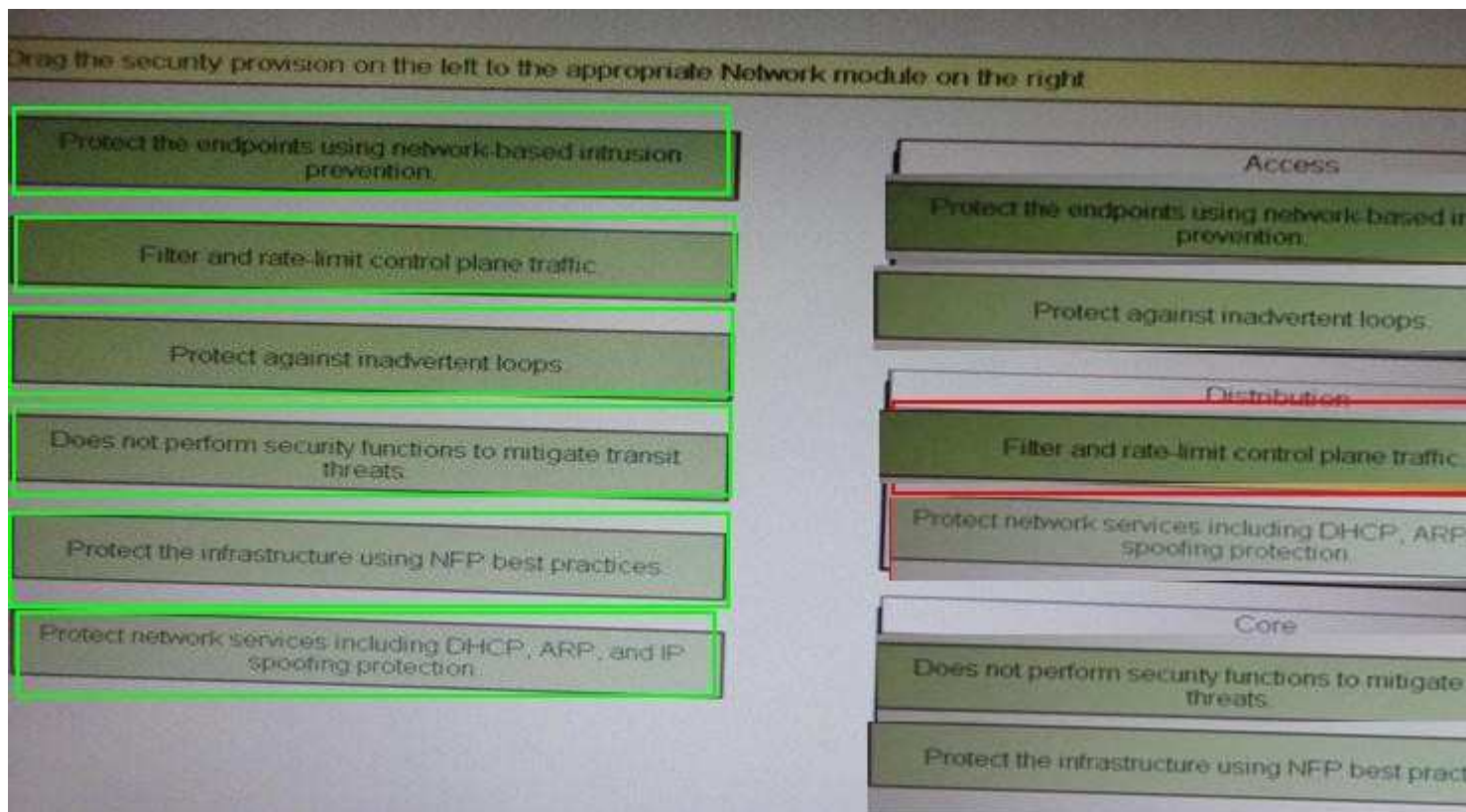
- A.
- B.
- C.
- D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:



Explanation: 1 Access

2 Distribution

3 Access

4 Core

5 Access

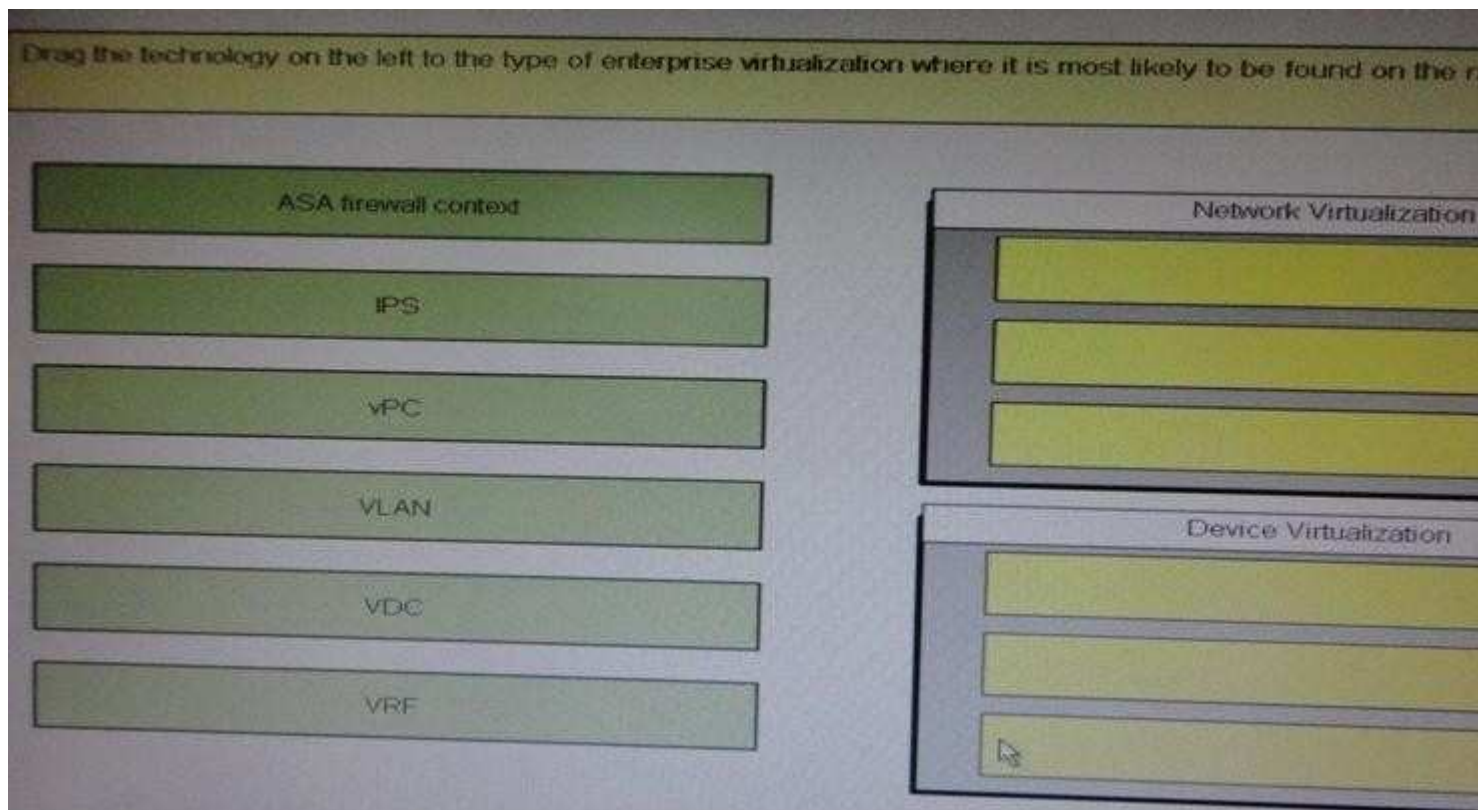
6 Distribution

Please refer to link.

Link: <http://www.ciscopress.com/articles/article.asp?p=1073230&seqNum=2>

QUESTION 36

DRAG DROP



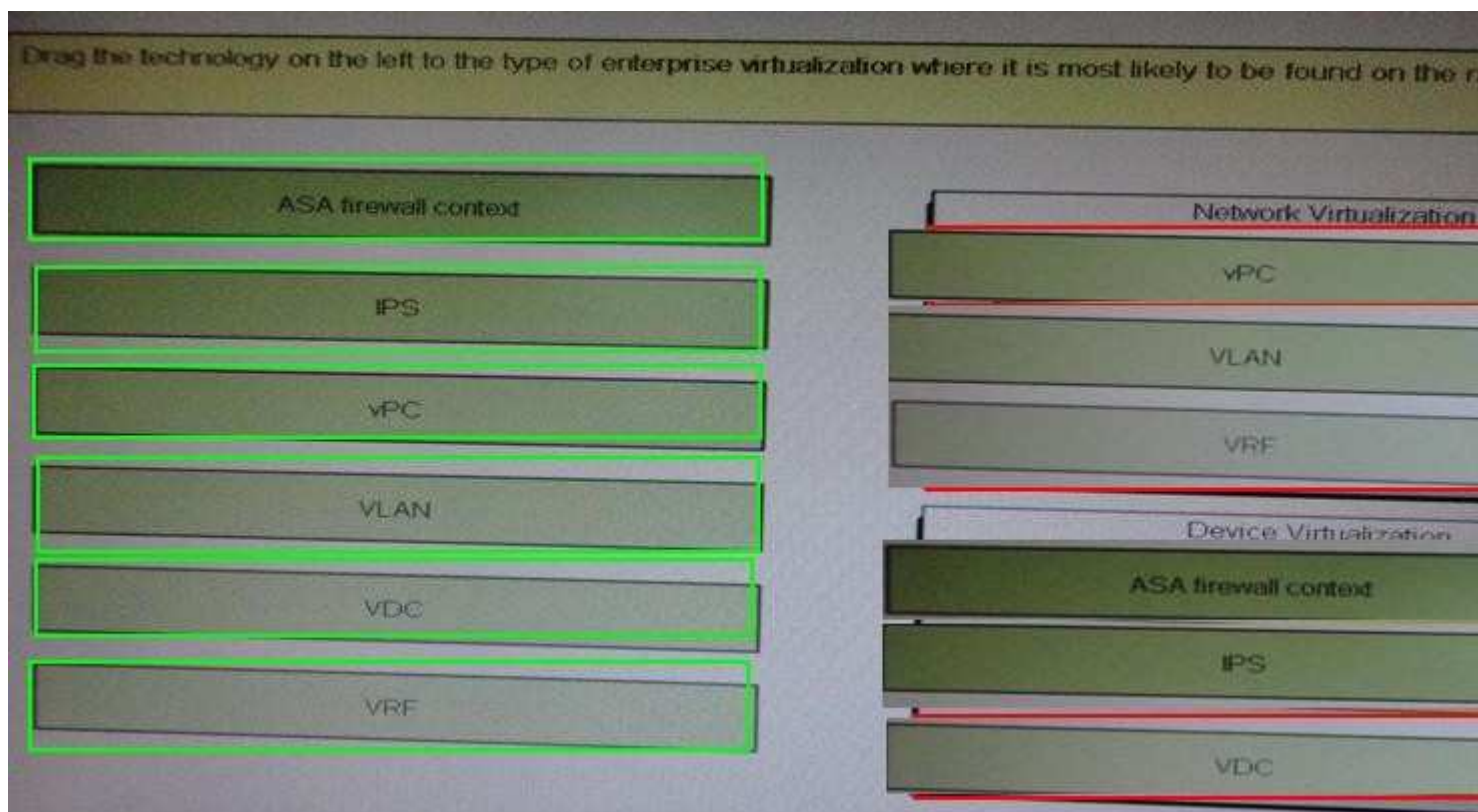
- A.
- B.
- C.
- D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:



Explanation: Here is the correct answer

Network Virtualization

- * VPC
- * VLAN
- * VRF

Device Virtualization

- *ASA firewall context
- *IPS
- *VDC

Explanation

Network virtualization encompasses logical isolated network segments that share the same physical infrastructure. Each segment operates independently and is logically separate from the other segments. Each network segment appears with its own privacy, security, independent set of policies, QoS levels, and independent routing paths.

Here are some examples of network virtualization technologies:

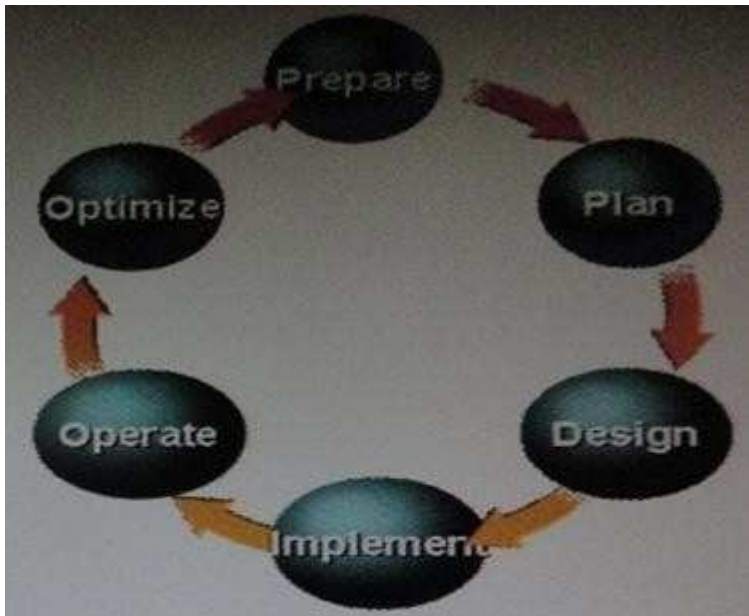
Device virtualization allows for a single physical device to act like multiple copies of itself. Device virtualization enables many logical devices to run independently of each other on the same physical piece of hardware. The software creates virtual hardware that can function just like the physical network device. Another form of device virtualization entails using multiple physical devices to act as one logical unit.

Here are some examples of device virtualization technologies:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 4

QUESTION 37

Refer to the exhibit.



During which stage of the PPDIOO process are implementation procedures prepared?

- A. Prepare
- B. Plan
- C. Design
- D. Implement
- E. Operate
- F. Optimize

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Design phase includes network diagrams and an equipment list. The project plan is updated with more granular information for implementation. This is the so-called "prepare implementation procedures". implementation is done during Implement phase.

Link: <http://www.ciscopress.com/articles/article.asp?p=1608131&seqNum=3>

QUESTION 38

Which statement describes the recommended deployments of IPv4 addressing in the Cisco Network Architecture for the Enterprise?

- A. private addressing throughout with public addressing in the Internet Connectivity module
- B. private addressing throughout with public addressing in the Internet Connectivity and E- Commerce modules
- C. private addressing throughout with public addressing in the Internet Connectivity, E-Commerce, and Remote Access and VPN modules
- D. private addressing throughout with public addressing in the Internet Connectivity, E-Commerce, and Enterprise Branch modules

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: E-Commerce, and Remote Access and VPN modules provide services to external users, customer and need to be available without NAT as NAT has inherent issues with many application level services.

Link: http://leaman.org/ccna4/Chap_1.pdf

QUESTION 39

For which network scenario is static routing most appropriate?

- A. parallel WAN links
- B. IPSec VPN
- C. expanding networks
- D. hierarchical routing

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: IPSec VPN are point to point connections and works easily with static routes.

Link: CCDA Self Study Guide: Diane Teare

QUESTION 40

When considering the three VoIP design models single site, centralized multisite, and distributed multisite which question below would help to eliminate one of these questions?

- A. Will the switches be required to provide inline power?
- B. Will users need to make off site calls, beyond the enterprise?
- C. Will users require applications such as voice mail and interactive voice response?
- D. Are there users whose only enterprise access is via a QoS-enabled WAN?

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: VoIP designing should consider how users are connecting to campus.

Link: http://www.net130.com/tutorial/cisco-pdf/Cisco_%20IP%20Telephony%20Network%20Design_Guide.pdf

QUESTION 41

Which aspect would most likely be found in the draft design document?

- A. a list of QoS requirements
- B. a note that there are no segments with more than 70 percent broadcast or multicast traffic
- C. the level of redundancy or high availability that currently exists or is required in the network
- D. the list of network infrastructure services which are in use, such as voice and video

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 42

Your company's Cisco routers are operating with EIGRP. You need to join networks with an acquisition's heterogeneous routers at 3 sites, operating with EIGRP and OSPF. Which describes the best practice for routing protocol deployment?

- A. apply OSPF throughout both networks
- B. apply one-way redistribution exclusively at each location
- C. apply two way redistribution exclusively at each location
- D. apply two-way redistribution at each location with a route filter at only one location
- E. apply two-way redistribution at each location with a route filter at each location
- F. apply EIGRP with the same autonomous system throughout both networks

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation: Without filters there is possibility of routing loops. Link: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a008009487e.shtml

QUESTION 43

When considering the enterprise campus design, which network application category most influences the network design?

- A. peer-to-peer
- B. client-local server
- C. client-enterprise edge server
- D. client-server farm

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: There should be considerations about traffic flow between client and servers.

Link:

[http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/Borderless_Campus_Network_1.0 / BN_Campus_Models.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/Borderless_Campus_Network_1.0/BN_Campus_Models.html)

QUESTION 44

Which two link state routing protocols support IPv6 routing? (Choose two)

- A. BGP4+
- B. OSPF
- C. RIPng
- D. EIGRP
- E. IS-IS

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation: only OSPF & IS-IS are LSPs which support IPv6.

Link:

http://www.cisco.com/en/US/partner/products/ps10591/products_installation_and_configuration_guides_list.html

QUESTION 45

When designing the wireless portion of an enterprise campus network, which one of these statements should serve as a strict guideline?

- A. Wireless controllers should be distributed throughout the building distribution layers
- B. Dynamic controller redundancy, where the access points attempt to join the least loaded controller, is a best-practice approach.
- C. Wireless controllers should be centralized in the core layer
- D. To improve the RF coverage, the controllers of any building should be put in the same mobility group.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 46

When designing using the Cisco Enterprise Architecture, in which Enterprise Campus layer does the remote Access and VPN module establish its connection?

- A. Building Access
- B. Campus Core
- C. Enterprise Branch
- D. Enterprise Data Center

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: All the modules must end up in the core for optimized routing & switching across the network modules.

Link:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/Borderless_Campus_Network_1.0/BN_Campus_Technologies.html

QUESTION 47

Which one of these statements is an example of how trust and identity management solutions should be deployed in the enterprise campus network?

- A. Authentication validation should be deployed as close to the data center as possible.
- B. Use the principle of top-down privilege, which means that each subject should have the privileges that are necessary to perform their defined tasks, as well as all the tasks for those roles below them.
- C. Mixed ACL rules, using combinations of specific sources and destinations, should be applied as close to the source as possible.
- D. For ease of management, practice defense in isolation security mechanisms should be in place one time, in one place.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Validating user authentication should be implemented as close to the source as possible, with an emphasis on strong authentication for access from untrusted networks. Access rules should enforce policy deployed throughout the network with the following guidelines:

An integral part of identity and access control deployments is to allow only the necessary access. Highly distributed rules allow for greater granularity and scalability but, unfortunately, increase the management complexity. On the other hand, centralized rule deployment eases management but lacks flexibility and scalability.

Practicing "defense in depth" by using security mechanisms that back each other up is an important concept to understand. For example, the perimeter Internet routers should use ACLs to filter packets in addition to the firewall inspecting packets at a deeper level.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 13

QUESTION 48

Which of these is the equation used to derive a 64 Kbps bit rate?

- A. $2 \times 8 \text{ kHz} \times 4\text{-bit code words}$
- B. $8 \text{ kHz} \times 8\text{-bit code words}$
- C. $2 \times 4\text{-bit code words} \times 8 \text{ kHz}$
- D. $2 \times 4 \text{ kHz} \times 8\text{-bit code words}$

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: While the human ear can sense sounds from 20 to 20,000 Hz, and speech encompasses sounds from about 200 to 9000 Hz, the telephone channel was designed to operate at about 300 to 3400 Hz. This economical range carries enough fidelity to allow callers to identify the party at the far end and sense their mood. Nyquist decided to extend the digitization to 4000 Hz, to capture higher-frequency sounds that the telephone channel may deliver. Therefore, the highest frequency for voice is 4000 Hz. According to Nyquist theory, we must double the highest frequency, so $2 \times 4 \text{ kHz} = 8 \text{ kHz}$.

Each sample will be encoded into a 8-bit code. Therefore $8 \text{ kHz} \times 8\text{-bit code} = 64 \text{ Kbps}$ (notice about the unit Kbps: $8 \text{ kHz} = 8000 \text{ samples per second}$ so $8000 \times 8\text{-bit} = 64000 \text{ bit per second} = 64 \text{ Kilobit per second} = 64 \text{ Kbps}$)

Link: <http://encyclopedia2.thefreedictionary.com/Nyquist+theorem> Note:

Nyquist theory:

"When sampling a signal (e.g., converting from an analog signal to digital), the sampling frequency must be greater than twice the bandwidth of the input signal in order to be able to reconstruct the original perfectly from the sampled version."

QUESTION 49

Which one of these statements best describes the challenge of the designer when dealing with IP routing?

- A. OSPF supports fast convergence does not require periodic routing table updates, so the optional network design is best simplified with the network as a single backbone area.
- B. Manual summarization is limited to ABRs and ASBRs, therefore the designer must pay strict attention to the EIGRP topology.
- C. EIGRP, as a proprietary protocol, has special challenges when dealing with networks deployed with IPv6.
- D. Effective scalability with OSPF requires the designer to pay strict attention to the hierarchical network structure, localizing topology changes.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: OSPF demands modular design, multiple areas for functioning optimally. Link: http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.shtml

QUESTION 50

When designing the identity and access control portions for the enterprise campus network, which of these solutions would be the most appropriate solution to consider?

- A. 802.1x
- B. ACLs in the core layer
- C. Cisco Security MARS
- D. NetFlow

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 51

Which three terms describe the primary functions of the distribution layer of the campus network design hierarchy? (Chose three)

- A. provides end-user connectivity
- B. provides high speed transport
- C. provides QoS services
- D. enforces security policies
- E. provides WAN connection
- F. connects access devices to the core backbone

Correct Answer: CDF

Section: (none)

Explanation

Explanation/Reference:

Explanation: D, C, F are properties of distribution layer. Link: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html#wp708979>

QUESTION 52

DataQuirk is a web-based medical transcription company for exotic-animal veterinarians. The company recently added a third ISP for international business. They are organizing the enterprise network into a fully operational Enterprise Edge.

To which two modules will the three ISPs be directly related? (Choose two.)

- A. PSTN
- B. E-commerce
- C. WAN/MAN
- D. Edge Distribution
- E. internet Connectivity
- F. Remote Access VPN

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation: The purpose of ISP link is for serving customers & it is also providing internet connectivity to internal & external users, thus it falls into above 2 categories.

Link: http://leaman.org/ccna4/Chap_1.pdf

QUESTION 53

DRAG DROP

Drag the network function on the left to the functional area or module where it is most likely to be performed in the enterprise campus infrastructure on the right.

aggregates connectivity to voice, video, and data outside the enterprise with QoS and security	Enterprise Campus
provides internal users with external HTTP, FTP, SMTP, and DNS connectivity	Enterprise Edge
enables service-oriented architectures, virtualization, and secure computing with load balancing, redundancy	E-Commerce
enables intelligent route and switch, high availability resilient multilayer design and integrated security	Internet Connectivity
supports application traffic through the Internet, initiated outside the enterprise network	Remote Access and VPN
terminates traffic that is forwarded by the Internet connectivity module	Data Center

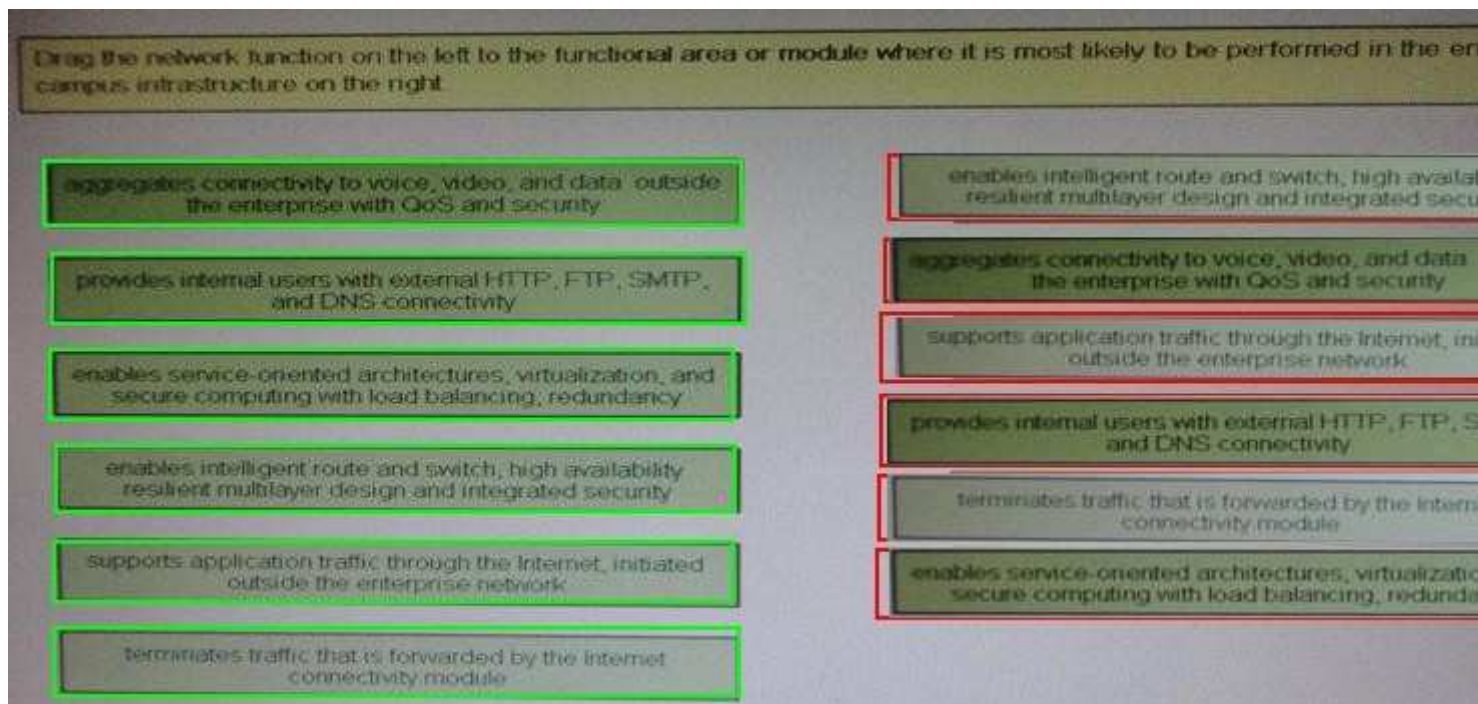
- A.
- B.
- C.
- D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:



Explanation: 1 Enterprise Edge

2 Internet Connectivity

3 Data Center

4 Enterprise Campus

5 E-Commerce

6 Remote Access and VPN

please refer to link.

Link: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html#wp708979> CCDA Study

Guide: Diane Teare

QUESTION 54

Which codec does Cisco recommend for WAN link?

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

Correct Answer: D

Section: (none)

Explanation

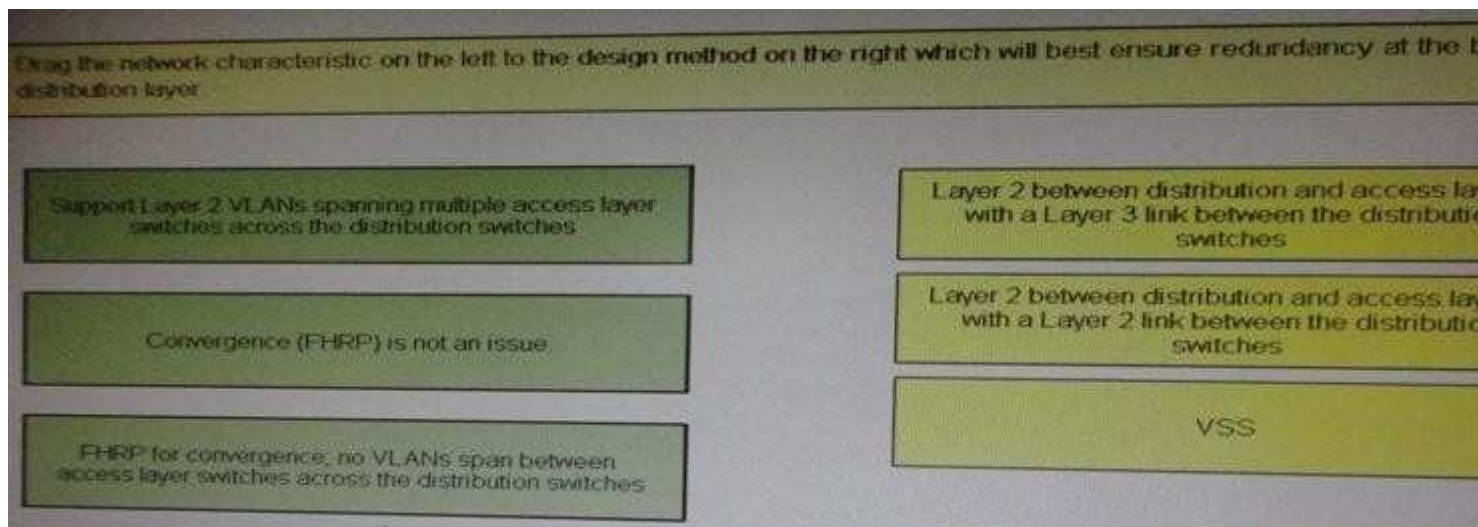
Explanation/Reference:

Explanation: When bandwidth is abundantly available, as in a LAN environment, the Cisco IP phone default G.711 is used in RTP. When bandwidth is at a premium, as on a slow WAN link, G.729 is used.

Link: http://www.globalknowledge.fr/PDF/WP_UnifiedComm.pdf

QUESTION 55

DRAG DROP



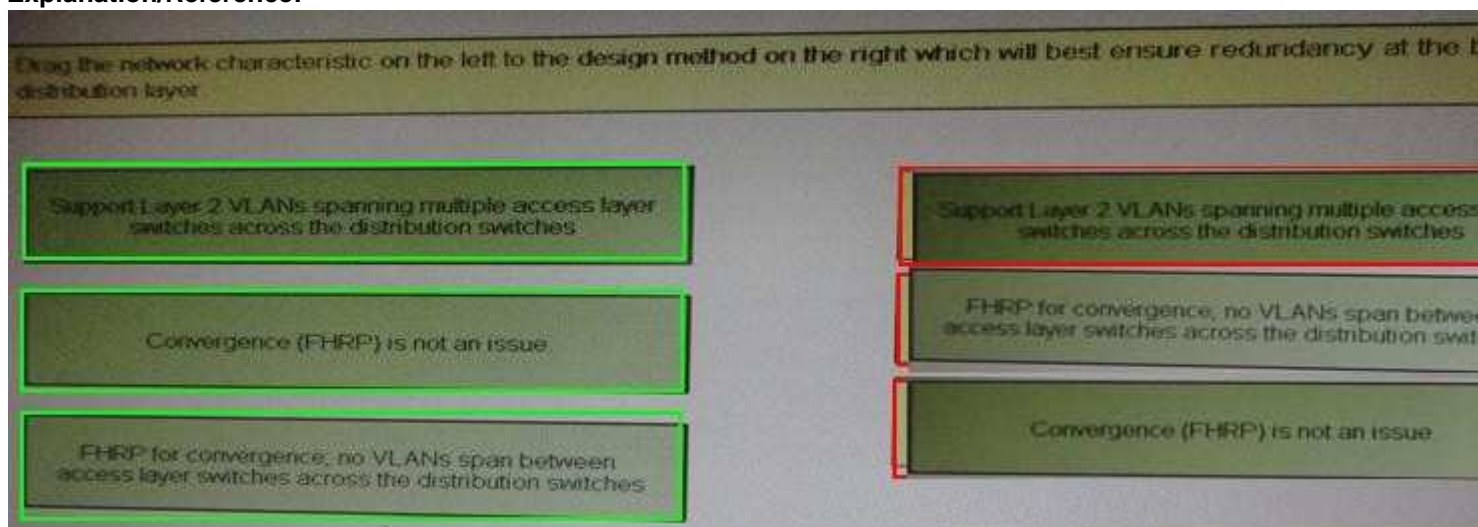
- A.
- B.
- C.
- D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:



Explanation: Correct Answer

Layer 2 between distribution and access layers, with a Layer 3 link between the distribution switches

-> Support Layer 2 VLANs spanning multiple access layer switches across the distribution switches

Layer 2 between distribution and access layers, with a Layer 2 link between the distribution switches

-> FHRP for convergence, no VLANs span between access layer switches across the distribution switches

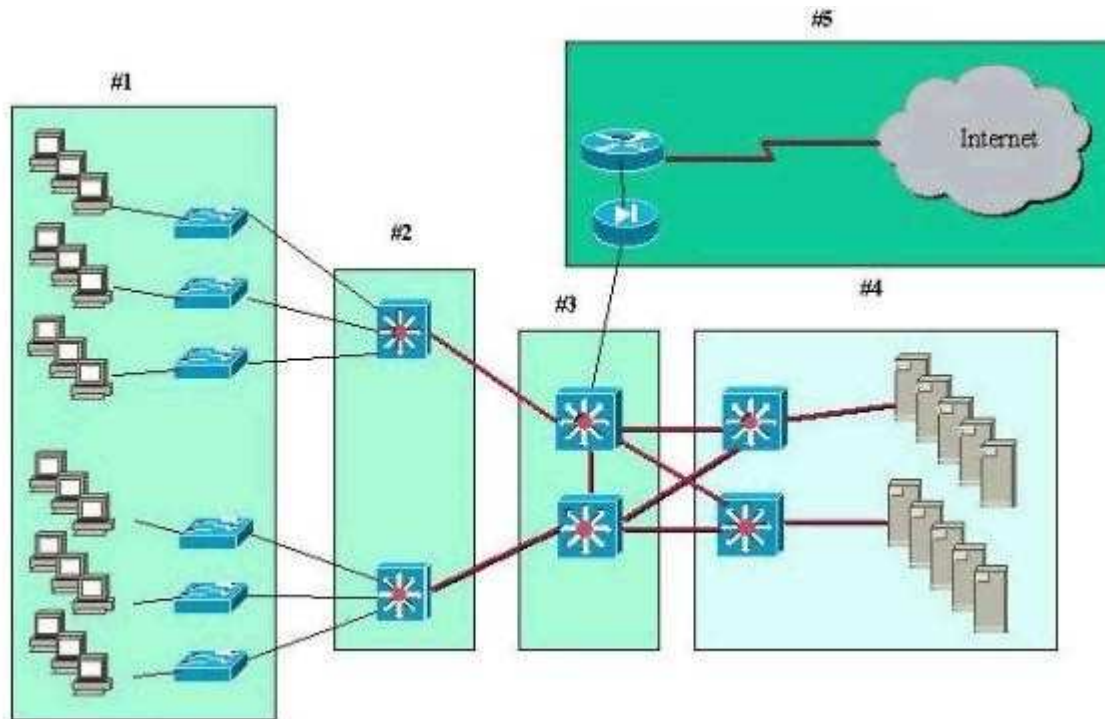
VSS -> Convergence (FHRP) is not an issue

The following are recommended best practices at the distribution layer:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 3

QUESTION 56

Refer to the exhibit.



A standard, Layer 2 campus network design is pictured. Which numbered box represents the distribution layer?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: #1 Access

#2 Distribution

#3 Core

#4 Server Farm / Data Center

#5 WAN Module

#1 is the access layer, since it interfaces directly with the clients #3 is the core layer, since these switches have a direct connection (highest resiliency) and they interface directly with the WAN module

#4 is the datacenter layer, because it interfaces directly with the campus servers #5 is the WAN module, it interfaces with the internet

QUESTION 57

Which codec does Cisco recommend for WAN links?

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

Correct Answer: D

Section: (none)

Explanation

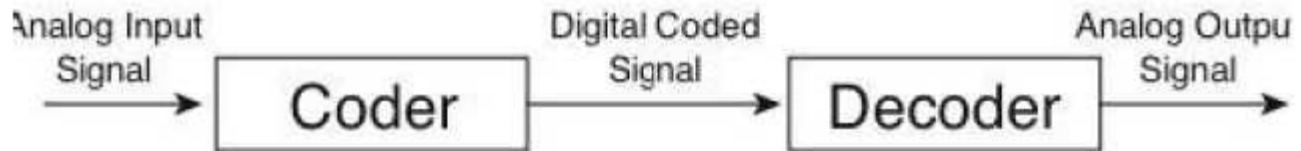
Explanation/Reference:

Explanation: Explanation

Codec Standards

Codecs transform analog signals into a digital bit stream and digital signals back into analog signals. Figure 14-14 shows that an analog signal is digitized with a coder for digital transport. The decoder converts the digital signal into analog form.

Figure 14-14. Codec



Each codec provides a certain quality of speech. Each codec provides a certain level of fidelity to the original audio, or quality of speech. The term mean opinion score (MOS) is used to rate the fidelity for a codec. A MOS score is not a scientific measure. Instead, it is a rating determined by sampling the output to a large group of listeners who judge the audio fidelity from 1 (bad) to 5 (best). The scores are then averaged to provide the MOS for each codec. For example, the established MOS score for G.711 is 4.1, and G.729 is 3.92. The default codec setting for VoIP dial peers in Cisco IOS software is G.729 (g729r8), but this can be configured with several other options, including G.711. Other codec standards are shown in Table 14-8. An explanation of the compression techniques is beyond the scope of the CCDA test.

Table. Codec Standards

Codec Standards			
Codec	Bit Rate	MOS	Description
G.711u	64 kbps	4.1	PCM. u-law (Mu-law) version used in North America and Japan. Samples speech 8000 times per second, represented in 8 bits.
G.711a	64 kbps	4.1	PCM. A-law used in Europe and international routes.
G.726	16/24/32/40 kbps	3.85	Adaptive Differential Pulse-Code Modulation (AD-PCM).
G.728	16 kbps	3.61	Low-Delay CELP (LDCELP).
G.729	8 kbps	3.92	Conjugate Structure ACELP (CS-ACELP).
G.723.1	6.3 kbps	3.9	Multipulse Excitation–Maximum Likelihood Quantization (MPE-MLQ).
G.723.1	5.3 kbps	3.65	Algebraic Code–Excited Linear Prediction (ACELP).

QUESTION 58

When considering the three VoIP design models: single site, centralized multisite, and distributed multisite, which question below would help to eliminate one of the options?

- A. Will the switches be required to provide inline power?
- B. Will users need to make offsite calls, beyond the enterprise?
- C. Will users require applications such as voice mail and interactive voice response?
- D. Are there users whose only enterprise access is via a QoS-enabled WAN?

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 59

The enterprise campus core layer has requirements that are unique from the distribution and access layers. Which of the following is true about the core layer?

- A. The core layer provides convergence using Layer 2 and Layer 3 services and features.
- B. The core layer provides high availability to support the distribution layer connections to the enterprise edge.
- C. The campus core layer is optional.
- D. The core layer requires high performance to manage the traffic policing across the backbone.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 60

Refer to the exhibit.

Exhibit Missing

Which statement is true concerning enterprise edge distribution switches?

- A. The speed of switching is the most critical feature.
- B. Security requirements are offloaded to the other modules for performance reasons.
- C. Edge distribution switches are only required when using a collapsed core backbone.
- D. Enterprise edge distribution switches are similar to the building distribution layer.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 61

Which one of these statements is true concerning the data center distribution (aggregation) layer design?

- A. With Layer 3 at the aggregation layer, the physical loops in the topology must still be managed by STP.
- B. The boundary between Layer 2 and Layer 3 must reside in the multilayer switches, independent of any other devices such as firewalls or content switching devices.
- C. A mix of both Layer 2 and Layer 3 access is sometimes the most optimal.
- D. In a small data center, the aggregation layer can connect directly to the campus core, exchanging IP routes and MAC address tables.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 62

When designing the threat detection and mitigation portion for the enterprise data center network, which of the following would be the most appropriate solution to consider?

- A. 802.1X
- B. ACLs in the core layer
- C. Cisco Security MARS
- D. Cisco Firewall Services Module

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Topic 2, Exam Set A

QUESTION 63

A Cisco Self-Defending Network has been installed, but DoS attacks are still being directed at e-commerce hosts. The connection rate at the Internet firewall was limited, but the problem persists. What more can be done?

- A. Move the servers to the DMZ.
- B. Install all relevant operating system patches.
- C. Block the servers' TCP traffic at the Internet firewall.
- D. Block the servers' UDP traffic at the Internet firewall.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 64

RST Corporation is planning to upgrade its current network. The chief technology officer has supplied a topology diagram and an IP addressing scheme of the current network during an interview.

RST has been growing at about twenty percent per year. It has been difficult to maintain customer support at a satisfactory level. Therefore, the RST board has met with and directed the chief technology officer to look into

network improvements.

Which two items are most relevant in documenting RST's business requirements? (Choose two.)

- A. existing network topologies
- B. network performance requirements
- C. the IP addresses assigned by the ISP
- D. improved customer support requirements
- E. projected growth estimates

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 65

Which two of these best describe the implementation of a WAN Backup design over the Internet? (Choose two.)

- A. a best-effort method
- B. bandwidth guaranteed based on interface configuration
- C. designed as an alternative to a failed WAN connection
- D. implemented with a point-to-point logical link using a Layer 2 tunnel
- E. requires no ISP coordination or involvement

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 66

Which two design criteria require VLANs in a proposed solution? (Choose two.)

- A. the segmenting of collision domains
- B. a limited corporate budget
- C. the use of multivendor equipment
- D. security between departments
- E. video streaming on the LAN
- F. the segmenting of broadcast domains

Correct Answer: DF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 67

Which two methods are used to enhance VPN performance on Cisco ISRs? (Choose two.)

- A. SSL Acceleration Network Module

- B. VPN Shared Port Adapter
- C. VPN Acceleration Module
- D. high-performance VPN encryption AIM
- E. VPN Service Adapter
- F. built-in hardware-based encryption acceleration

Correct Answer: DF

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

ISR G2 Security Hardware Options

The Cisco G2 ISRs have additional hardware options that enhance the routers' security capabilities. Here are some of the available hardware options:

Note

For a complete ISR G2 series comparison, go to www.cisco.com/en/US/products/ps10536/prod_series_comparison.html.

QUESTION 68

Which three factors best justify WAN link redundancy between geographically dispersed sites? (Choose three.)

- A. high expense of transmitting data
- B. important traffic flows
- C. excessive packet transmission rate
- D. uncertain reliability
- E. high link utilization
- F. lack of speed

Correct Answer: BDF

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

WAN Backup Design

Redundancy is critical in WAN design for the remote site because of the unreliable nature of WAN links, when compared to LANs that they connect. Most enterprise edge solutions require high availability between the primary and remote site. Because WAN links have lower reliability and lack bandwidth, they are good candidates for most WAN backup designs.

Branch offices should have some type of backup strategy in the event of a primary link failure. Backup links can be either dialup, permanent WAN, or Internet-based connections. WAN backup options are as follows:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 7

QUESTION 69

Which three pieces of information should be documented for each step of each phase in a design implementation plan? (Choose three.)

- A. easy guidelines in case of failure

- B. estimated rollback time in case of failure
- C. simple implementation guidelines
- D. estimated implementation time
- E. design document references
- F. step description

Correct Answer: DEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The implementation of a network consists of several phases. The each step should contain the following information:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 1

QUESTION 70

The topology map in the draft design document should cover which two layers of the OSI model? (Choose two.)

- A. session
- B. data link
- C. transport
- D. application
- E. physical
- F. network

Correct Answer: EF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 71

In a Cisco CatOS switch, what is the recommended practice when configuring switch-to-switch intercommunications to carry multiple VLANs for Dynamic Trunk Protocol?

- A. auto to auto_negotiate
- B. disable Dynamic Trunk Protocol when operating in the distribution layer
- C. auto to auto_no_negotiate
- D. desirable to desirable_no_negotiate
- E. on to on_negotiate
- F. desirable to desirable_negotiate

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Explanation

Explanation

Access Layer Best Practices

When designing the building access layer, you must consider the number of users or ports required to size up

the LAN switch. Connectivity speed for each host should also be considered. Hosts might be connected using various technologies such as Fast Ethernet, Gigabit Ethernet, or port channels. The planned VLANs enter into the design.

Performance in the access layer is also important. Redundancy and QoS features should be considered. The following are recommended best practices for the building access layer:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 3

QUESTION 72

What are the two most likely driving forces motivating businesses to integrate voice and data into converged networks? (Choose two.)

- A. Voice networks cannot carry data unless the PRI circuits aggregate the BRI circuits.
- B. Their PSTNs cannot deploy features quickly enough.
- C. Data, voice, and video cannot converge on their current PSTN structures.
- D. Voice has become the primary traffic on networks.
- E. WAN costs can be reduced by migrating to converged networks.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

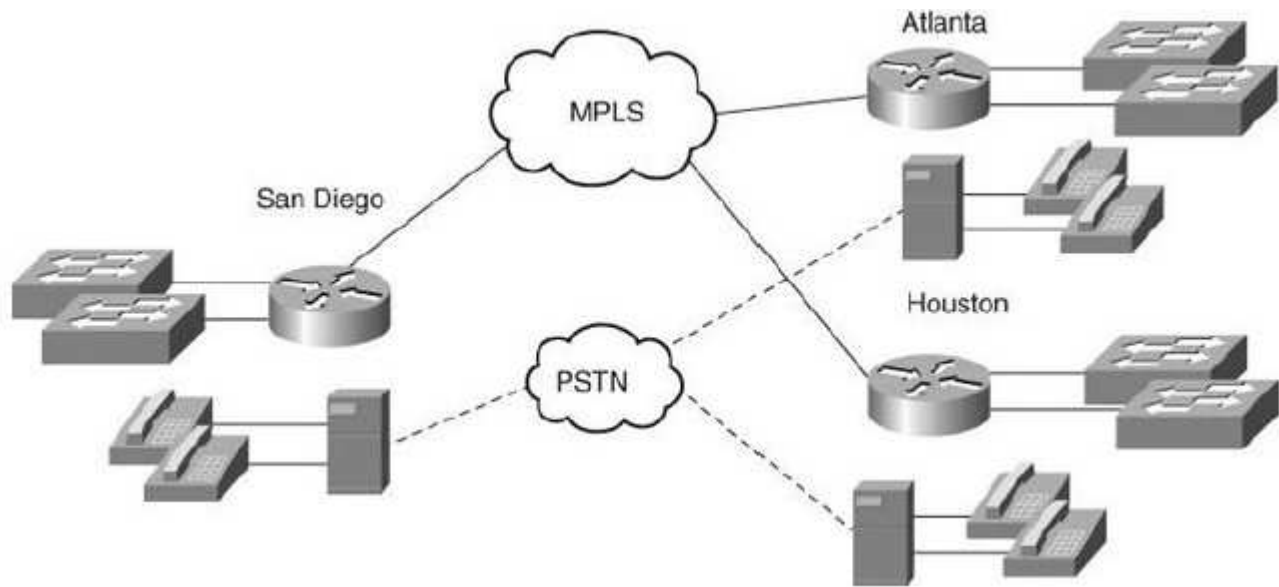
VoIP

VoIP provides transport of voice over the IP protocol family. IP makes voice globally available regardless of the data-link protocol in use (Ethernet, ATM, Frame Relay). With VoIP, enterprises do not have to build separate voice and data networks. Integrating voice and data into a single converged network eliminates duplicate infrastructure, management, and costs.

Figure 14-7 shows a company that has separate voice and data networks. Phones connect to local PBXs, and the PBXs are connected using TDM trunks. Off-net calls are routed to the PSTN. The data network uses LAN switches connected to WAN routers. The WAN for data uses Frame Relay. Separate operations and management systems are required for these networks. Each system has its corresponding monthly WAN charges and personnel, resulting in additional costs.

With separate voice and data networks,

Figure 14-7 Separate Voice and Data Networks



Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 14

QUESTION 73

A lightweight access point is added to a working network. Which sequence will it use to associate itself with a wireless LAN controller?

- A. primary, secondary, tertiary, greatest AP capacity, master
- B. primary, secondary, tertiary, master, greatest AP capacity
- C. master, primary, secondary, tertiary, greatest AP capacity
- D. greatest AP capacity, primary, secondary, tertiary, master

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Table. WLAN Controller Platforms

Order	WLC
First	Primary <u>sysName</u> (preconfigured)
Second	Second <u>sysName</u> (preconfigured)
Third	Tertiary <u>sysName</u> (preconfigured)
Fourth	Master controller
Fifth	WLC with <u>greatest capacity</u> for AP associations

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 5

QUESTION 74

Which three mechanisms are required to deploy QoS on an IP WAN? (Choose three.)

- A. queuing and scheduling
- B. Call Admission Control

- C. traffic shaping
- D. link efficiency techniques
- E. traffic classification
- F. bandwidth provisioning

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Queuing, Traffic Shaping, and Policing

Cisco has developed many different QoS mechanisms, such as queuing, policing, and traffic shaping, to enable network operators to manage and prioritize the traffic flowing on the network. Applications that are delay sensitive, such as VoIP, require special treatment to ensure proper application functionality. Queuing refers to the buffering process used by routers and switching when they receive traffic faster than can be transmitted. Different queuing mechanisms can be implemented to influence the order in which the different queues are serviced (that is, how different types of traffic are emptied from the queues). Table 6-6 identifies QoS considerations to optimize bandwidth.

QoS Category	Description
Classification	Identifies and marks flow and provides priority to certain flows
Congestion management	Mechanism to handle traffic overflow using a queuing algorithm
Link-efficiency mechanisms	Reduce latency and jitter for network traffic on low-speed links
Traffic shaping and policing	Avoids congestion by policing ingress and egress flows

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 6

QUESTION 75

Which two statements best describe the implementation of Overlay VPN connectivity for remote access in the Enterprise Edge WAN module? (Choose two.)

- A. Bandwidth is provisioned on a site-to-site basis.
- B. It uses dedicated point-to-point links.
- C. Optimum routing between customer sites requires a full mesh of virtual circuits.
- D. It must use Layer 2 labels to forward packets
- E. The ISP actively participates in customer routing.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Network-Layer VPNs

The network layer in the TCP/IP protocol suite consists of the IP routing system--how reachability information is conveyed from one point in the network to another. There are a few methods to construct VPNs within the network layer; each is examined in the following paragraphs. A brief overview of non-IP VPNs is provided in Part II of this article. A brief overview of the differences in the "peer" and "overlay" VPN models is appropriate at this point. Simply put, the "peer" VPN model is one in which the network-layer forwarding path computation is done on a hop-by-hop basis, where each node in the intermediate data transit path is a peer with a next-hop node. Traditional routed networks are examples of peer models, where each router in the network path is a peer with its next-hop adjacencies. Alternatively, the "overlay" VPN model is one in which the network-layer

forwarding path is not done on a hop-by-hop basis, but rather, the intermediate link-layer network is used as a "cut-through" to another edge node on the other side of a large cloud. Examples of "overlay" VPN models include ATM, Frame Relay, and tunneling implementations. Having drawn these simple distinctions between the peer and overlay models, it should be noted that the overlay model introduces some serious scaling concerns in cases where large numbers of egress peers are required because the number of adjacencies increases in direct proportion to the number of peers--the amount of computational and performance overhead required to maintain routing state, adjacency information, and other detailed packet forwarding and routing information for each peer becomes a liability in very large networks. If all the egress nodes in a cut-through network become peers in an effort to make all egress nodes one "Layer 3" hop away from one another, the scalability of the VPN overlay model is limited quite remarkably.

The Internet Protocol Journal - Volume 1, No. 1
What Is a VPN? - Part I

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/what_is_a_vpn.html

QUESTION 76

DRAG DROP

Drop

Click and drag the QoS feature type on the left to the category of QoS mechanism on the right

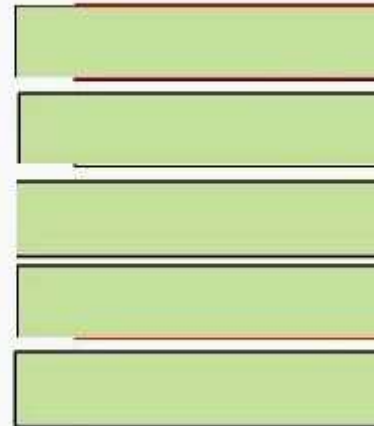
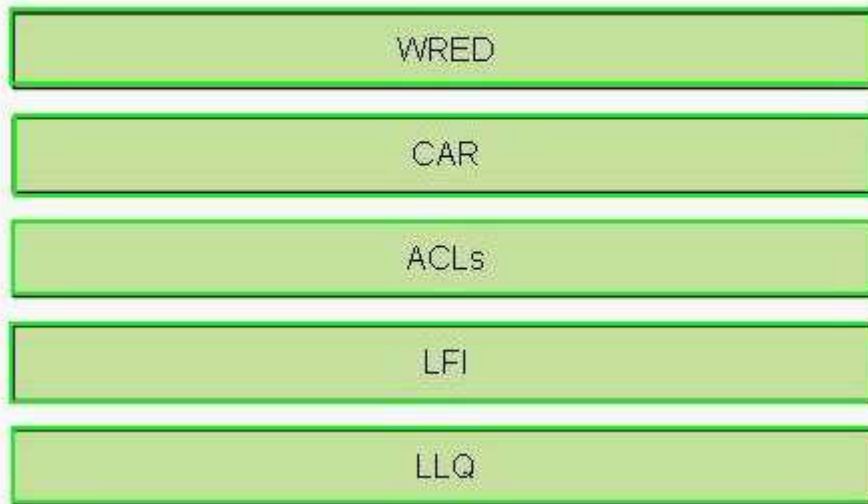
WRED	classification
CAR	congestion
ACLs	traffic
LFI	congestion
LLQ	liability

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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

Click and drag the QoS feature type on the left to the category of QoS mechanism on the right



Explanation:

- + classification and marking: ACLs
- + congestion avoidance: WRED
- + traffic conditioners: CAR
- + congestion management: LLQ
- + link efficiency: LFI

Explanation

Classification is the process of partitioning traffic into multiple priority levels or classes of service. Information in the frame or packet header is inspected, and the frame's priority is determined. Marking is the process of changing the priority or class of service (CoS) setting within a frame or packet to indicate its classification. Classification is usually performed with access control lists (ACL), QoS class maps, or route maps, using various match criteria.

Congestion-avoidance techniques monitor network traffic loads so that congestion can be anticipated and avoided before it becomes problematic. Congestion-avoidance techniques allow packets from streams identified as being eligible for early discard (those with lower priority) to be dropped when the queue is getting full. Congestion avoidance techniques provide preferential treatment for high priority traffic under congestion situations while maximizing network throughput and capacity utilization and minimizing packet loss and delay.

Weighted random early detection (WRED) is the Cisco implementation of the random early detection (RED) mechanism. WRED extends RED by using the IP Precedence bits in the IP packet header to determine which traffic should be dropped; the drop-selection process is weighted by the IP precedence.

Traffic conditioner consists of policing and shaping. Policing either discards the packet or modifies some aspect of it, such as its IP Precedence or CoS bits, when the policing agent determines that the packet meets a given criterion. In comparison, traffic shaping attempts to adjust the transmission rate of packets that match a certain criterion. Shaper typically delays excess traffic by using a buffer or queuing mechanism to hold packets and shape the flow when the source's data rate is higher than expected. For example, generic traffic shaping uses a weighted fair queue to delay packets to shape the flow. Traffic conditioner is also referred to as Committed Access Rate (CAR).

Congestion management includes two separate processes: queuing, which separates traffic into various queues or buffers, and scheduling, which decides from which queue traffic is to be sent next. There are two types of queues: the hardware queue (also called the transmit queue or TxQ) and software queues. Software queues schedule packets into the hardware queue based on the QoS requirements and include the following types: weighted fair queuing (WFQ), priority queuing (PQ), custom queuing (CQ), class-based WFQ (CBWFQ), and

low latency queuing (LLQ).

LLQ is also known as Priority Queuing. Class-Based Weighted Fair Queuing (PQ-CBWFQ). LLQ provides a single priority but it's preferred for VoIP networks because it can also configure guaranteed bandwidth for different classes of traffic queue. For example, all voice call traffic would be assigned to the priority queue, VoIP signaling and video would be assigned to a traffic class, FTP traffic would be assigned to a low-priority traffic class, and all other traffic would be assigned to a regular class.

Link efficiency techniques, including link fragmentation and interleaving (LFI) and compression. LFI prevents small voice packets from being queued behind large data packets, which could lead to unacceptable delays on low-speed links. With LFI, the voice gateway fragments large packets into smaller equal-sized frames and interleaves them with small voice packets so that a voice packet does not have to wait until the entire large data packet is sent. LFI reduces and ensures a more predictable voice delay.

(Reference: Cisco Press Designing for Cisco Internetwork Solutions)

QUESTION 77

A manufacturing company has decided to add a website to enhance sales. The web servers in the E-Commerce module must be accessible without compromising network security. Which two design recommendations can be made to meet these requirements? (Choose two.)

- A. Move the E-Commerce servers to the WAN module.
- B. Use intrusion detection on the E-Commerce server farm.
- C. Limit the number of incoming connections to the E-Commerce module.
- D. Use private and public key encryption.
- E. Place E-Commerce servers and application servers on isolated LANs (DMZs).

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 78

After a period of rapid growth, FloCzar Boats is seeking better network management tools. Managers have developed this needs list:

Move from static to dynamic device information.

Gain information to assist in long-term trend analysis.

Concentrate on Layer 4 monitoring.

Which management protocol will most help FloCzar achieve its goals?

- A. RMON2
- B. SNMP
- C. NetFlow
- D. RMON
- E. Cisco Discovery Protocol

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation
RMON2

RMON1 is focused on the data link and physical layers of the OSI model. As shown in Figure 15- 4, RMON2 provides an extension for monitoring upper-layer protocols.

Figure. RMON1 and RMON2 Compared to the OSI Model

Defined by RFC 2021, RMON2 extends the RMON group with the MIB groups listed in the following Table

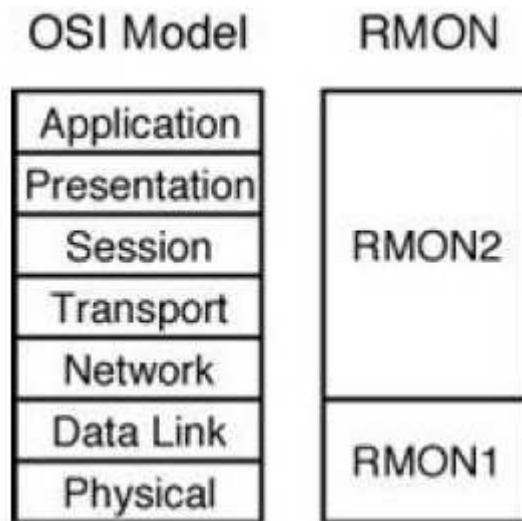


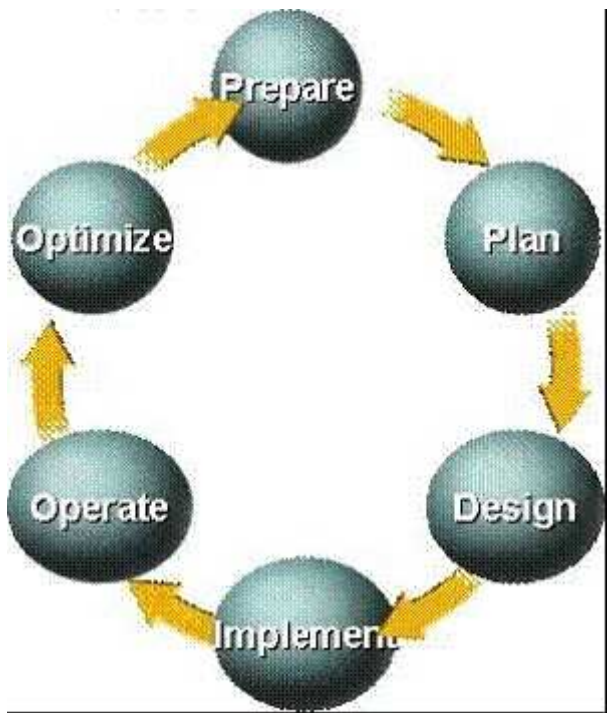
Table. RMON2 Groups

ID	Name	Description
11	Protocol Directory	Lists the protocols the device supports
12	Protocol Distribution	Traffic statistics for each protocol
13	Address Mapping	Contains network-to-MAC layer address mapping (IP to MAC)
14	Network Layer Host	Contains statistics for traffic sent to or from network layer hosts
15	Network Layer Matrix	Contains statistics for conversations between two network layer hosts
16	Application Layer Host	Contains application layer statistics for traffic sent to or from each host
17	Application Layer Matrix	Contains application layer statistics for conversations between pairs of hosts
18	User History	Contains periodic samples of specified variables
19	Probe Configuration	Probes parameter configuration

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 15

QUESTION 79

At which stage in the PPDIOO process would you analyze a customer's network in order to discover opportunities for network improvement?



- A. Operate
- B. Implement
- C. Plan
- D. Design
- E. Prepare
- F. Design Assessment

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Design phase: Developing a detailed design is essential to reducing risk, delays, and the total cost of network deployments. A design aligned with business goals and technical requirements can improve network performance while supporting high availability, reliability, security, and scalability.

(Reference: <http://www.ciscozine.com/2009/01/29/the-ppdioo-network-lifecycle/>)

QUESTION 80

A very large organization has received its IPv6 address range from its Internet Service Provider and intends to use only IPv6 addresses internally. Employees will access the Internet using port address translation. What is a requirement for their DNS servers?

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

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 81

Which two statements represent advantages that the top-down network design process has over the bottom-up network design process? (Choose two.)

- A. utilizes previous experience
- B. identifies appropriate technologies first
- C. is able to provide the big picture
- D. takes less time to design a network
- E. provides a design for current and future development

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation: Explanation



<http://www.gratisexam.com/>

By incorporating the organization's requirements, the top-down network design process provide the big picture that meets current and future requirements.

QUESTION 82

Which two statements about IPv6 addresses are true? (Choose two.)

- A. Two colons (::) are used to represent successive hexadecimal fields of zeros.
- B. Leading zeros are required.
- C. Two colons (::) are used to separate fields.
- D. A single interface will have multiple IPv6 addresses of different types.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 83

Which three security measures can be used to mitigate DoS attacks that are directed at exposed hosts within the E-Commerce module? (Choose three.)

- A. Use NIDSs and HIPSs to detect signs of attack and to identify potentially successful breaches.
- B. Partition the exposed hosts into a separate LAN or VLAN.
- C. Use LAN switch VTP pruning to separate hosts on the same segment.

- D. Use a VPN concentrator (IPSec) to protect and verify each connection to the exposed host or hosts.
- E. Use firewalls to block all unnecessary connections to the exposed hosts.

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 84

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

- A. VSANs
- B. VPDNs
- C. VLANs
- D. GRE
- E. IPsec

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

IPsec - A security architecture that operates in a host to protect IP traffic. The IETF defined IPsec in RFC 4301. IPsec uses open standards and provides secure communication between peers to ensure data confidentiality, integrity, and authentication through network layer encryption.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition

QUESTION 85

Which statement best describes Call Admission Control?

- A. It extends QoS capabilities to protect voice from excessive data traffic.
- B. It protects voice from voice.
- C. It provides endpoint registration control.
- D. It provides endpoint bandwidth control.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

CAC should be used to keep excess voice traffic from the network by ensuring that there is enough bandwidth for new calls. Call admission control (CAC) is used to control the number of calls to reduce the WAN bandwidth for a site that has IPT. CAC is configured for the site on the CUCM servers. A maximum bandwidth or maximum number of calls is provisioned for the site. CAC enforces a maximum number of calls between two locations to ensure that call quality will not be degraded by allowing more calls than a network can support. CAC causes excessive calls between two locations to be refused. The IPT system must then either reroute the call to different available path, such as the PSTN, or deny the call.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 14

QUESTION 86

A customer wishes to implement VoIP using centralized call-processing. In addition, the customer wishes to ice quality and good bandwidth utilization. Which codec would you suggest?

- A. G.711
- B. G.729
- C. G.726
- D. G.723.1

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 87

DRAG DROP

Drop

Click and drag the Cisco Self-Defending Network term on the left to the SDN description on the right that is used.

Threat Defense

provides secure n
controls infected

Secure Remote Access

uses encryption a
secure transport

Cisco Self-Defending Network

uses security integra
appliances to

Secure Connectivity

integrates security
prevent, a

Trust and Identity Management

- A.
- B.
- C.

D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

Click and drag the Cisco Self-Defending Network term on the left to the SDN description on the right.

Threat Defense

Secure Remote Access

Cisco Self-Defending Network

Secure Connectivity

Trust and Identity Management

Trust and Identity Management

Secure Remote Access

Threat Defense

Cisco Self-Defending Network

Explanation:

Trust and Identity Management

Secure Connectivity

Threat Defense

Cisco Self-Defending Network

- + provides secure network access, isolates and controls infected devices attempting access: Trust and Identity Management
- + uses encryption and authentication to provide secure transport across untrusted networks: Secure Connectivity
- + uses security integrated into routers, switches, and appliances to defend against attacks: Threat Defense
- + integrates security into the network to identify, prevent, and adapt to threats: Cisco Self-Defending Network

Explanation

Trust and identity management solutions provide secure network access and admission at any point in the network and isolate and control infected or unpatched devices that attempt to access the network. If you are trusted, you are granted access. We can understand "trust" is the security policy applied on two or more network entities and allows them to communicate or not in a specific circumstance. "Identity" is the "who" of a trust relationship.

The main purpose of Secure Connectivity is to protect the integrity and privacy of the information and it is mostly done by encryption and authentication. The purpose of encryption is to guarantee confidentiality; only authorized entities can encrypt and decrypt data. Authentication is used to establish the subject's identity. For example, the users are required to provide username and password to access a resource...

QUESTION 88

Which three sources does a network designer use to collect information for characterizing an existing network? (Choose three.)

- A. server statistics
- B. network audit
- C. traffic analysis
- D. visual inventory
- E. staff input

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Explanation

Characterizing the Existing Network

Characterizing the network is Step 2 of the design methodology. In this section, you learn to identify a network's major features, tools to analyze existing network traffic, and tools for auditing and monitoring network traffic.

Steps in Gathering Information

When arriving at a site that has an existing network, you need to obtain all the existing documentation.

Sometimes no documented information exists. You should be prepared to use tools to obtain information and get access to log in to the network devices to obtain information.

Here are the steps for gathering information:

When gathering existing documentation, you look for site information such as site names, site addresses, site contacts, site hours of operation, and building and room access. Network infrastructure information includes locations and types of servers and network devices, data center and closet locations, LAN wiring, WAN technologies and circuit speeds, and power used. Logical network information includes IP addressing, routing protocols, network management, and security access lists used. You need to find out whether voice or video is being used on the network.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 1

QUESTION 89

Which of the following Cisco router services performs network traffic analysis to assist in documenting a customer's existing network?

- A. NetMon
- B. MRTG
- C. SNMP MIB compiler
- D. NetFlow

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 90

Which statement identifies a benefit obtained when using a top-down network design plan?

- A. provides a more detailed picture of the desired network
- B. facilitates design based on previous experience
- C. is less time-consuming than using a bottom-up approach
- D. allows quick responses to design requests
- E. incorporates customer organizational requirements

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

The top-down approach begins with the organization's requirements before looking at technologies. Network designs are tested using a pilot or prototype network before moving into the Implement phase.

QUESTION 91

Lightweight access points are being deployed in remote locations where others are already operational. The new access points are in a separate IP subnet from the wireless controller. OTAP has not been enabled at any locations. Which two methods can the AP use to locate a wireless controller? (Choose two.)

- A. NV-RAM IP address
- B. master
- C. primary, secondary, tertiary
- D. DHCP
- E. local subnet broadcast
- F. DNS

Correct Answer: DF

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Over-the-Air-Provisioning (OTAP) Process

During the LAP boot process, the LAP uses different mechanisms in order to discover controllers that it can join. The LAP keeps each of the controller that IP addresses it learned through the different methods in different lists in order to reflect how the LAP learned about them. For example, the LAP can learn management IP addresses of multiple controllers through the DNS entry for CISCO-LWAPP-CONTROLLER.localdomain, DHCP option 43, through broadcasts on the local subnet, locally stored controller IP address discovery, and

through OTAP. Once the access point has completed the LWAPP WLC Discovery steps, it chooses a WLC from the candidate WLC list and sends that WLC an LWAPP Join Request.

Cisco 4400 series Wireless LAN Controllers
Understanding Over-the-Air-Provisioning (OTAP)
Document ID: 100516

QUESTION 92

Which Cisco security solution can quarantine and prevent non-compliant end stations from accessing the network until they achieve security policy compliance?

- A. Cisco Security Monitoring, Analysis, and Response System
- B. Adaptive Security Appliance
- C. Network Admission Control
- D. Network Intrusion Prevention System
- E. Cisco Secure Connectivity
- F. Access Control Server

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

The Network Admission Control protects the network from threats by enforcing security compliance on all devices attempting to access the network. It only allows access to endpoints only after they have passed authentication based on security policies.

QUESTION 93

A network design includes private addressing, but there is also a need for two or three network devices to each be assigned a unique public address so they can be accessed from the Internet. Which technique will satisfy this requirement?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

NAT has several forms:

·Static NAT: Maps an unregistered or private IP address to a registered IP address; it is configured manually. It is commonly used to assign a network device with internal private IP address a unique public address so that they can be accessed from the Internet. ·Dynamic NAT: Dynamically maps an unregistered or private IP address to a registered IP address from a pool (group) of registered addresses. The two subsets of dynamic NAT are overloading and overlapping:

oOverloading: Maps multiple unregistered or private IP addresses to a single registered IP address by using different ports. This is also known as PAT, single-address NAT, or port-level multiplexed NAT.

oOverlapping: Maps registered internal IP addresses to outside registered IP addresses It can also map external addresses to internal registered addresses. Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 8

QUESTION 94

A Cisco security mechanism has the following attributes:

it is a sensor appliance

it searches for potential attacks by capturing and analyzing traffic

it is a "purpose-built device"

it is installed passively

it introduces no delay or overhead

Which Cisco security mechanism is this?

- A. NIDS
- B. PIX
- C. IKE
- D. HIPS
- E. HMAC

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Inline IPS and anomaly detection: Cisco has innovated in the area of NIDS by being the first to incorporate NIDS into the IOS on routing and switching platforms. In addition, IPS solutions have inline filtering features that can remove unwanted traffic with programmable features that classify traffic patterns. The Cisco IPS 4200 sensor appliances, Cisco Catalyst 6500 IDS-M-2, and the Cisco IOS IPS can identify, analyze, and stop unwanted traffic from flowing on the network. Another set of tools used to prevent distributed DoS (DDoS) attacks and ensure business continuity is the Cisco Traffic Anomaly Detector XT and Guard XT appliances, along with the Cisco Catalyst 6500 Traffic Anomaly Detector Module and Cisco Anomaly Guard Module.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 13

QUESTION 95

Which two routing protocols operate over NBMA point-to-multipoint networks without the use of point-to-point subinterfaces? (Choose two.)

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

OSPF over NBMA

For OSPF to run over NBMA you are required to implement the neighbor IP Address but not subinterfaces

Configure an Interface as Point-to-Multipoint, Nonbroadcast (Non-Broadcast Multi-access NBMA)

To treat the interface as point-to-multipoint when the media does not support broadcast, perform the following task in interface configuration mode:

Task	Command
Step 1 Configure an interface as point-to-multipoint for nonbroadcast media.	ip ospf network point-to-multipoint non-broadcast
Step 2 Enter global configuration mode.	exit
Step 3 Configure an OSPF routing process and enter router configuration mode.	router ospf process-id
Step 4 Specify an OSPF neighbor and optionally assign a cost to the neighbor.	neighbor ip-address [cost number]
Step 5 Repeat Step 4 for each neighbor.	

http://www.cisco.com/en/US/docs/ios/11_3/feature/guide/ospfpmp.html#wp1960

EIGRP over NBMA

NBMA Interfaces (Frame Relay, X.25, ATM)

It is particularly critical to configure nonbroadcast multi-access (NBMA) interfaces correctly, because otherwise many EIGRP packets may be lost in the switched network. There are three basic rules:

There are three different scenarios for NBMA interfaces. http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094063.shtml#nbma Configuration Commands

```
no ip split-horizon eigrp
no ip next-hop-self eigrp
```

RIP over NBMA

Exchange of Routing Information

RIP is normally a broadcast protocol, and in order for RIP routing updates to reach nonbroadcast networks, you must configure the Cisco IOS software to permit this exchange of routing information.

To control the set of interfaces with which you want to exchange routing updates, you can disable the sending of routing updates on specified interfaces by configuring the passive-interface router configuration command. See the discussion on filtering in the "Filter Routing Information" section in the "Configuring IP Routing Protocol-Independent Features" module.

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP. Optionally, you can limit the offset list with either an access list or an interface. To increase the value of routing metrics, use the following command in router configuration mode:

Routing protocols use several timers that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better suit your internetwork needs. You can make the following timer adjustments:

http://www.cisco.com/en/US/docs/ios/iproute_rip/configuration/guide/irr_cfg_rip_ps6441_TSD_Products_Configuration_Guide_Chapter.html#wp1061185

IS-IS over NBMA

IS-IS can work over an NBMA multipoint network only if the network is configured with a full mesh. Anything less than a full mesh could cause serious connectivity and routing issues. However, even if a full mesh is

configured, this is no guarantee that a full mesh will exist at all times. A failure in the underlying switched WAN network or a misconfiguration on one or more routers could break the full mesh either temporarily or permanently. Therefore, you should avoid NBMA multipoint configurations for IS-IS networks. Use point-to-point subinterfaces instead. <http://www.ciscopress.com/articles/article.asp?p=31319&seqNum=5>

QUESTION 96

Which three types of WAN topologies can be deployed in the Cisco Enterprise Architecture Enterprise Edge WAN module? (Choose three.)

- A. ring
- B. full mesh
- C. partial mesh
- D. collapsed core
- E. star
- F. core
- G. edge

Correct Answer: BCE

Section: (none)

Explanation

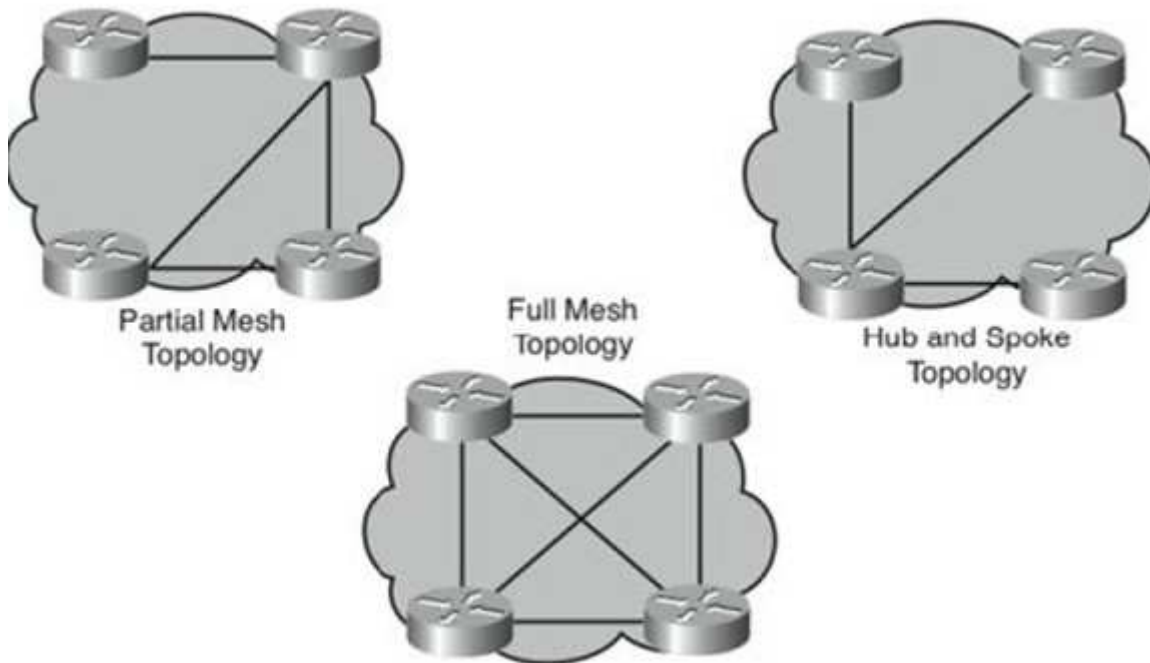
Explanation/Reference:

Explanation: Explanation

Packet and cell switched: Connections that use virtual circuits (PVC/SVC) established by the SP. Packet-switched technologies include Frame Relay and cell-switched technologies such as ATM. ATM uses cells and provides support for multiple quality of service (QoS) classes. The virtual circuits are part of the shared ATM/Frame Relay SP backbone network. This gives the SP greater flexibility with its service offerings.

When planning and designing a packet-switched WAN, you should become familiar with some basic WAN topologies. These WAN topologies include hub-and-spoke, partial-mesh, and full-mesh topologies, as shown in Figure 7-1.

Figure. WAN Topologies



Hub-and-Spoke Topology

A star or hub-and-spoke topology provides a hub router with connections to the spoke routers through the WAN cloud. Network communication between the sites flows through the hub router. Significant WAN cost savings, lower circuit counts, and simplified management are benefits of the hub-and-spoke topology. In addition, hub-and-spoke topologies provide WAN hierarchy and can provide high availability through the use of dual routers at the hub site.

A major disadvantage of this approach is that if you use a single hub router, it can represent a single point of failure. The hub-and-spoke topology can also limit the overall performance when resources are accessed through the central hub router from the spoke routers, such as with spoke-to-spoke network traffic.

Full-Mesh Topology

With full-mesh topologies, each site has a connection to all other sites in the WAN cloud (any-to-any). As the numbers of sites grow, so does the number of spoke connections that are ultimately required. Consequently, the full-mesh topology is not viable in very large networks. However, a key advantage of this topology is that it has plenty of redundancy in the event of network failures. But redundancy implemented with this approach does have a high price associated with it.

Here are some issues inherent with full-mesh topologies:

The number of VCs required for a full mesh can be calculated using the formula $((N - 1) \times N / 2)$. For example if you have 4 sites, $((4 - 1) \times 4 / 2) = 6$ VCs are required.

Partial-Mesh Topology

A partial-mesh topology has fewer VC connections than a full-mesh topology. Therefore, not all sites in the cloud are required to be connected to each other. However, some sites on the WAN cloud have full-mesh characteristics. Partial-mesh topologies can give you more options and flexibility for where to place the high redundancy VCs based on your specific requirements.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 7

QUESTION 97

Which statement accurately describes one difference between a small office and medium office topology?

- A. Medium offices commonly use integrated route and switching platforms.
- B. Medium offices use integrated 10/100/1000 interfaces as Layer 2 trunks.
- C. Medium offices use external access switches to support LAN connectivity.
- D. Small offices commonly use Rapid PVST+ for Layer 3 deployments.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Medium Branch Design

The medium branch design is recommended for branch offices of 50 to 100 users, which is similar to the small branch but with an additional access router in the WAN edge (slightly larger) allowing for redundancy services. Typically, two 2921 or 2951 routers are used to support the WAN, and separate access switches are used to provide LAN connectivity.

The infrastructure components are dual-access routers, external Layer 2 / Layer 3 switches, laptops, desktops, printers, and IP phones. Dual Frame Relay links provide the private WAN services, which are used to connect back to the corporate offices via both of the access routers. Layer 3 protocols such as EIGRP are typically deployed. Because there are two routers, Hot Standby Router Protocol (HSRP) or Gateway Load Balancing Protocol (GLBP) can be used to provide redundancy gateway services. QoS can also be used to provide guaranteed bandwidth for VoIP, and policing can be used to restrict certain traffic classes from overwhelming the available bandwidth. Cisco IOS features such as QoS, access control lists (ACL), and RIP routing capabilities are available in the IP Base feature set, but IP unicast routing and multicast routing require the IP Services feature set.

The medium branch design supports using a higher-density external switch or using the EtherSwitch module with the ISR to create trunks to the external access switches. The Cisco Catalyst 3750 series switches have StackWise technology, allowing multiple switches to be connected and managed as one. This also increases the port density available for end-user connections. With Cisco StackWise technology, customers can create a single, 32-Gbps switching unit that can connect up to nine 3750 series switches using a variety of fiber and copper ports, allowing greater flexibility with the connection options.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 7

QUESTION 98

A customer has the following Enterprise Campus design requirements:

at least 10 Gbps of bandwidth
network runs of up to 40km

no concern for transmission medium cost

Which transmission medium should you recommend to this customer?

- A. unshielded twisted pair
- B. shielded twisted pair
- C. single-mode fiber
- D. wireless
- E. multimode fiber

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation
Below is the comparison of transmission media

Media	Bandwidth	Distance
Twisted pair	Up to 1 Gbps	100 m
Multimode fiber	Up to 1 Gbps	2 km (FE) 550 m (GE)
Single-mode fiber	10 Gbps	90 km (FE) 40 km (GE)
Wireless	54 Mbps (27 Mbps effective)	500 m at 1 Mbps

(Reference from CCDA Official Exam Certification Guide. Some other books have different figures but we should answer it according to the "Official" book)

QUESTION 99

You design a network with the following network addresses:

192.168.168.0

192.168.169.0

192.168.170.0

192.168.171.0

192.168.172.0

192.168.173.0

192.168.174.0

192.168.175.0

Which route address is the best summary of these network addresses?

- A. 192.168.0.0/16
- B. 192.168.168.0/21
- C. 192.168.0.0/24
- D. 192.168.171.128/3
- E. 192.168.175.0/3
- F. None of the above

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Route Summarization is called route aggregation. Route aggregation creates one route in the routing table represents many other routes. Summarizing routes reduces the routing update traffic and reduces the number of routes in the routing table and overall router overhead in the router receiving the routes

Example of creating Summary Route:

192.168.168.0 = 11000000 10101000 10101 000 00000000 192.168.169.0 = 11000000 10101000 10101 001 00000000 192.168.170.0 = 11000000 10101000 10101 010 00000000 192.168.171.0 = 11000000 10101000

10101 011 00000000

192.168.172.0 = 11000000 10101000 10101 100 00000000

192.168.173.0 = 11000000 10101000 10101 101 00000000 192.168.174.0 = 11000000 10101000 10101 110 00000000

192.168.175.0 = 11000000 10101000 10101 111 00000000

Number of Common Bits = 21

Number of Non-Common Network Bits = 3

Number of Host Bits = 8

So Answer 192.168.168.0/21 is correct.

QUESTION 100

Which two of the following statements represent a preferred wireless LWAPP implementation? (Choose two.)

- A. verify open ports for:
Layer 2 LWAPP on ethertype 0xB BBBB
Layer 3 LWAPP on UDP 12222 and UDP 12223
- B. use of Layer 3 LWAPP is preferred over Layer 2 LWAPP
- C. use of Layer 2 LWAPP is preferred over Layer 3 LWAPP
- D. verify open ports for:
Layer 2 LWAPP on ethertype 0xBABA
Layer 3 LWAPP on UDP 12222 and TCP 12223
- E. verify open ports for:
Layer 2 LWAPP on ethertype 0xABAB
Layer 3 LWAPP on TCP 12222 and TCP 12223

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

LWAPP

Lightweight Access Point Protocol (LWAPP) is a draft Internet Engineering Task Force (IETF) standard for control messaging for setup, authentication, and operations between APs and WLAN controllers (WLC).

In the LWAPP RFC draft, LWAPP control messages can be transported at Layer 2 tunnels or Layer 3 tunnels. Layer 2 LWAPP tunnels were the first method developed in which the APs did not require an IP address. The disadvantage of Layer 2 LWAPP was that the WLC needed to be on every subnet on which the AP resides. Layer 2 LWAPP is a deprecated solution for Cisco. Layer 3 LWAPP is the preferred solution. In the configuration, Layer 2 or Layer 3 transport modes can be selected. When set Layer 3, the LWAPP uses IP addresses to communicate with the access points; these IP addresses are collected from a mandatory DHCP server. When set to Layer 2, the LWAPP uses proprietary code to communicate with the access points.

Note

Layer 2 LWAPP tunnels use EtherType code 0xB BBBB. Layer 3 LWAPP uses UDP ports 12222 and 12223.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 5

QUESTION 101

Which two capabilities of NetFlow accounting assist designers with network planning? (Choose two.)

- A. the monitoring of processor time on network devices

- B. the calculation of packet and byte counts of network traffic
- C. the decoding and analyzing of packets
- D. the presentation of a time-based view of application usage on the network
- E. the monitoring of user network utilization

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 102

What is the benefit of deploying a gatekeeper in an H.323 IP telephony network?

- A. provides spatial redundancy through the use of HSRP
- B. provides load balancing via GUP when alternate gatekeepers are deployed
- C. reduces configuration complexity by centralizing the dial plan
- D. increases redundancy by allowing each gateway to maintain a copy of the dial plan

Correct Answer: C

Section: (none)

Explanation

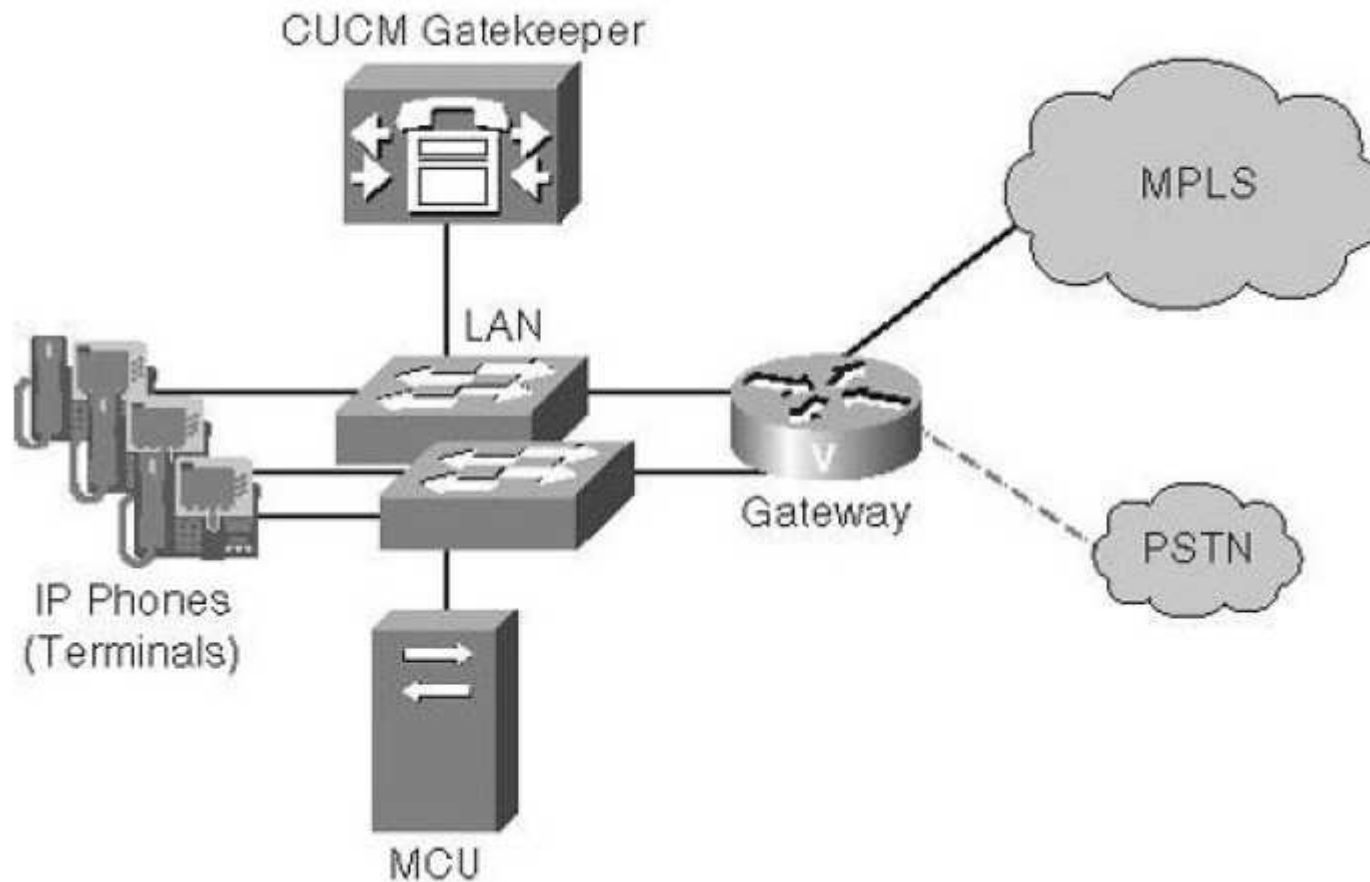
Explanation/Reference:

Explanation: Explanation

H.323

H.323 is a standard published by the ITU that works as a framework document for multimedia protocols, including voice, video, and data conferencing, for use over packet-switched networks. H.323 standards describe terminal (endpoints), gateway, gatekeeper, and multipoint control unit (MCU) devices to be used in a multimedia network. As shown in Figure 14-20, H.323 includes the following elements:

Figure 14-20. H.323 Components



Note: With a gatekeeper, each gateway contains a simpler dial plan and connects only to the gatekeeper.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 14

QUESTION 103

An organization needs a WAN Transport technology that meets these criteria:

has a low initial cost

provides low-to-medium BW

has medium-to-high latency and jitter

Which technology would you suggest?

- A. ISDN
- B. X.25
- C. analog modem
- D. DSL
- E. wireless

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Table. WAN Comparison

WAN Comparison				
WAN Technology	Bandwidth	Reliability	Latency	Cost
ISDN	Low	Medium	Medium	Low
DSL	Low/Medium	Low	Medium	Low
Cable	Low/Medium	Low	Medium	Low
Wireless	Low/Medium	Low	Medium	Medium
Frame Relay	Low/Medium	Medium	Low	Medium
TDM	Medium	High	Low	Medium
Metro Ethernet	Medium/High	High	Low	Medium

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 6

QUESTION 104

Which Cisco security solution offers protection against "day zero" attacks?

- A. Cisco IOS IPS
- B. Cisco IOS Firewall
- C. Cisco Traffic Anomaly Detector
- D. Cisco Adaptive Security Appliance
- E. Cisco Security Agent

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

The Cisco Security Agent (CSA) software protects server and desktop endpoints from the latest threats caused by malicious network attacks. CSA can identify and prevent network attacks that are considered unknown or "Day Zero"-type threats. CSAs are packed with many features, including firewall capabilities, intrusion prevention, malicious mobile code protection, operating-system integrity assurance, and audit log consolidation. (Reference: CCDA Official Exam Certification Guide 3rd)

QUESTION 105

Which type of trunk is required in order to connect a fax machine to a PBX?

- A. intra-office
- B. Foreign Exchange Office
- C. central office
- D. Foreign Exchange Station
- E. inter-office

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Foreign Exchange Station (FXS) provides a connection from a switch to an analog endpoint device such as traditional telephones or fax machines. It provides line power, dial tone, and ring voltage.

Foreign Exchange Office (FXO) allows a switch such as a PBX to use a standard analog connection (FXS) from the PSTN or from another switch. In this case the PBX is emulating an endpoint device. Because this is a standard endpoint connection it uses two-wire connections just like a standard phone and often uses an RJ-11 connector interface.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 14

QUESTION 106

Which H.323 protocol controls call setup between endpoints?

- A. RTCP
- B. H.245
- C. H.225
- D. RAS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

H.323 terminals must support the following standards:

H.245 specifies messages for opening and closing channels for media streams and other commands, requests, and indications. It is a control channel protocol.

Q.931 is a standard for call signaling used by H.323 within the context of H.225. It is also used by PRI links.

H.225 performs registration, admission, and status (RAS) signaling for H.323 sessions.

RTP is the transport layer protocol used to transport VoIP packets. RTCP is also a transport layer protocol.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 14

QUESTION 107

Which two of these represent a best practice implementation of a Split MAC LWAPP deployment in a Cisco Unified Wireless Network? (Choose two.)

- A. Each wireless client authentication type maps to a unique SSID which in turn maps to a unique VLAN.
- B. 802.1Q trunking extends from the wired infrastructure to the access point for translation into SSID(s).
- C. 802.1Q trunking extends from the wired infrastructure to a wireless LAN controller for translation into SSID(s).
- D. Each wireless client authentication type maps to a shared SSID which in turn maps to a common shared VLAN.
- E. Each wireless client authentication type maps to a unique SSID which in turn maps to a common shared VLAN.
- F. 802.1Q trunking extends from the wired infrastructure to a wireless LAN controller. Then the 802.1Q packet is encapsulated in LWAPP and sent to the access point for transmission over the SSID(s).

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Cisco Unified Wireless Network Split-MAC Architecture With the Cisco UWN split-MAC operation, the control and data messages are split. LWAPs communicate with the WLCs using control messages over the wired network. LWAPP or CAPWAP data messages are encapsulated and forwarded to and from wireless clients. The WLC manages multiple APs, providing configuration information and firmware updates as needed. LWAP MAC functions are

Controller MAC functions are

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 5

QUESTION 108

Which two statements best describe intradomain route summarization? (Choose two.)

- A. EIGRP and OSPF must be manually configured to summarize at non-classful boundaries.
- B. EIGRP and OSPF automatically summarize at classful network boundaries.
- C. OSPF and RIP automatically summarize at classful network boundaries.
- D. EIGRP and RIP automatically summarize at classful network boundaries.
- E. EIGRP and OSPF automatically summarize at non-classful boundaries.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Both RIPv2 and EIGRP automatically summarize at Classful network boundaries

auto-summary (EIGRP)

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the auto-summary command in router configuration mode. To disable this function and transmit subprefix routing information across classful network boundaries, use the no form of this command.

auto-summary
no auto-summary

http://www.cisco.com/en/US/docs/ios/12_0/np1/command/reference/1reigrp.html

auto-summary (RIP)

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the auto-summary command in router configuration mode. To disable this function and send subprefix routing information across classful network boundaries, use the no form of this command.

auto-summary
no auto-summary
Usage Guidelines

Route summarization reduces the amount of routing information in the routing tables.

RIP Version 1 always uses automatic summarization. If you are using RIP Version 2, you can turn off automatic

summarization by specifying the no auto-summary command. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is off, subnets are advertised.

http://www.cisco.com/en/US/docs/ios/12_2/iproute/command/reference/1rfrip.html

QUESTION 109

Which two VoIP characteristics are affected most by codec choice? (Choose two.)

- A. voice quality
- B. voice packet header size
- C. bandwidth required for voice calls
- D. silent packet handling

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 110

A network design document is being prepared for a customer. Which three network design elements must be included? (Choose three.)

- A. proof of concept
- B. data sources
- C. design details
- D. organizational policies
- E. implementation plan

Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation
Design Document

The design document describes the business requirements; old network architecture; network requirements; and design, plan, and configuration information for the new network. The network architects and analysts use it to document the new network changes, and it serves as documentation for the enterprise. The design document should include the following sections:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 1

QUESTION 111

Which of these accurately describes dial backup routing?

- A. it always uses distance vector routing protocols
- B. once the backup link is activated it will remain active even after the primary link is restored
- C. it always uses permanent static routes
- D. it is supplied by the service provider as a secondary PVC at no additional charge
- E. the router initiates the dial backup link when a failure is detected on the primary link

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

WAN Backup Design

Redundancy is critical in WAN design for the remote site because of the unreliable nature of WAN links, when compared to LANs that they connect. Most enterprise edge solutions require high availability between the primary and remote site. Because WAN links have lower reliability and lack bandwidth, they are good candidates for most WAN backup designs.

Branch offices should have some type of backup strategy in the event of a primary link failure. Backup links can be either dialup, permanent WAN, or Internet-based connections.

WAN backup options are as follows:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 7

QUESTION 112

Which statement correctly describes queuing in environments supporting teleworkers?

- A. Queuing occurs on the outbound interface.
- B. Hardware queues are configured for appropriate PQ, CQ, or WFQ.
- C. Priority queuing guarantees some level of service to all traffic.
- D. WFQ is the Cisco IOS default on all WAN links regardless of speed.
- E. CQ is for time-sensitive protocols.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 113

Which two techniques can reduce voice packet transfer delay across a link of less than 512 kbps? (Choose two.)

- A. deploy LFI
- B. increase link bandwidth
- C. extend the trust boundary
- D. deploy software compression
- E. increase queue depth

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Table. Link-Efficiency Mechanisms

Link Efficiency mechanisms	
Mechanisms	Description
Link Fragmentation and Interleaving (LFI)	Reduces delay and jitter on slower-speed links by breaking up large packet flows and inserting smaller data packets (Telnet, VoIP) in between them
Multilink PPP (MLP)	Bond multiple links together between two nodes which <u>increases</u> the available bandwidth. MLP can be used on analog or digital links and is based RFC 1990.
Real-Time Transport (RTP) header compression	Provides increased efficiency for applications that take advantage of RTP on slow links. Compresses RTP/UDP/IP header from 40 bytes down to 2-5 bytes.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 6

QUESTION 114
DRAG DROP

Drop

Match the Cisco security solution on the left to its function on the right.

Anomaly Guard and Detector

protects the endpoints

Cisco Security Agent

provides multiple functions for security

IPS Appliance

prevents attacks

ASA

provides Web security

SSL Service Module

prevents data leakage

- A.
- B.
- C.

D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

Match the Cisco security solution on the left to its function on the right.

Anomaly Guard and Detector

Cisco Security Agent

IPS Appliance

ASA

SSL Service Module

Cisco

Anomaly

SSL

IP

Explanation: + protects the endpoints (desktops, laptops and servers): Cisco Security Agent + provides multiple functions as a high performance security appliance: ASA + prevents DDoS attacks: Anomaly Guard and Detector + provides Web-Based VPN services: SSL Service Module + prevents attacks inline: IPS Appliance

Cisco Security Agent

ASA

Anomaly Guard and Detector

SSL Service Module

IPS Appliance

QUESTION 115

Your company uses OSPF for internal routing. The company will be connected to VendorA via a single dedicated link and to VendorB via redundant dedicated links. Both vendors also use OSPF for internal routing. Which of the following deployments describes the best intra-domain routing practice in this situation?

- A. Redistribute the routes on each link between your company and the vendors to a shared EIGRP routing protocol.
- B. Use IBGP to reach VendorA and EBGP to reach VendorB.
- C. Use static routes to reach VendorA and EBGP to reach VendorB.
- D. Use static routes to reach both VendorA and VendorB.
- E. Connect your company to both VendorA and VendorB using existing OSPF.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 116

Which statement can a network designer use to describe route summarization to an IT manager?

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

Correct Answer: C

Section: (none)

Explanation

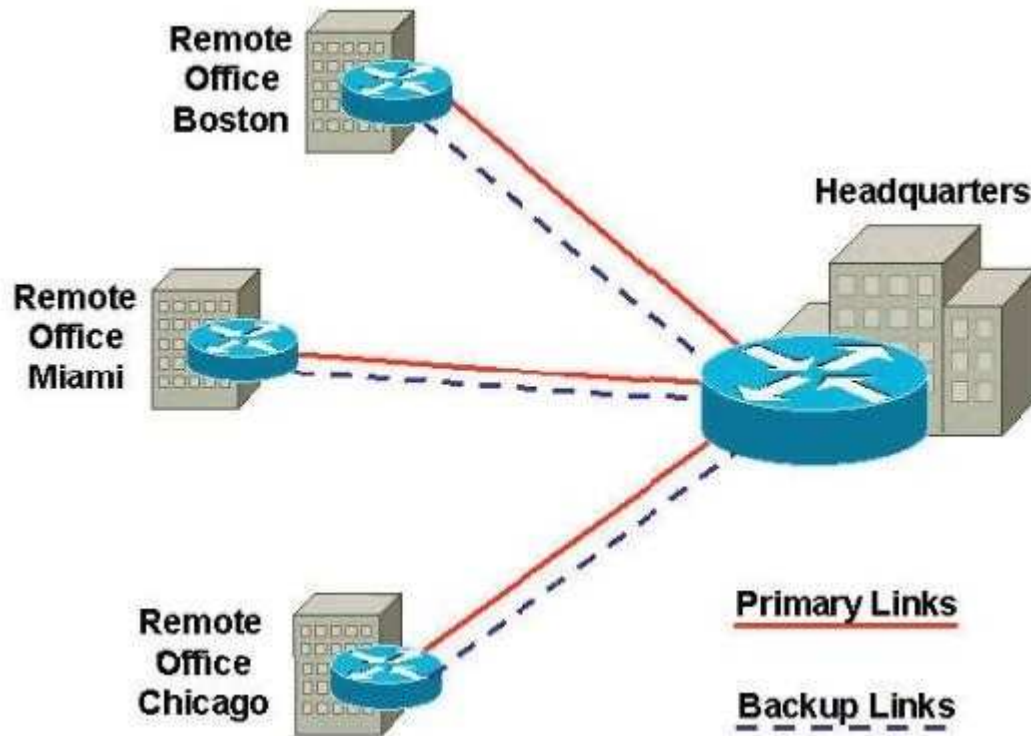
Explanation/Reference:

Explanation:

QUESTION 117

Refer to the exhibit. All primary links are T1s. The customer wants to have a backup to each remote office from the Headquarters office.

Which two types of backup links would be viable solutions? (Choose two.)



- A. dial backup routing
- B. shadow SVC
- C. permanent secondary WAN link
- D. VPDN

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

WAN Backup Design

Redundancy is critical in WAN design for the remote site because of the unreliable nature of WAN links, when compared to LANs that they connect. Most enterprise edge solutions require high availability between the primary and remote site. Because WAN links have lower reliability and lack bandwidth, they are good candidates for most WAN backup designs.

Branch offices should have some type of backup strategy in the event of a primary link failure. Backup links can be either dialup, permanent WAN, or Internet-based connections.

WAN backup options are as follows:

Dial backup: ISDN provides backup dialup services in the event of a primary failure of a WAN circuit. The backup link is initiated if a failure occurs with the primary link. The ISDN backup link provides network continuity

until the primary link is restored, and then the backup link is terminated such as with floating static route techniques.

Secondary WAN link: Adding a secondary WAN link makes the network more fault tolerant. This solution offers two key advantages:

Backup link: Provides for network connectivity if the primary link fails. Dynamic or static routing techniques can be used to provide routing consistency during backup events. Application availability can also be increased because of the additional backup link.

Additional bandwidth: Load sharing allows both links to be used at the same time, increasing the available bandwidth. Load balancing can be achieved over the parallel links using automatic routing protocol techniques.

Shadow PVC: SPs can offer shadow Frame Relay PVCs, which provide additional PVCs for use if needed. The customer is not charged for the PVC if it does not exceed limits set by the provider while the primary PVC is available. If the limit is exceeded, the SP charges the customer accordingly.

IPsec tunnel across the Internet: An IPsec VPN backup link can direct redirect traffic to the corporate headquarters when a network failure has been detected.

QUESTION 118

A Cisco SONA architecture layer is described as follows:

The layer's IT resources are interconnected across a converged network foundation.

The layer's IT resources include servers, storage, and clients.

The layer represents how resources exist across the network.

The customer objective for the layer is to have anywhere/anytime connectivity.

Which Cisco SONA architecture layer is being described?

- A. Application
- B. Integrated Transport
- C. Physical
- D. Networked Infrastructure
- E. Interactive Services

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 119

Which information should a network summary report identify?

- A. actions needed to support the existing network
- B. customer requirements
- C. new network features
- D. customer requirement modifications
- E. actions needed to support existing network features
- F. infrastructure shortcomings

Correct Answer: F

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 120

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. 7 calls
- B. 13 calls
- C. 8 calls
- D. 9 calls
- E. 11 calls

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Codecs

Because speech is an analog signal, it must be converted into digital signals for transmission over digital systems. The first basic modulation and coding technique was pulse-code modulation (PCM). The international standard for PCM is G.711. With PCM, analog speech is sampled 8000 times a second. Each speech sample is mapped onto 8 bits. Thus, PCM produces (8000 samples per second) * (8 bits per sample) = 64,000 bits per second = 64-kbps coded bit rate. Other coding schemes have been developed to further compress the data representation of speech. G.711 is used as the primary with IPT over LANs where high bandwidth is available.

G.711 = 64Kbps

Packet Header = 6 bytes

Payload = 160 bytes

Total = 64166 bytes or 64.166 Kbps per call

768 Kbps / 64.166 Kbps = 11.96

Therefore 11 Calls can be supported

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 6

QUESTION 121

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

- A. Use organizational input.
- B. Analyze the user-mapping of a running application.
- C. Perform a traffic analysis.
- D. Perform a packet-level audit to verify carrier service guarantees.

- E. Use reports that analyze the metrics of the customer's existing network.
- F. Perform a network audit to gather more detail about the network.

Correct Answer: CEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Table, Characterizing the Network

Characterizing the Network	
Characteristic	Description
Steps in gathering information	Step 1: Obtain existing information and documentation Step 2: Network audit Step 3: Traffic analysis
Primary sources of network audit information	Existing documentation Existing network management software New network management tools

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 1

QUESTION 122

Which two of these are required for wireless client mobility deployment when using a Cisco Unified Wireless Network? (Choose two.)

- A. matching RF power
- B. matching security
- C. assigned master controller
- D. matching mobility group name
- E. matching RF channel
- F. matching RF group name

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 123

In the Cisco branch office design, what categorizes an office as large?

- A. between 50 and 100 users and a single-tier design
- B. between 100 and 200 users and a three-tier design
- C. between 50 and 100 users and a three-tier design
- D. over 200 users and a two-tier design
- E. between 100 and 200 users and a two-tier design

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 124

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

- A. broadcast
- B. multicast
- C. anycast
- D. unicast

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

IPv6 Anycast Addresses

The IPv6 anycast (one-to-nearest) address identifies a set of devices. An anycast address is allocated from a set of unicast addresses. These destination devices should share common characteristics and are explicitly configured for anycast.

You can use the anycast address to identify a set of routers or servers within an area. When a packet is sent to the anycast address, it is delivered to the nearest device as determined by the routing protocol. An example of the use of anycast addresses is to assign an anycast address to a set of servers--one in North America, and the other in Europe. Users in North America would be routed to the North American server, and those in Europe to the European server.

You cannot use an anycast address as a source address. Also, you must explicitly configure nodes to which the anycast address is assign to recognize the anycast address.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 9

QUESTION 125

When designing using the Cisco Enterprise Architecture, in which Enterprise Campus layer do the Enterprise Edge and Enterprise WAN modules establish their connection?

- A. Building Access
- B. Building Distribution
- C. Campus Core
- D. Enterprise Branch
- E. Enterprise Data Center

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Enterprise Edge connects to the edge-distribution module of the enterprise campus. In small and medium sites, the edge distribution can collapse into the campus-backbone component. It provides connectivity to outbound services that are further described in later sections.

Cisco Enterprise Architecture Model	
Enterprise Area or Module	Description
Enterprise Campus Area	The Enterprise Campus module includes the building-access and building-distribution components and the shared campus backbone component or campus core. Edge distribution provides connectivity to the Enterprise Edge. High availability is implemented in the server farm, and network management monitors the Enterprise Campus and Enterprise Edge.
Enterprise Edge Area	Consists of e-commerce, Internet, VPN/remote access, and WAN modules.
Enterprise WAN Module	This module provides MPLS or other WAN technologies.
Enterprise Remote Branch Module	The Enterprise Branch normally consists of remote offices, small offices, or sales offices. These branch offices rely on the WAN to use the services and applications provided in the main campus.
Enterprise Data Center Module	The Enterprise Data Center consists of using the network to enhance the server, storage, and application servers. The offsite data center provides disaster recovery and business continuance services for the enterprise.
Enterprise Teleworker	The Enterprise Teleworker module supports a small office, mobile users, or home users providing access to corporate systems via VPN tunnels.

QUESTION 126

Which three of these describe the best practice for Cisco wireless outdoor Mesh network deployment? (Choose three.)

- A. mesh hop counts of 4 or fewer
- B. RAP implemented with 20 or fewer MAP nodes
- C. client access via 802.11a and backhaul with 802.11b/g
- D. client access via 802.11b/g and backhaul with 802.11a
- E. mesh hop counts of 8 to 4
- F. RAP implemented with 20 to 32 MAP nodes

Correct Answer: ADF

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Mesh Design Recommendations

The following are Cisco recommendations (and considerations) for mesh design:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 5

QUESTION 127

The Cisco Data Center Network Architecture comprises which two Cisco SONA layers? (Choose two.)

- A. Collaboration Applications
- B. WAN/Internet
- C. Interactive Services
- D. Network Infrastructure
- E. Business Applications

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

The SONA framework defines the following three layers:

+ Networked Infrastructure layer: Where all the IT resources interconnect across a converged network foundation. The objective of this layer is to provide connectivity, anywhere and anytime. + Interactive Services layer: Includes both application networking services and infrastructure services. This layer enables efficient allocation of resources to applications and business processes delivered through the networked infrastructure. + Application layer: Includes business applications and collaboration applications. The objective of this layer is to meet business requirements and achieve efficiencies by leveraging the Interactive Services layer. With above information, you can answer question 2 and 3 below.

QUESTION 128

Which two of these are scalability benefits of designing a network that utilizes VPNs?

(Choose two.)

- A. reduces dial infrastructure expenditures
- B. reduces the number of physical connections
- C. allows networks to be set up and restructured quickly
- D. simplifies the underlying structure of a customer WAN
- E. extends the network to remote users

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

What Are the Advantages and Benefits of a VPN?

A VPN - Virtual Private Network - is one solution to establishing long-distance and/or secured network connections. VPNs are normally implemented (deployed) by businesses or organizations rather than by individuals, but virtual networks can be reached from inside a home network. Compared to other technologies, VPNs offers several advantages, particularly benefits for wireless local area networking.

Answer: For an organization looking to provide a secured network infrastructure for its client base, a VPN offers two main advantages over alternative technologies: cost savings, and network scalability. To the clients accessing these networks, VPNs also bring some benefits of ease of use.

Cost Savings with a VPN

A VPN can save an organization money in several situations:

VPNs vs leased lines - Organizations historically needed to rent network capacity such as T1 lines to achieve full, secured connectivity between their office locations. With a VPN, you use public network infrastructure

including the Internet to make these connections and tap into that virtual network through much cheaper local leased lines or even just broadband connections to a nearby Internet Service Provider (ISP).

Long distance phone charges - A VPN also can replace remote access servers and long- distance dialup network connections commonly used in the past by business travelers needing to access to their company intranet. For example, with an Internet VPN, clients need only connect to the nearest service provider's access point that is usually local. Support costs - With VPNs, the cost of maintaining servers tends to be less than other approaches because organizations can outsource the needed support from professional third- party service providers. These provides enjoy a much lower cost structure through economy of scale by servicing many business clients.

http://compnetworking.about.com/od/vpn/f/vpn_benefits.htm

QUESTION 129

You are designing a small branch office that requires these attributes:

support for 60 users

the growth capacity to add another 15 users soon

redundant access

higher bandwidth between the Layer 2 switch and routing to the WAN

Which branch office topology or technology must be used?

- A. EtherChannel
- B. loop-free
- C. three-tier
- D. two-tier
- E. integrated routing and switching

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

EtherChannel

The Cisco EtherChannel implementations provide a method to increase the bandwidth between two systems by bundling Fast Ethernet, Gigabit Ethernet, or 10GE links. When bundling Fast Ethernet links, use Fast EtherChannel. Gigabit EtherChannel bundles Gigabit Ethernet links. EtherChannel port bundles enable you to group multiple ports into a single logical transmission path between the switch and a router, host, or another switch. EtherChannels provide increased bandwidth, load sharing, and redundancy. If a link fails in the bundle, the other links take on the traffic load. You can configure EtherChannel bundles as trunk links.

Depending on your hardware, you can form an EtherChannel with up to eight compatibly configured ports on the switch. The participating ports must have the same speed and duplex mode and belong to the same VLAN. Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 3

QUESTION 130

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 includes these connectivity technologies:

Frame Relay

ATM

SONET

cable

DSL

wireless

From a Layer 1 viewpoint, which Enterprise Edge module will be most affected?

- A. Internet Connectivity
- B. E-Commerce
- C. PSTN
- D. Edge Distribution
- E. ISP
- F. WAN/MAN

Correct Answer: F

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Enterprise Edge Area

As shown in Figure 2-7, the enterprise edge consists of the following submodules:

QUESTION 131

DRAG DROP

Match the bandwidth usage optimization technique on the left with its definition on the right.

queuing

limits the number of
acknowledgements

window size

reduces data size
optimizing the

traffic policing

allows network ad
varying demands

data compression

discards packets or
(such as

- A.
- B.

- C.
- D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

Match the bandwidth usage optimization technique on the left with its definition on the right.

queuing

window size

traffic policing

data compression

Explanation: + limits the number of frames transmitted before an acknowledgement is received:
 window size+ reduces data size to save transmission time, optimizing the use of WAN bandwidth:
 data compression+ allows network administrators to manage the varying demands generated by applications:
 queuing+ discards packets or modifies some aspect of them (such as IP precedence): traffic policing

QUESTION 132

Which two implementation plan principles best describe how to deal with potential failures? (Choose two.)

- A. A table of failure points, rollback steps, and estimated rollback times.
- B. A good implementation plan.
- C. A test should be included at every step.
- D. A detailed rollback procedure for each implementation step.
- E. A successful test network test.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

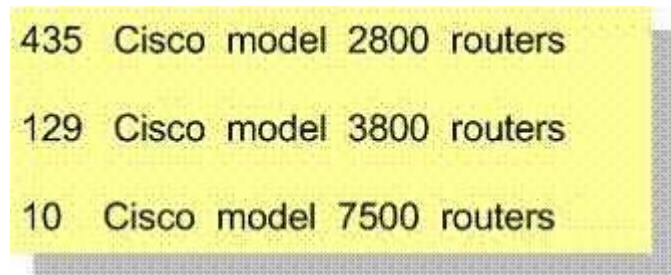
Implement Phase

New equipment is installed and configured, according to design specifications, in the Implement phase. New devices replace or augment the existing infrastructure. The project plan is followed during this phase. Planned network changes should be communicated in change control meetings, with necessary approvals to proceed. Each step in the implementation should include a description, detailed implementation guidelines, estimated time to implement, rollback steps in case of a failure, and any additional reference information. As changes are implemented they are also tested before moving to the Operate phase.

QUESTION 133

Refer to the exhibit. You are documenting the existing network of a customer with a large installed Cisco network. The routers listed are in use on the network.

Which two additional pieces of information would be the most valuable in completing your documentation of these routers? (Choose two.)



435	Cisco model 2800 routers
129	Cisco model 3800 routers
10	Cisco model 7500 routers

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 134

Which of these is the next step after the design phase in the PPDIOO process?

- A. Develop a high-level migration plan.
- B. Develop the implementation plan in as much detail as possible.
- C. Create a pilot or a prototype network.
- D. Identify which network management protocol will be used for which function.
- E. Order the equipment.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

The Implement phase begins after the design phase has been finished. In this phase, new devices are installed, configured and tested according to the design specifications.

QUESTION 135

You are designing IPv6 into an existing IPv4 network. Which two strategies can you use to allow both address

schemes to coexist, thus facilitating migration? (Choose two)

- A. translate one protocol into the other
- B. redistribute between IPv6-capable and non-IPv6-capable routing protocols
- C. encapsulate IPv6 packets within IPv4 packets
- D. bridge between the IPv6 and IPv4 networks
- E. enable anycast capability in the routing protocol

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

IPv4 to IPv6 Transition Mechanisms and Deployment Models

This section describes transition mechanisms and deployment models to migrate from IPv4 to IPv6. During a transition time, both protocols can coexist in the network. The three major transition mechanisms are

Each model provides several advantages and disadvantages; familiarize yourself with those. Of all these models, the dual-stack model is recommended because it requires no tunneling and is easier to manage.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 9

QUESTION 136

A network is being designed to meet the requirements listed.

Within the enterprise network:

All routers are Cisco 3800 Series routers running the latest Cisco IOS release.

The fastest convergence time possible is required.

Unequal cost load-balancing is required.

For Internet connections:

A single link is used to connect to a single ISP.

Which two routing protocols should be used?(Choose two.)

- A. Use Internal BGP as the IGP within the enterprise.
- B. Use Static (Default) routing between the enterprise and the ISP.
- C. Use OSPF as the IGP within the enterprise.
- D. Use EIGRP as the IGP within the enterprise.
- E. Use EIGRP between the enterprise and the ISP.
- F. Use External BGP between the enterprise and the ISP.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The requirements are to have an IGP that have the fastest possible convergence and Unequal cost load balancing. The routing protocol options listed are BGP, Static, OSPF, and EIGRP. EIGRP has the fastest

convergence time and supports unequal cost load balancing. BGP has the slowest possible convergence time. Static routes do not support unequal cost load balancing. OSPF has a slower convergence time than EIGRP.

In regards to the ISP connection typically you would use an EGP or static route. The only EGP available is BGP. However, BGP should ONLY be used when connecting to multiple ISPs or with multiple default gateways. Not to mention this adds additional layers of complexity and slows down convergence time. The best option for a single internet connection is to configure a static route.

QUESTION 137

Which two statements best describe Cisco Wireless LAN Guest Access in a Cisco Unified Wireless Network? (Choose two.)

- A. Dedicated guest VLANs are only extended to the wireless controllers in the network to ensure path isolation.
- B. Guest tunnels have limitations on which wireless controllers can originate the tunnel.
- C. Dedicated guest VLANs are extended throughout the network to the access points for path isolation.
- D. Guest tunnels can originate and terminate on any wireless controller platform.
- E. Guest tunnels have limitations on which wireless controllers can terminate the tunnel.
- F. Dedicated guest access in the DMZ extends from the origination to the termination controllers without dedicated guest VLANs.

Correct Answer: EF

Section: (none)

Explanation

Explanation/Reference:

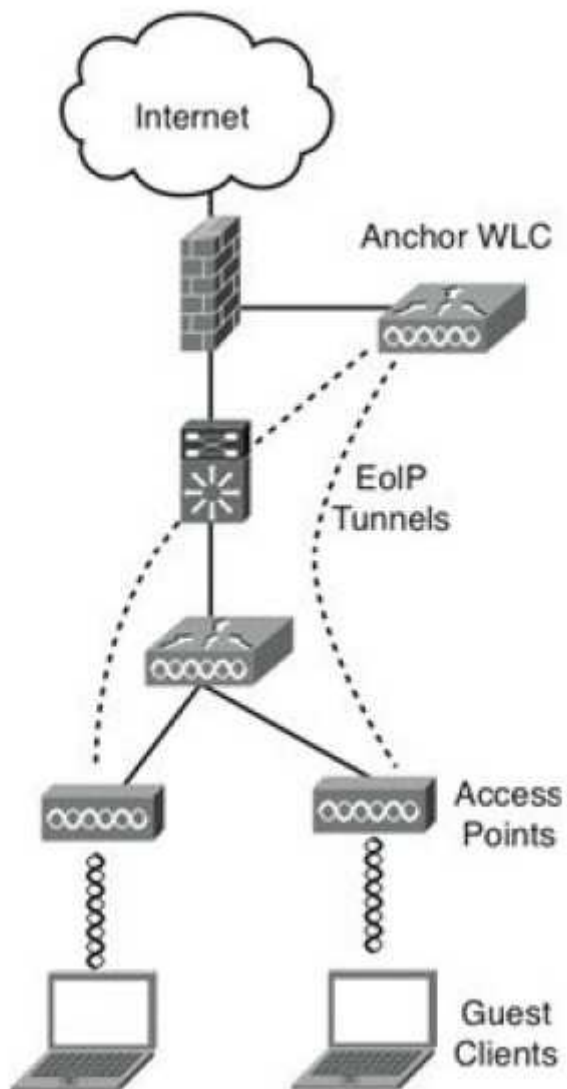
Explanation: Explanation

Using EoIP Tunnels for Guest Services

Basic solutions use separate VLANs for guest and corporate users to segregate guest traffic from corporate traffic. The guest SSID is broadcast, but the corporate SSID is not. All other security parameters are configured. Another solution is to use Ethernet over IP (EoIP) to tunnel the guest traffic from the CAPWAP to an anchor WLC.

As shown in Figure 5-17, EoIP is used to logically segment and transport guest traffic from the edge AP to the anchor WLC. There is no need to define guest VLANs in the internal network, and corporate traffic is still locally bridged. The Ethernet frames from the guest clients are maintained across the CAPWAP and EoIP tunnels.

Figure. EoIP Tunnels



Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 5

QUESTION 138

For which technology is IPsec required for a site-to-site enterprise WAN/MAN architecture?

- A. self-deployed MPLS
- B. ATM
- C. Frame Relay
- D. SP MPLS VPN
- E. ISP Service

Correct Answer: E

Section: (none)

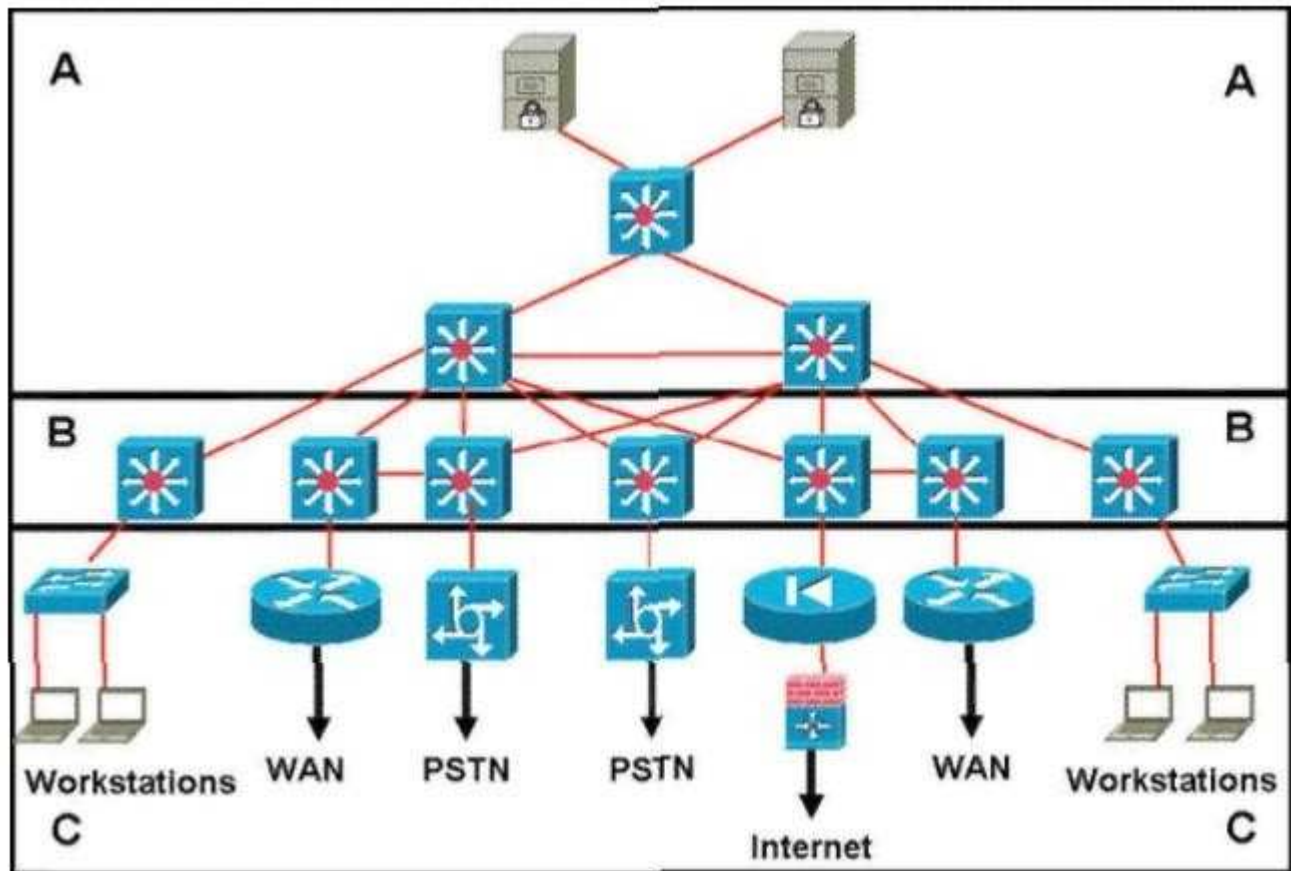
Explanation

Explanation/Reference:

Explanation:

QUESTION 139

Refer to the exhibit. Which statement accurately represents the characteristics of the core layer in this design?



- A. Access lists should be used in the core to perform packet manipulation.
- B. QoS should be performed only in the core.
- C. Load balancing should never be implemented or used in the core.
- D. It is acceptable to use a partial mesh in the core if it is connected to each device by multiple paths.
- E. Policy-based traffic control is implemented in the core to enable prioritization, ensuring the best performance for all time-critical applications.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 140

What does Cisco recommend as the foundation of any deployed security solution?

- A. Customer needs
- B. Security audit
- C. Service-level agreement
- D. Corporate security policy

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Security Policy and Process

To provide the proper levels of security and increase network availability, a security policy is a crucial element in providing secure network services. This is an important concept to understand, and such business requirements should be considered throughout the system life cycle. Business requirements and risk analysis are used in the development of a security policy. It is often a balance between ease of access versus the security risk and cost of implementing the security technology.

In terms of network security in the system life cycle, the business needs are a key area to consider. Business needs define what the business wants to do with the network.

Risk analysis is another part of the system life cycle. It explains the risks and their costs. Business needs and risk assessment feed information into the security policy.

The security policy describes the organization's processes, procedures, guidelines, and standards. Furthermore, industry and security best practices are leveraged to provide well-known processes and procedures.

Finally, an organization's security operations team needs to have processes and procedures defined. This information helps explain what needs to happen for incident response, security monitoring, system maintenance, and managing compliance.

Table, outlines key network security considerations.

Table 12-6 Key Network Security Elements of the network Security Life Cycle	
Security Consideration	Name
What are the business requirements?	Business Needs
What is associated risk and cost?	Risk Analysis
What policy governs the business requirements and risk?	Security Policy
What are the recommend industry security best practices?	Best practices
What will the process be for incident, compliance, and change management?	Security Operations

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 12

QUESTION 141

What is the administrative distance of eBGP routes?

- A. 200
- B. 100
- C. 20
- D. 110

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Default Administrative Distances for IP Routes	
IP Route	Administrative Distance
Connected interface	0
Static route directed to a connected interface	0
Static route directed to an IP address	1
EIGRP summary route	5
External BGP route	20
Internal EIGRP route	90
IGRP route	100
OSPF route	110
IS-IS route	115
RIP route	120
EGP route	140
External EIGRP route	170
Internal BGP route	200
Route of unknown origin	255

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 10

QUESTION 142

Which name is for the Cisco product that provides centralized, policy-based security management?

- A. IDS
- B. Out-of-band management
- C. AAA
- D. CSPM

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cisco Secure Policy Manager 2.3

The Cisco Secure Policy Manager (CSPM) allows you to configure, manage, and monitor their end-to-end Cisco Systems security networks. CSPM is a policy-based product that enables you to abstract the complexities of security networking. With CSPM you can create high-level security policies that are independent of underlying device platforms and software releases. CSPM is the Cisco strategic security management platform

for Cisco Secure PIX Firewalls, Cisco Secure IOS Firewalls, Cisco IOS® virtual private networking (VPN) routers, and Cisco Secure Intrusion Detection System (IDS) sensors.

CSPM provides the following benefits:

CSPM 2.3 incorporates many of the network operations features that are used in LAN and WAN environments.
Reference:

http://www.cisco.com/en/US/products/sw/secursw/ps2133/prod_technical_reference09186a00800_a9ebc.html

QUESTION 143

Which statement represents a likely starting point for planning network changes?

- A. Protocol assessment
- B. Determining the design requirements
- C. Determining the business needs
- D. Determining the application requirements

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

There are three key objectives of an effective WAN design:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 6

QUESTION 144

What does IGMP stand for?

- A. Internet Group Management Protocol
- B. Interior Gateway Routing Protocol
- C. Interior Group Management Protocol
- D. Interior Gateway Media Protocol

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

IGMP

Internet Group Management Protocol is the protocol used in multicast implementations between the end hosts and the local router. RFC 2236 describes IGMP Version 2 (IGMPv2). RFC 3376 describes IGMP Version 3 (IGMPv3). RFC 1112 describes the first version of IGMP.

IP hosts use IGMP to report their multicast group memberships to routers. IGMP messages use IP protocol number 2. IGMP messages are limited to the local interface and are not routed.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 11

QUESTION 145

DRAG DROP

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

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

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

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

Explanation:

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

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 NMS and 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 a simple 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 146

ISDN is short for Integrated Services Digital Network. Under what category of WAN technologies does ISDN belong?

- A. Cell-switched
- B. Circuit-switched
- C. Packet-switched
- D. Leased lines

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Traditional WAN Technologies When selecting a particular WAN technology, you should be familiar with the three major categories that represent traditional WANs:

Circuit switched: Data connections that can be brought up when needed and terminated when finished. Examples include ordinary public switched telephone network (PSTN) phone service, analog modems, and ISDN. Carriers reserve that call path through the network for the duration of the call.

Leased lines: A dedicated connection provided by the SP. These types of connections are point to point and generally more expensive. Time-division multiplexing (TDM)-based leased lines usually use synchronous data transmission.

Packet and cell switched: Connections that use virtual circuits (PVC/SVC) established by the SP. Packet-switched technologies include Frame Relay and cell-switched technologies such as ATM. ATM uses cells and provides support for multiple quality of service (QoS) classes. The virtual circuits are part of the shared ATM/Frame Relay SP backbone network. This gives the SP greater flexibility with its service offerings.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter

QUESTION 147

As a network engineer, can you tell me accounting management on a network-management system allows a network manager to perform which function?

- A. Assess the network's effectiveness and throughput
- B. Charge back to users for network resources
- C. Performance management
- D. Identify problem areas in the network

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 148

Which address type is 225.10.1.1?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Answer A is incorrect as Unicast is an IPv6 address

Answer B is incorrect as Anycast is an IPv6 one to nearest address that identifies a set of devices Answer C is correct as multicast addresses range from 224.0.0.1 to 239.255.255.255. Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 8

QUESTION 149

What is the length of the key used with Triple Data Encryption Standard (3DES)?

- A. 64 bits
- B. 168 bits
- C. 128 bits
- D. 56 bits

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

In cryptography, Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Because of the availability of increasing computational power, the key size of the original DES cipher was becoming subject to brute force attacks; Triple DES was designed to provide a relatively simple method of increasing the key size of DES to protect against such attacks, without designing a completely new block cipher algorithm.

Triple DES uses a "key bundle" which comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits). The encryption algorithm is:
$$\text{ciphertext} = \text{EK3}(\text{DK2}(\text{EK1}(\text{plaintext})))$$

I.e., DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3.

Decryption is the reverse:

$$\text{plaintext} = \text{DK1}(\text{EK2}(\text{DK3}(\text{ciphertext})))$$

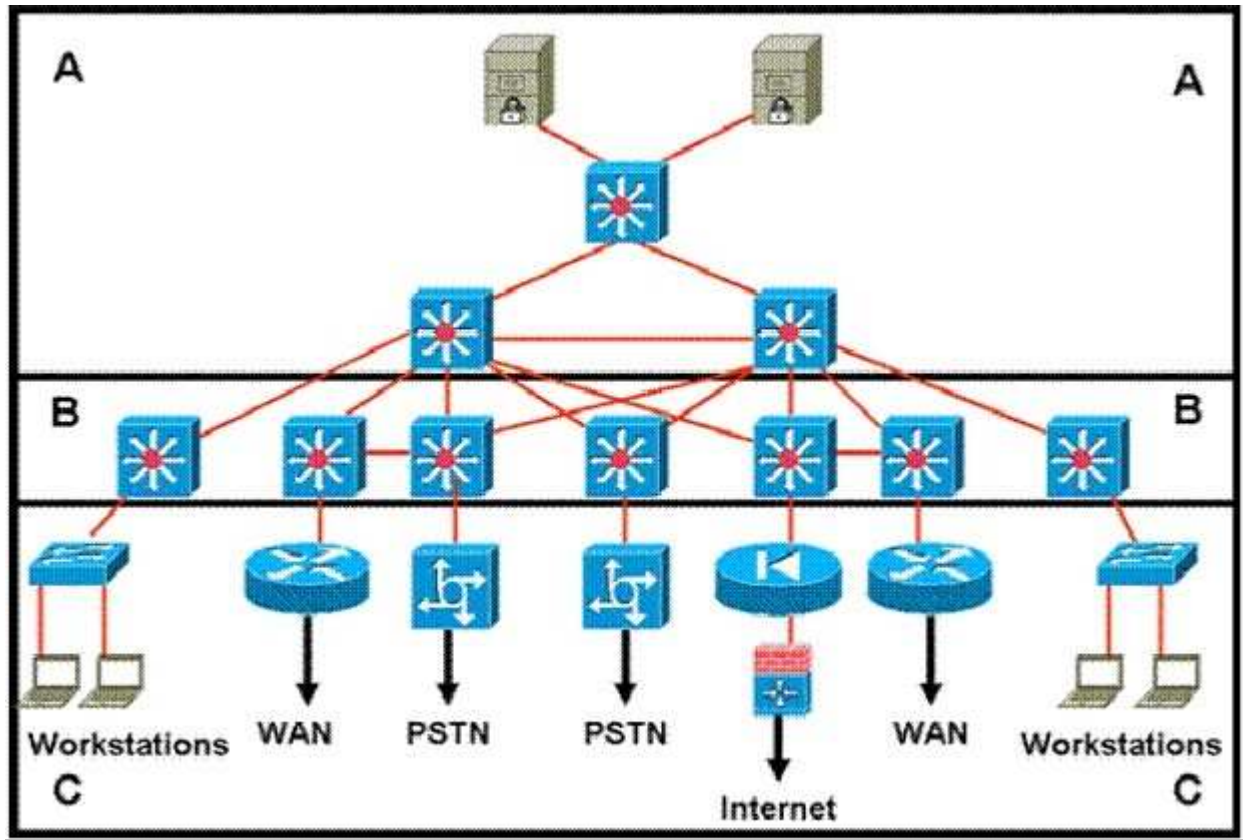
I.e., decrypt with K3, encrypt with K2, then decrypt with K1. Each triple encryption encrypts one block of 64 bits of data. In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3.

The standards define three keying options:

Keying option 1 is the strongest, with $3 \times 56 = 168$ independent key bits. Keying option 2 provides less security, with $2 \times 56 = 112$ key bits. This option is stronger than simply DES encrypting twice, e.g. with K1 and K2, because it protects against meet-in-the-middle attacks. Keying option 3 is equivalent to DES, with only 56 key bits. This option provides backward compatibility with DES, because the first and second DES operations cancel out. It is no longer recommended by the National Institute of Standards and Technology (NIST),[5] and is not supported by ISO/IEC 18033-3.

QUESTION 150

Refer to the exhibit.



Which layer is the distribution layer?

- A. Layer A
- B. Layer B
- C. Layer C
- D. Layers A and B form a consolidated core and distribution layer

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 151

A wireless LAN or WLAN is a wireless local area network, which is the linking of two or more computers or devices without using wires. How are wireless LANs identified?

- A. Service Set Identifier (SSID)

- B. Internet Group Management Protocol (IGMP)
- C. IP network
- D. Wired Equivalent Privacy (WEP) key

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Service Set Identifier

WLANs use a service set identifier (SSID) to identify the WLAN's "network name." The SSID can be 2 to 32 characters long. All devices in the WLAN must have the same configured SSID to communicate. It is similar to a VLAN identifier in a wired network. The difficulty in large networks is configuring the SSID, frequency, and power settings for hundreds of remotely located access points. Cisco addresses this problem with the Cisco Wireless Control System (WCS). WCS is covered in more detail in the "Cisco UWN Architecture" section.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 5

Topic 3, Volume B

QUESTION 152

Observe the following options, what is the hierarchy for IPv6 aggregatable addresses?

- A. Global, site, loop
- B. Multicast, anycast, unicast
- C. Public, site, interface
- D. Internet, site, interface

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Global Unicast Addresses

IPv6 global addresses connect to the public network. These unicast addresses are globally unique and routable. This address format is initially defined in RFC 2374. RFC 3587 provides updates to the format.

The original specification defined the address format with a three-layer hierarchy: public topology, site topology, and interface identifier. The public topology consisted of service providers that provided transit services and exchanges of routing information. It used a top-level aggregator (TLA) identifier and a next-level identifier. A site-level aggregator (SLA) was used for site topology. The site topology is local to the company or site and does not provide transit services. The TLA, NLA, and SLA identifiers are deprecated by RFC 3587. RFC 3587 simplifies these identifiers with a global routing prefix and subnet identifier for the network portion of the address.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 9

QUESTION 153

Which IGP protocol is a common choice to EIGRP and OSPF as a routing protocol for large networks?

- A. RIPv2
- B. IS-IS
- C. IGRP
- D. OSPFv2

Correct Answer: B

Section: (none)

Explanation

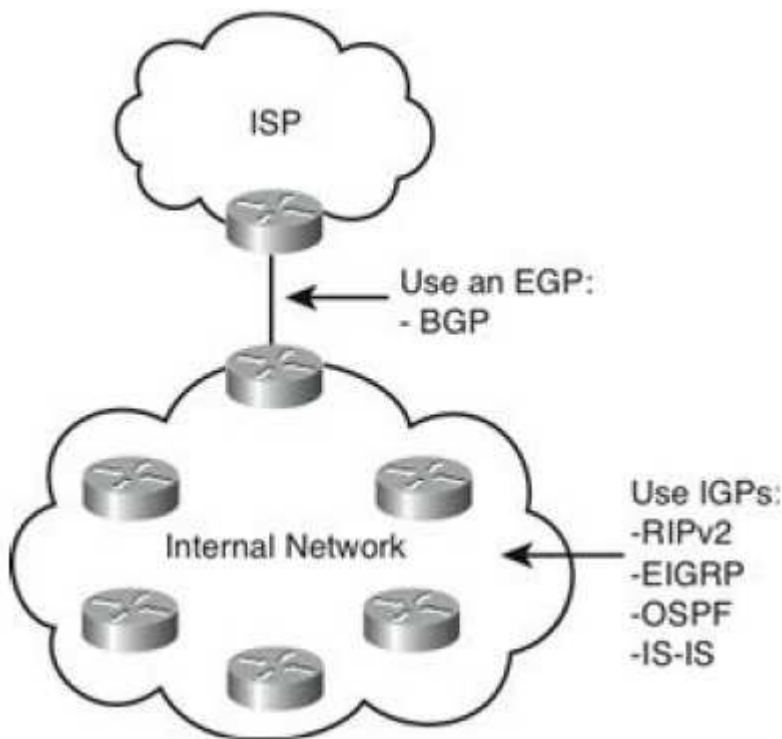
Explanation/Reference:

Explanation: Explanation

Interior Versus Exterior Routing Protocols

Routing protocols can be categorized as interior gateway protocols (IGP) or exterior gateway protocols (EGP). IGPs are meant for routing within an organization's administrative domain (in other words, the organization's internal network). EGPs are routing protocols used to communicate with exterior domains, where routing information is exchanged between administrative domains. Figure 10-2 shows where an internetwork uses IGPs and EGPs with multiple autonomous administrative domains. BGP exchanges routing information between the internal network and an ISP. IGPs appear in the internal private network.

Figure 10-2. Interior and Exterior Routing Protocols



One of the first EGPs was called exactly that: Exterior Gateway Protocol. Today, BGP is the de facto (and the only available) EGP. Potential IGPs for an IPv4 network are

Potential IGPs for an IPv6 network are

RIPv1 is no longer recommended because of its limitations. RIPv2 addresses many of the limitations of RIPv1 and is the most recent version of RIP. IGRP is an earlier version of EIGRP. RIPv1 and IGRP are no longer CCDA exam topics.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 10

QUESTION 154

Which type of routing protocol will be used when connecting to an Internet service provider?

A. Classless routing protocol

- B. Exterior gateway protocol
- C. Interior gateway protocol
- D. Classful routing protocol

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Routing protocols can be categorized as interior gateway protocols (IGP) or exterior gateway protocols (EGP). IGPs are meant for routing within an organization's administrative domain (in other words, the organization's internal network). EGPs are routing protocols used to communicate with exterior domains, where routing information is exchanged between administrative domains.

When connecting to an ISP you are exchanging routing information between administrative domains so an EGP is required

QUESTION 155

Which routing protocol is classful?

- A. Intermediate System-to-Intermediate System (IS-IS) and OSPF
- B. Routing Information Protocol Version 1 (RIPv1) and RIPv2
- C. IGRP and RIPv1
- D. Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF)

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Classless Versus Classful Routing Protocols

Routing protocols can be classified based on their support of VLSM and CIDR. Classful routing protocols do not advertise subnet masks in their routing updates; therefore, the configured subnet mask for the IP network must be the same throughout the entire internetwork. Furthermore, the subnets must, for all practical purposes, be contiguous within the larger internetwork. For example, if you use a classful routing protocol for network 130.170.0.0, you must use the chosen mask (such as 255.255.255.0) on all router interfaces using the 130.170.0.0 network. You must configure serial links with only two hosts and LANs with tens or hundreds of devices with the same mask of 255.255.255.0. The big disadvantage of classful routing protocols is that the network designer cannot take advantage of address summarization across networks (CIDR) or allocation of smaller or larger subnets within an IP network (VLSM). For example, with a classful routing protocol that uses a default mask of /25 for the entire network, you cannot assign a /30 subnet to a serial point-to-point circuit.

Classful routing protocols are

Classless routing protocols advertise the subnet mask with each route. You can configure subnetworks of a given IP network number with different subnet masks (VLSM). You can configure large LANs with a smaller subnet mask and configure serial links with a larger subnet mask, thereby conserving IP address space.

Classless routing protocols also allow flexible route summarization and supernetting (CIDR). You create supernets by aggregating classful IP networks. For example, 200.100.100.0/23 is a supernet of 200.100.100.0/24 and 200.100.101.0/24.

Classless routing protocols are

QUESTION 156

Which attack type would you expect on segments that have many servers for some well-known applications?

- A. Trojan horses
- B. DoS attacks
- C. Application-layer attacks
- D. Password attacks

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Application security and content security defense: Several new application layer network products have been released that help address new classes of threats, such as spam, phishing, spyware, packet abuse, and unauthorized point-to-point file sharing. Content security products such as Cisco IronPort Appliances provide comprehensive antivirus, antispware, file-blocking, antispam, URL blocking, and content-filtering services. These products supplement traditional firewalls and network-based intrusion detection system (NIDS) solutions with more granular traffic inspection services, thereby quarantining traffic so that it does not propagate throughout the network.

Denial-of-service (DoS) attack - Tries to overwhelm resources such as memory, CPU, and bandwidth, thus impacting the attacked system and denying legitimate users access.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition

QUESTION 157

Which types of communicating devices compose RMON architecture ?(choose two)

- A. Router
- B. Switch
- C. Management station
- D. Monitor

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

RMON

RMON is a standard monitoring specification that enables network monitoring devices and console systems to exchange network monitoring data. RMON provides more information than SNMP, but more sophisticated data collection devices (network probes) are needed. RMON looks at MAC- layer data and provides aggregate information on the statistics and LAN traffic.

Enterprise networks deploy network probes on several network segments; these probes report back to the RMON console. RMON allows network statistics to be collected even if a failure occurs between the probe and the RMON console. RMON1 is defined by RFCs 1757 and 2819, and additions for RMON2 are defined by RFC 2021.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 15

QUESTION 158

Which FCAPS function includes finding network problems that reduce availability?

- A. Security management
- B. Accounting management
- C. Fault management
- D. Performance management

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

The ISO defines five types of network management processes that are commonly known as FCAPS. These processes are as follows:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 15

QUESTION 159

What is the name of the organization that is in charge of creating the FCAPS architecture?

- A. ISP
- B. IOS
- C. ITU-T
- D. IEEE

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

FCAPS was actually created by the ISO not the ITU-T so if the above is a type-o than B is the correct answer. However, the ITU-T did refine FCAPS as stated below.

In the early 1980s the term FCAPS was introduced within the first Working Drafts (N1719) of ISO 10040, the Open Systems Interconnection (OSI) Systems Management Overview (SMO) standard. At that time the intention was to define five separate protocol standards, one for each functional area. Since initial experiences showed that these protocols would become very similar, the ISO working group responsible for the development of these protocols (ISO/TC97/SC16/WG4, later renamed into ISO-IEC/JTC1/SC21/WG4) decided to create a single protocol for all five areas instead. This protocol is called common management information protocol (CMIP). In the 1990s the ITU-T, as part of their work on Telecommunications Management Network (TMN), further refined the FCAPS as part of the TMN recommendation on Management Functions (M.3400). The idea of FCAPS turned out to be very useful for teaching network management functions; most text books therefore start with a section that explains the FCAPS.

QUESTION 160

Define some of the activities, tools, and techniques used in today's network-design process.(Choose three.)

- A. Analyzing network traffic
- B. Simulation of network traffic
- C. Network auditing
- D. Filtering incoming network traffic

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Characterizing the Existing Network

Characterizing the network is Step 2 of the design methodology. In this section, you learn to identify a network's major features, tools to analyze existing network traffic, and tools for auditing and monitoring network traffic.

Steps in Gathering Information

When arriving at a site that has an existing network, you need to obtain all the existing documentation.

Sometimes no documented information exists. You should be prepared to use tools to obtain information and get access to log in to the network devices to obtain information.

Here are the steps for gathering information:

When gathering exiting documentation, you look for site information such as site names, site addresses, site contacts, site hours of operation, and building and room access. Network infrastructure information includes locations and types of servers and network devices, data center and closet locations, LAN wiring, WAN technologies and circuit speeds, and power used. Logical network information includes IP addressing, routing protocols, network management, and security access lists used. You need to find out whether voice or video is being used on the network.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 1

QUESTION 161

Which is the remote monitoring agent in the RMON architecture called?

- A. Tree
- B. Station
- C. Agent
- D. Probe

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

RMON

RMON is a standard monitoring specification that enables network monitoring devices and console systems to exchange network monitoring data. RMON provides more information than SNMP, but more sophisticated data collection devices (network probes) are needed. RMON looks at MAC- layer data and provides aggregate information on the statistics and LAN traffic. Enterprise networks deploy network probes on several network segments; these probes report back to the RMON console. RMON allows network statistics to be collected even if a failure occurs between the probe and the RMON console. RMON1 is defined by RFCs 1757 and 2819, and additions for RMON2 are defined by RFC 2021.

The RMON MIB is located at iso.org.dod.internet.mgt.mib.rmon or by the equivalent object descriptor, 1.3.6.1.2.1.16. RMON1 defines nine monitoring groups; each group provides specific sets of data. One more group is defined for Token Ring. Each group is optional, so vendors do not need to support all the groups in the MIB.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 15

QUESTION 162

Which type of DSL does residential service use?

- A. VDSL
- B. SDSL
- C. IDSL
- D. ADSL

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Digital Subscriber Line

Digital subscriber line (DSL) is a technology that provides high-speed Internet data services over ordinary copper telephone lines. It achieves this by using frequencies that are not used in normal voice telephone calls.

The term xDSL describes the various competing forms of DSL available today.

ADSL is the most popular DSL technology and is widely available. The key to ADSL is that the downstream bandwidth is asymmetric or higher than the upstream bandwidth. Some limitations include that ADSL can be used only in close proximity to the local DSLAM, typically less than 2 km. The local DSLAM, or digital subscriber line access multiplexer, allows telephone lines to make DSL connections to the Internet. Download speeds usually range from 768 kbps to 9 Mbps, and upload speeds range from 64 kbps to 1.5 Mbps. The customer premises equipment (CPE) refers to a PC along with DSL modem or DSL router that connects back to the network access provider (NAP) DSLAMs.

The ADSL circuit consists of a twisted-pair telephone line that contains their information channels:

DSL splitters are used to separate basic telephone service from the ADSL modem/router to provide service even if the ADSL signaling fails.

Although DSL is primarily used in the residential community, this technology can also be used as a WAN technology for an organization. However, keep in mind that because this is a public network connection over the Internet, it is recommended that this technology be used in conjunction with a firewall/VPN solution back into your corporate enterprise network. The high speeds and relatively low cost make this a popular Internet access WAN technology.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 6

QUESTION 163

Which item is not a part of the process recommended by Cisco for WAN designs?

- A. Characterize the existing network.
- B. Analyze customer requirements.
- C. Configure deployed services.
- D. Design the new WAN topology.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 164

In IS-IS networks, which routers does the backup designated router (BDR) form adjacencies to?

- A. Only to the DR.

- B. The BDR only becomes adjacent when the DR is down.
- C. To all routers.
- D. There is no BDR in IS-IS.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

BDRs are used by OSPF and NOT IS-IS. IS-IS uses L1 and L2 routers. A backup designated router (BDR) is a router that becomes the designated router if the current designated router has a problem or fails. The BDR is the OSPF router with second highest priority at the time of the last election.

QUESTION 165

What does Compressed Real-Time Transport Protocol (cRTP) compress ?

- A. RTP, TCP, and IP headers
- B. RTP headers
- C. RTP, User Datagram Protocol (UDP), and IP headers
- D. Real-Time Transport Control Protocol (RTCP) headers

Correct Answer: C

Section: (none)

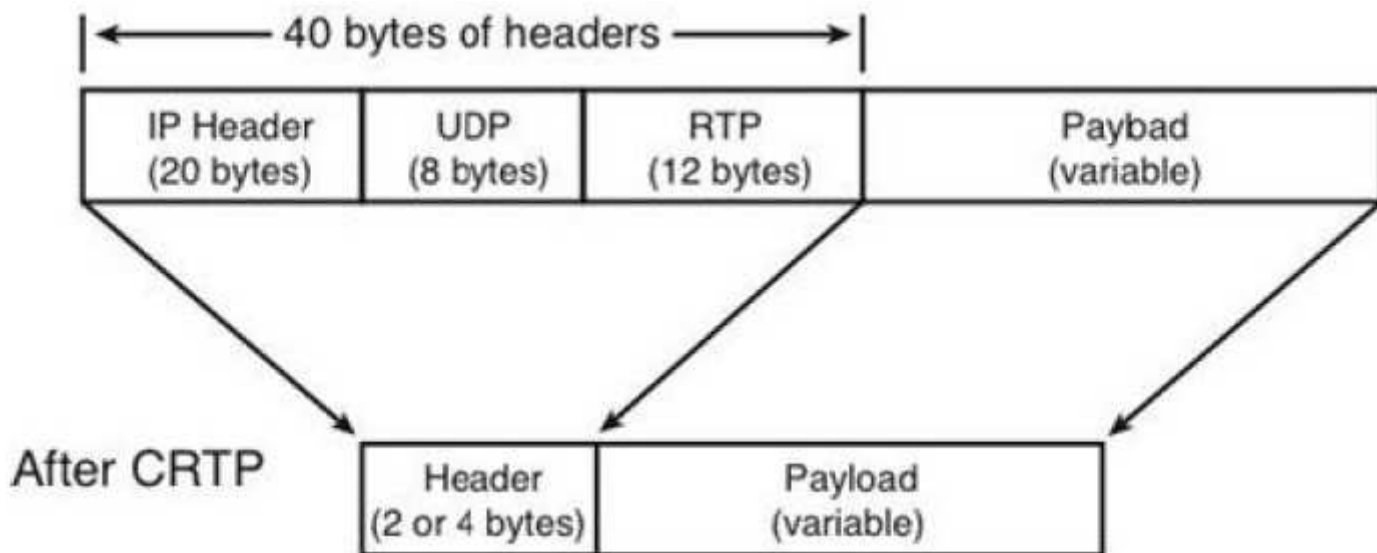
Explanation

Explanation/Reference:

Explanation:

WAN links use RTP header compression to reduce the size of voice packets. This is also called Compressed RTP (cRTP), which is defined in RFC 2508. As shown in Figure 14-18, cRTP reduces the IP/UDP/RTP header from 40 bytes to 2 or 4 bytes (a significant decrease in overhead). cRTP happens on a hop-by-hop basis, with compression and decompression occurring on every link. It must be configured on both ends of the link. It is recommended for slow links up to 768 kbps. cRTP is not used much anymore because slow WAN link bandwidths are seen less. Higher speed links are not recommended because of the high CPU requirements and they reduce call quality.

Figure 14-18. cRTP



Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 14

QUESTION 166

Which mechanism will be often used by service providers to define their service offerings and to differentiate their services from their competitors?

- A. SLM
- B. SLA
- C. SLC
- D. SAA

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Service Level Manager: The SLM Collection Manager 2.0 bundled product is part of the CiscoWorks2000 Service Management Solution (SMS). The CiscoWorks2000 SMS enables IT managers to establish and validate Service Level Agreements (SLAs) for their Cisco-based networks. The SLM Collection Manager (also referred to as the remote CM), is a distributable software agent designed to perform job management, data collection, and aggregation of performance data needed for network management applications. This in turn enables the Service Assurance Agent (SA Agent) testing in the Cisco IOS software to validate that SLAs are being met. Customers can scale their SMS by deploying additional remote CMs as required.

http://www.cisco.com/en/US/products/sw/cscowork/ps2428/products_quick_start09186a0080108a_46.html

Service level agreement (SLA): Defines the availability of the network. Networked applications rely on the underlying network between the client and server to provide its functions. There are multiple levels of application availability that can be part of a negotiated SLA with a service provider. Organizations have to work with the carrier to define what level of service, such as bandwidth, allowed latency, and loss, is acceptable to the organization.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition

Service Assurance Agent: The SA Agent is an both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS release 11.2. The feature allows you to monitor

network performance between a Cisco router and a remote device (which can be another Cisco router, an IP host, or a mainframe host) by measuring key Service Level Agreement (SLA) metrics such as response time, network resources, availability, jitter, connect time, packet loss, and application performance. This feature enables you to perform troubleshooting, problem analysis, and notification based on the statistics collected by the SA Agent.

http://www.cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/1dt_saa.html

QUESTION 167

What is the virtual information store used within SNMP called?

- A. MIB
- B. RMON
- C. Protocol data unit (PDU)
- D. Abstract Syntax Notation One (ASN.1)

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

MIB

A Management Information Base (MIB) is a collection of information that is stored on the local agent of the managed device. MIBs are organized hierarchically and are accessed by the NMS. MIBs are databases of objects organized in a tree-like structure, with each branch containing similar objects. Each object has a unique object identifier (number) that uniquely identifies the managed object of the MIB hierarchy. Read and write community strings are used to control access to MIB information.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 15

QUESTION 168

Which standard language will be used by SNMP to define the device information to be stored?

- A. SNMPv4
- B. ASN.1
- C. MIBs
- D. Agents

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Each individual manageable feature in the MIB is called a MIB variable. The MIB module is a document that describes each manageable feature that is contained in an agent. The MIB module is written in Abstract Syntax Notation 1 (ASN.1). Three ASN.1 data types are required: name, syntax, and encoding. The name serves as the object identifier. The syntax defines the object's data type (integer or string). The encoding data describes how information associated with a managed object is formatted as a series of data items for transmission on the network. Some examples of standard managed objects that can be obtained from the MIB tree are as follows:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 15

QUESTION 169

Which WAN scenario might be appropriate for queuing solutions?

- A. A newly implemented WAN connection has yet to demonstrate sufficient WAN statistics for congestion-level tracking.
- B. A WAN connection features consistent congestion problems, and data transfers often suffer.
- C. A WAN connection is rarely congested, and data transfers never suffer.
- D. A WAN connection features occasional periods of congestion, and data transfers have occasionally suffered as a result.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 170

Your boss is interested in a wireless WAN solution which provides higher bandwidth than point-to-multipoint (p2mp) wireless. Which description is correct?

- A. Service providers cannot install point-to-point (p2p) links from a p2mp hub.
- B. P2p wireless connections can provide up to 44 Mbps raw bandwidth.
- C. P2p links tend to be slower than p2mp.
- D. P2mp wireless connections can provide up to 1.544 Mbps raw bandwidth.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 171

Examine the following protocols, which two are used for IP Security?

- A. Generic Routing Encapsulation (GRE) and Internetwork Packet Exchange (IPX)(EIGRP)
- B. Border Gateway Protocol (BGP) and Enhanced Interior Gateway Routing Protocol
- C. Authentication Header (AH) and Encapsulating Security Payload (ESP)
- D. Virtual Private Dial-Up Network (VPDN) and GRE

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

VPN Protocols	
VPN Description	VPN Name
Use AH and ESP to secure data; requires endpoints have IPsec software	Standard IPsec
Secure encrypted point-to-point GRE tunnels; on-demand spoke to spoke connectivity	Cisco DMVPN
Simplifies hub-and-spoke VPNs; need to reduce VPN management	Cisco Easy VPN
Enables routing and multicast traffic across an IPsec VPN; non-IP protocol and QoS support	Cisco GRE-based VPN
Encryption integration on IP and MPLS WANs; Simplifies encryption management using group keying; Any-to-any connectivity	Cisco GET VPN

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 12

QUESTION 172

What is SNMP?

- A. Simple Network Management Protocol
- B. Simple Network Monitoring Protocol
- C. Sampling Network Management Process
- D. Simple Network Maintenance Procedure

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an IP application layer protocol that has become the standard for the exchange of management information between network devices. SNMP was initially described in RFC 1157. It is a simple solution that requires little code to implement, which allows vendors to build SNMP agents on their products. SNMP runs over User Datagram Protocol (UDP) and therefore does not inherently provide for sequencing and acknowledgment of packets, but it still reduces the amount of overhead used for management information.

SNMP Components

SNMP has three network-managed components:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 15

QUESTION 173

When building Global network businesses , which three principles should be used?

- A. Customer focus, continuous standardization, and core versus context
- B. Customer focus, centralization, and core versus context
- C. Customer focus, decentralization, and core versus edge
- D. Customer focus, decentralization, and core versus context

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 174

For the following items, which component of the CiscoWorks product allows a network administrator to define and manage service levels?

- A. Service assurance agent (SAA)
- B. Service level manager (SLM)
- C. Collection Manager (CM)
- D. Service level agreement (SLA)

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Service Level Manager: The SLM Collection Manager 2.0 bundled product is part of the CiscoWorks2000 Service Management Solution (SMS). The CiscoWorks2000 SMS enables IT managers to establish and validate Service Level Agreements (SLAs) for their Cisco-based networks. The SLM Collection Manager (also referred to as the remote CM), is a distributable software agent designed to perform job management, data collection, and aggregation of performance data needed for network management applications. This in turn enables the Service Assurance Agent (SA Agent) testing in the Cisco IOS software to validate that SLAs are being met. Customers can scale their SMS by deploying additional remote CMs as required.

http://www.cisco.com/en/US/products/sw/cscowork/ps2428/products_quick_start09186a0080108a_46.html

QUESTION 175

NAT-PT is an IPv6-IPv4 translation mechanism. What is NAT-PT?

- A. Network address translation?ìCport translation; translates RFC 1918 addresses to public IPv4 addresses
- B. Network address translation-protocol translation; translates between IPv4 and IPv6 addresses
- C. Next address translation?ìCport translation
- D. Network addressable transparent-port translation; translates network addresses to ports

Correct Answer: B

Section: (none)

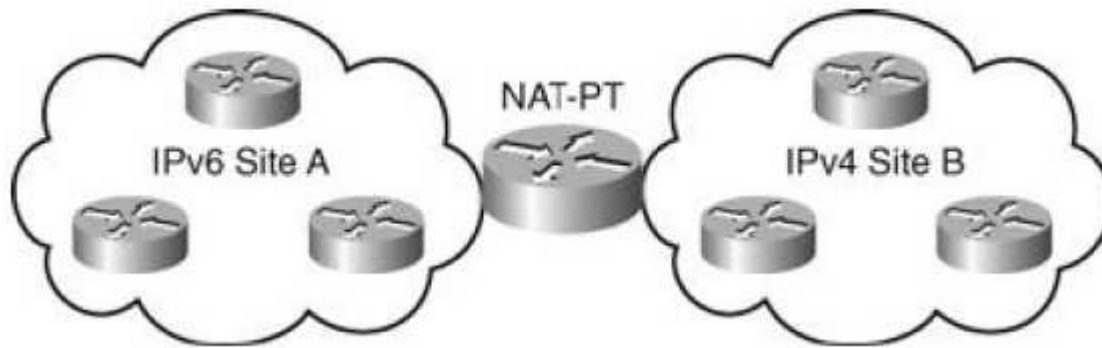
Explanation

Explanation/Reference:

Explanation: Explanation

RFC 2766 describes NAT-PT, which provides translation between IPv6 and IPv4 hosts. NAT-PT operates similarly to the NAT mechanisms to translate IPv4 private addresses to public address space. NAT-PT binds addresses in the IPv6 network to addresses in the IPv4 network and vice versa. Figure 9-12 shows a network using NAT-PT. RFC 4699 is a recent Informational RFC that recommends that NAT-PT be placed into historical status and recommends against its use (although the protocol is still supported in IOS).

Figure 9-12. Network Address Translation-Protocol Translation



Cisco also introduces the Cisco 6PE for Multiprotocol Label Switching (MPLS) service providers. Cisco 6PE allows IPv6 islands to communicate over an MPLS/IPv4 core network using MPLS label-switched paths (LSP). The Cisco 6PE routers are dual stack. The method relies on BGP extensions in the IPv4 6PE routers to exchange IPv6 reachability information, along with an MPLS label for each IPv6 address prefix announced.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 9

QUESTION 176

What Cisco router configuration component does an implementer use to create a floating static route?

- A. Primary interface
- B. Administrative distance
- C. Loopback
- D. Description

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Often, backup links use a different technology. For example, a leased line can be in parallel with a backup dialup line or ISDN circuit. However, it is more common to use DSL lines as backup in today's networks. By using floating static routes, you can specify that the backup route have a higher administrative distance (used by Cisco routers to select routing information) so that it is not normally used unless the primary route goes down. This design is less available than the partial mesh presented previously. Typically, on-demand backup links reduce WAN charges.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 2

QUESTION 177

Which Cisco proprietary protocol will be used in LAN switches to control multicast traffic at the data link layer within a LAN switch?

- A. MAC filters
- B. Cisco Group Management Protocol (CGMP)
- C. Cisco Discovery Protocol (CDP)
- D. IGMP

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

CGMP

Cisco Group Management Protocol is a Cisco proprietary protocol implemented to control multicast traffic at Layer 2. Because a Layer 2 switch is unaware of Layer 3 IGMP messages, it cannot keep multicast packets from being sent to all ports.

With CGMP, the LAN switch can speak with the IGMP router to find out the MAC addresses of the hosts that want to receive the multicast packets. You must also enable the router to speak CGMP with the LAN switches. With CGMP, switches distribute multicast sessions to the switch ports that have group members.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 3

QUESTION 178

A common response to an attack by this device can be either to send an alert or to take corrective action. What is this device?

- A. Vulnerability assessment
- B. Firewall
- C. Intrusion-detection system (IDS)
- D. Router

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Intrusion Detection System Overview Summary

Network-based IDS relies on the use of network sensors strategically placed throughout the network. These probes monitor and analyze all network traffic traversing the local network. Network traffic is compared to a signature database or a defined profile to detect intrusive activity. If the monitored traffic matches a profile or signature, an alarm is generated. Additionally, sensors can be configured to take corrective action to stop an attack once it's been detected. The advantage to a network-based IDS is its macro view of the network. A network-based IDS has the advantage of viewing the entire network and, therefore, isn't limited to viewing only the traffic to a single host. The drawback to a network-based IDS is its cost. A network-based IDS relies on additional hardware in the form of network probes. Additional drawbacks to network-based IDS are the following:

Although different types of IDS systems exist, each type must support at least one triggering mechanism. Triggering mechanisms are simply how an alarm is generated. There are two types of triggering mechanisms: Anomaly-based systems use profiles created by the IDS or the security administrator. These profiles are then used to detect an attack and generate an alarm. Traffic patterns or computer activity that doesn't match a defined profile generates an alert. The advantage of anomaly detection is it has the capability to detect previously unknown attacks or new types of attacks. The drawback to anomaly detection is an alarm is generated any time traffic or activity deviates from the defined "normal" traffic patterns or activity. This means it's up to the security administrator to discover why an alarm was generated. Anomaly-based systems have a higher rate of false positives because alarms are generated any time a deviation from normal occurs. Defining normal traffic and activity can be a difficult and time-consuming task.

<http://www.ciscoarticles.com/CCSP-Cisco-Certified-Security-Professional/Intrusion-Detection-System-Overview-Summary.html>

QUESTION 179

How many more bits does IPv6 use for addresses than IPv4?

- A. 32
- B. 64
- C. 96
- D. 128

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

IPv6 uses 128-bit addresses rather than the 32-bit addresses in IPv4. This supports more address hierarchy levels and uses simpler address autoconfiguration.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 9

QUESTION 180

Which protocol will be used to exchange IP routes between autonomous systems?

- A. eBGP
- B. IGMP
- C. IGRP
- D. OSPF

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

BGP Neighbors

BGP is usually configured between two directly connected routers that belong to different autonomous systems. Each autonomous system is under different technical administration. BGP is frequently used to connect the enterprise to service providers and to interconnect service providers. The routing protocol within the enterprise could be any Interior Gateway Protocol (IGP). Common IGP choices include RIPv2, EIGRP, OSPF, IS-IS. BGPv4 is the only deployed Exterior Gateway Protocol (EGP).

BGP is an interdomain routing protocol that allows BGP speakers residing in different autonomous systems to exchange routing (NLRI) information. An autonomous system is a collection of devices under common administration. BGP autonomous systems range from 1 through 65,535. Autonomous system numbers (ASN) 1 through 64,511 are considered public ASNs. These are allocated by IANA to Regional Internet Registries (RIR). Entities wanting to receive an ASN must complete the application process of their local RIR and be approved before being assigned an ASN. ASNs 65,512 through 65,535 are considered private ASNs. These ASNs can be used by any organization, but, like RFC 1918 addresses, cannot be used on the Internet.

Before two BGP routers can exchange routing updates, they must become established neighbors. After BGP routers establish a TCP connection, exchange information, and accept the information, they become established neighbors and start exchanging routing updates. If the neighbors do not reach an established state, they do not exchange BGP updates. The information exchanged before the neighbors are established includes the BGP version number, ASN, BGP router ID, and BGP capabilities.

eBGP

External Border Gateway Protocol is the term used to describe BGP peering between neighbors in different autonomous systems. As required by RFC 1771, the eBGP peers share a common subnet (although Cisco does allow some flexibility to avoid doing so). In Figure 11-9, all routers speak eBGP with routers in other autonomous systems. Within autonomous system 500, the routers communicate using iBGP, which is covered

next.

iBGP

Internal Border Gateway Protocol is the term used to describe the peering between BGP neighbors in the same autonomous system. iBGP is used primarily in transit autonomous systems. Transit autonomous systems forward traffic from one external autonomous system to another external autonomous system. 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. Normally, the number of eBGP routes is too large for an IGP to handle.

iBGP provides a better way to control the routes within the transit autonomous system. With iBGP, the external route information (attributes) is forwarded. The various IGPs that might be used do not understand or forward BGP attributes, including autonomous system paths, between eBGP routers.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 11

QUESTION 181

What does the Cisco security architecture called SAFE stand for?

- A. Security Architecture for Enterprise
- B. Standard Assessment for Enterprise
- C. Security Analysis for Enterprise
- D. Standard Architecture for Enterprise

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Cisco SAFE Architecture

Cisco Security Architecture for the Enterprise (SAFE) is a security reference architecture that provides detailed design and implementation guidelines to assist in the development of secure and reliable networks. Part of the SAFE architecture discusses the building blocks of secure networks that are resilient to well-known and new forms of attack. Because enterprise networks are key enablers of business, networks must be designed with integrated security in mind to ensure confidentiality, integrity, and availability of network resources, especially those networks that support critical business activity.

One key principle of Cisco SAFE architecture relates to the need for deep security and protection from both the inside and outside of the organization, along with providing guidelines for analyzing security requirements. The Cisco SAFE approach allows for the analysis of expected threats and supports the design of the network security strategy. In addition, the modular nature of Cisco SAFE allows for the security system to be expanded and scaled as the business grows.

Here are the goals of Cisco SAFE:

Here are the benefits of Cisco SAFE:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 13

QUESTION 182

You are a network technician, can you tell me how many IP addresses are available for hosts in the subnet 198.10.100.64/27?

- A. 62
- B. 30
- C. 126
- D. 14

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Dotted Decimal	Bit Mask	Hexadecimal	Hosts
255.0.0.0	/8	FF000000	16,777,214
255.192.0.0	/10	FFC00000	4,194,302
255.255.0.0	/16	FFFF0000	65,534
255.255.224.0	/19	FFFFE000	8,190
255.255.240.0	/20	FFFFF000	4,094
255.255.255.0	/24	FFFFFFF0	254
255.255.255.128	/25	FFFFFFF8	126
255.255.255.192	/26	FFFFFFC0	62
255.255.255.224	/27	FFFFFFE0	30
255.255.255.240	/28	FFFFFFF0	14
255.255.255.248	/29	FFFFFFF8	6
255.255.255.252	/30	FFFFFFFC	2
255.255.255.255	/32	FFFFFFFF	0

QUESTION 183

Which two encryption transforms will be used by both ESP and AH for authentication?

- A. HMAC-MD5 or Hash Message Authentication Code-Secure Hash Algorithm-1(HMAC-SHA-1)
- B. DES or 3DES
- C. DES or Hash Message Authentication Code-Message Digest 5 (HMAC-MD5)
- D. 3DES or MD5

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

The IPsec protocols include Internet Security Association and Key Management Protocol (ISAKMP), and two other IPsec IP protocols: Encapsulating Security Payload (ESP) and Authentication Header (AH). IPsec uses symmetrical encryption algorithms to provide data protection. These algorithms need a secure method to exchange keys to ensure that the data is protected. Internet Key Exchange (IKE) ISAKMP protocols provide these functions. ESP is used to provide confidentiality, data origin authentication, connectionless integrity, and anti-replay services. AH is used to provide integrity and data origin authentication, usually referred to as just authentication.

In addition, IPsec can secure data from eavesdropping and modification using transforms sets, which give you varying levels of strength for the data protection. IPsec also has several Hash Message Authentication Codes (HMAC) available to provide protection from attacks such as man-in-the-middle, packet-replay, and data-integrity attacks.

A compliant ESP implementation MUST support the following mandatory-to-implement algorithms:

<http://www.ietf.org/rfc/rfc2406.txt>

A compliant AH implementation MUST support the following mandatory-to-implement algorithms:

<http://www.ietf.org/rfc/rfc2402.txt>

QUESTION 184

For the following options, which emerging WAN technology uses DSL coding and digital modulation techniques with Ethernet?

- A. Cable
- B. Wireless
- C. SMDS
- D. Long-Reach Ethernet (LRE)

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Long Reach Ethernet (LRE) was a proprietary networking protocol developed by Cisco Systems, intended to support multi-megabit (5 to 15 Mbit/s) performance over telephone-grade Category 1/2/3 wiring over distances up to 5,000 feet (1.5 km). Supporting such great distances, LRE is technically classified a Metropolitan area network (MAN) technology. Technically the protocol was similar to VDSL.

The technology was sometimes referred to as Ethernet in the First Mile (EFM). Several networking vendors offered compatible networking hardware, but the technology became obsolete. Like standard VDSL, LRE allowed existing telephone wiring that connects an organization's offices to be used to network those offices together using standard Ethernet protocol without incurring the huge cost of deploying fiber optic cable or limiting organizations to the bandwidth provided by modems or xDSL devices.

Other sample applications included Ethernet access to hotel rooms or college dormitories over existing installed telephone wiring.

LRE was compatible with VDSL ETSI Band Plan 998.

LRE sold Cisco Catalyst model 2900 switches using Infineon PEF22822/PEB22811 VDSL QAM (10Base-S) chipset like many other VDSL concentrators. Cisco announced end-of-sale for the LRE products in October 2006, and its explanation page was removed from their web site in 2007. VDSL is a comparable or better solution.

QUESTION 185

What is SLC?

- A. Standard level contracts
- B. Standard level configuration
- C. Service level contracts
- D. Service level configuration

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

SLA Defined

A service-level agreement is a key component of a service-level contract (SLC). The SLC specifies connectivity and performance agreements for an end-user service from a provider of service. The service provider could be within the enterprise--for example the IS organization could be the service provider to internal departments--or an external company such as an ISP providing wide-area or hosted application services.

The SLC typically includes multiple SLAs. A violation of any particular SLA could create a violation of the overall SLC. The service-level management solution needs to provide a means of managing collections of agreements that constitute a contract with the service provider. The solution should enable the user to monitor multiple SLCs individually, drill down into SLA details, and monitor the percentage of SLA conformance for a given SLC.

For example, an SLC for connectivity from several branch sites to the central site may read "a connection of 64 Kbps at a latency of no greater than 100 milliseconds averaged over one hour, and an availability of 99.9 percent is to be provided." The constituent SLAs would be:

QUESTION 186

What does ODR stand for?

- A. Open default routing
- B. Optical demand routing
- C. Open dedicated routing
- D. On-demand routing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

On-Demand Routing (ODR) is an enhancement to Cisco Discovery Protocol (CDP), a protocol used to discover other Cisco devices on either broadcast or non-broadcast media. With the help of CDP, it is possible to find the device type, the IP address, the Cisco IOS® version running on the neighbor Cisco device, the capabilities of the neighbor device, and so on. In Cisco IOS software release 11.2, ODR was added to CDP to advertise the connected IP prefix of a stub router via CDP. This feature takes an extra five bytes for each network or subnet, four bytes for the IP address, and one byte to advertise the subnet mask along with the IP. ODR is able to carry Variable Length Subnet Mask (VLSM) information

QUESTION 187

Observe the following options, in which section of the network document does Cisco recommend a discussion of performance, scalability, capacity, security, and traffic needs?

- A. Design summary
- B. Design solution
- C. Executive summary
- D. Design requirements

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 188

In telephony, the local loop is the physical link or circuit. Where is the local loop located?

- A. Between the loopback interfaces of two VoIP routers

- B. Between phones and the central office (CO) switch
- C. Between two PBXs
- D. Between two PSTN switches

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The local loop is the pair of wires that runs from the CO to the home or business office.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 14

QUESTION 189

Which advantage is of security systems that are part of the Cisco ecosystem?

- A. There is a suite of products to choose from.
- B. Various partners as well as supporting products increase the effectiveness of security systems.
- C. There are no advantages.
- D. The Cisco ecosystem ensure that partners can implement the solution.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

The Cisco Service Provider ecosystem was created to help Cisco, and our Service Provider customers capitalize on the huge market opportunities created by the circuit to packet transition. We have a strong community of best in class technology development and deployment partners that enable service providers to deploy innovative new services on their new or existing networks. Cisco partners with System Integrators, Network Integrators and Independent Software Vendors (ISVs) who are leaders in Operations Support Systems and Business Support Systems to help Service Provider customers better manage and leverage their networks and support systems.

The Ecosystem Advantages

No single vendor can possibly offer service providers the choice and flexibility that a horizontally structured network of Ecosystem partners can provide.

Ecosystem partners are chosen because of their expertise in the service provider OSS environment. They may be independent software vendors (ISVs) providing functional blocks such as billing or fault management, or Systems Integrators who integrate, design and deploy OSS solutions, or even infrastructure companies who sit right at the very heart of the network in terms of cabling and electronic provisioning.

All Ecosystem partners across EMEA are subject to vigorous interoperability testing, not only with Cisco hardware and software, but also with complementary products and applications provided by other Ecosystem members. Once testing has been successfully completed, a particular product or application is given the Cisco Verified Interoperability Product (VIP) Mark that distinguishes it in the market place.

Interoperability testing is also product or application revision-specific in order to maintain the highest levels of compatibility and is required before each version of the partner product release receives the Cisco VIP Mark.

A key area for Cisco and its Ecosystem partners is the ability to demonstrate sufficient pre and post sales support for all qualifying products and services. All EMEA Ecosystem partners have to satisfy Cisco's stringent requirements before they can be classed as true EMEA-wide partners. In order to maintain this level of support, all Ecosystem partners are accredited by 'theatre' - EMEA, Asia Pacific, Latin America and Northern America. Only if all theatre requirements are met can any partner be truly classified as Global. In the same way that Cisco prides itself on its commitment to ethical practices across all areas of business, Ecosystem partners are required to adhere to clearly defined best practices with regard to all customer engagements. It is with confidence that service providers can be sure that the service and commitment levels from any of Cisco's Ecosystem partners will be supplied to the highest standards possible.

QUESTION 190

What is ASBR short for?

- A. Area Border Router
- B. Auxiliary System Border Router
- C. Area System Border Router
- D. Autonomous System Boundary Router

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

ASBR (Autonomous System Boundary Router) - Connects the OSPF backbone to external networks. Routers that inject external LSAs into the OSPF database (redistribution).

Table, Major LSA Types

Type

Description

Internal Router

Any router whose interfaces all belong to the same OSPF area. These routers keep only one link-state database.

ABR

Routers that are connected to more than one area. These routers maintain a link-state database for each area they belong to. These routers generate summary LSAs.

ASBR

Routers that inject external LSAs into the OSPF database (redistribution). These external routes are learned via either other routing protocols or static routes.

Backbone router

Routers with at least one interface attached to Area 0.

Tip: An OSPF router can be an ABR, an ASBR, and a backbone router at the same time. The router is an ABR if it has an interface on Area 0 and another interface in another area. The router is a backbone router if it has one or more interfaces in Area 0. The router is an ASBR if it redistributes external routes into the OSPF network. Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 11

QUESTION 191

Area Border Router (ABR) is defined by which protocol?

- A. Enhanced Interior Gateway Routing Protocol (EIGRP)
- B. OSPF
- C. On-Demand Routing (ODR)
- D. IS-IS

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

ABR (Area Border Router) - Routers that connect to more than one OSPF area

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition

QUESTION 192

Which queuing mechanism establishes four interface output queues that will be used for traffic scheduling?

- A. Priority queuing (PQ)
- B. First-in, first-out (FIFO)
- C. Weighted fair queuing (WFQ)
- D. Custom queuing (CQ)

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Congestion Management

Two types of output queues are available on routers: the hardware queue and the software queue. The hardware queue uses the strategy of first in, first out (FIFO). The software queue schedules packets first and then places them in the hardware queue. Keep in mind that the software queue is used only during periods of congestion. The software queue uses QoS techniques such as priority queuing, custom queuing, weighted fair queuing, class-based weighted fair queuing, low-latency queuing, and traffic shaping and policing.

Priority Queuing

Priority queuing (PQ) is a queuing method that establishes four interface output queues that serve different priority levels: high, medium, default, and low. Unfortunately, PQ can starve other queues if too much data is in one queue because higher-priority queues must be emptied before lower-priority queues.

Custom Queuing

Custom queuing (CQ) uses up to 16 individual output queues. Byte size limits are assigned to each queue so that when the limit is reached, it proceeds to the next queue. The network operator can customize these byte size limits. CQ is fairer than PQ because it allows some level of service to all traffic. This queuing method is considered legacy due to the improvements in the queuing methods.

Weighted Fair Queuing

Weighted fair queuing (WFQ) ensures that traffic is separated into individual flows or sessions without requiring that you define ACLs. WFQ uses two categories to group sessions: high bandwidth and low bandwidth. Low-bandwidth traffic has priority over high-bandwidth traffic. High-bandwidth traffic shares the service according to assigned weight values. WFQ is the default QoS mechanism on interfaces below 2.0 Mbps.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 6

QUESTION 193

Which option is not valid for using the public Internet as a backup WAN medium?

- A. IP Security (IPSec) tunnels
- B. Shared PVC
- C. IP routing without constraints
- D. Generic Routing Encapsulation (GRE) tunnels

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

The Internet as a WAN Backup Technology

This section describes the Internet as an alternative option for a failed WAN connection. This type of connection is considered best-effort and does not guarantee any bandwidth. Common methods for connecting noncontiguous private networks over a public IP network include the following:

The following sections describe these methods.

Routing Without Constraints

When relying on the Internet to provide a backup for branch offices, a company must fully cooperate with the ISP and announce its networks. The backup network--the Internet--therefore becomes aware of the company's data, because it is sent unencrypted.

Layer 3 Tunneling with GRE and IPsec

Layer 3 tunneling uses a Layer 3 protocol to transport over another Layer 3 network. Typically, Layer 3 tunneling is used either to connect two noncontiguous parts of a non-IP network over an IP network or to connect two IP networks over a backbone IP network, possibly hiding the IP addressing details of the two networks from the backbone IP network. Following are the two Layer 3 tunneling methods for connecting noncontiguous private networks over a public IP network:

GRE enables simple and flexible deployment of basic IP VPNs. Deployment is easy; however, tunnel provisioning is not very scalable in a full-mesh network because every point-to-point association must be defined separately. The packet payload is not protected against sniffing and unauthorized changes (no encryption is used), and no sender authentication occurs.

Using GRE tunnels as a mechanism for backup links has several drawbacks, including administrative overhead, scaling to large numbers of tunnels, and processing overhead of the GRE encapsulation.

Following are some features of IPsec:

Authorized Self-Study Guide Designing for Cisco Internetwork Solutions (DESGN), Second Edition

QUESTION 194

For the following items, which is an SP Edge module in the Enterprise Composite Network model?

- A. Core layer
- B. Edge distribution
- C. Public Switched Telephone Network (PSTN) service
- D. Server farm

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Service Provider Edge Module

The SP edge module, shown in Figure 2-12, consists of SP edge services such as the following:



Figure, WAN/Internet SP Edge Module

Enterprises use SPs to acquire network services. ISPs offer enterprises access to the Internet. ISPs can route the enterprise's networks to their network and to upstream and peer Internet providers. Some ISPs can provide Internet services with DSL access. Connectivity with multiple ISPs was described in the section, "Internet Edge."

For voice services, PSTN providers offer access to the global public voice network. For the enterprise network, the PSTN lets dialup users access the enterprise via analog or cellular wireless technologies. It is also used for WAN backup using ISDN services.

WAN SPs offer MPLS, Frame Relay, ATM, and other WAN services for enterprise site-to-site connectivity with permanent connections.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 2

QUESTION 195

Which method will be used to secure a network against man-in-the-middle attack?

- A. Two-factor authentication
- B. Management module
- C. Encryption

D. Firewall

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 196

What is important for the top-down design concept?

- A. Engagement of the HR representatives during the design process
- B. Engagement of the top executives during the design process
- C. Engagement of the employees working on the top floors in the building during the design process
- D. Engagement of the top executives once the design process is finalized

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 197

Which one of the following QoS mechanisms is recommended for VoIP networks?

- A. Low-latency queuing (LLQ)
- B. Switched-based queuing
- C. Fast queuing
- D. Custom queuing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Low-Latency Queuing

Low-latency queuing (LLQ) adds a strict priority queue (PQ) to CBWFQ. The strict PQ allows delay sensitive traffic such as voice to be sent first, before other queues are serviced. That gives voice preferential treatment over the other traffic types. Unlike priority queuing, LLQ provides for a maximum threshold on the PQ to prevent lower priority traffic from being starved by the PQ.

Without LLQ, CBWFQ would not have a priority queue for real-time traffic. The additional classification of other traffic classes is done using the same CBWFQ techniques. LLQ is the standard QoS method for many VoIP networks.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 6

QUESTION 198

In which layer of the OSI model does Real-Time Transport Protocol (RTP) operate ?

- A. Network
- B. Application

- C. Transport
- D. Session

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

OSI MODEL, LAYERS & PROTOCOLS

7 Application

Web Browser, Email, Print Services, SIP, SSH and SCP, NFS, RTSP, Feed, XMPP, Whois, SMB; DNS; FTP; TFTP; BOOTP; SNMP; RLOGIN; SMTP; MIME; NFS; FINGER; TELNET; NCP; APPC; AFP; SMB

6 Presentation

XDR, ASN.1, SMB, AFP, NCP, MIDI, HTML, GIF, TIFF, JPEG, ASCII, EBCDIC

5 Session

TLS, SSH, X.225, RPC, NetBIOS, ASP, Winsock, BSD

4 Transport

TCP, UDP, RTP, SCTP, SPX, ATP

Gateway, Advanced Cable Tester, Brouter

3 Network

IP, ICMP, IGMP, BGP, OSPF, RIP, IGRP, EIGRP, ARP, RARP, X.25, NETBEUI Brouter, Router, Frame Relay Device, ATM Switch, Advanced Cable Tester, DDP 2 Data Link

Ethernet, Token ring, StarLAN, HDLC, Frame relay, ISDN, ATM, 802.11 WiFi, FDDI, PPP, Bridge, Switch, ISDN Router, Intelligent Hub, NIC, Advanced Cable Tester, ARCNET, LocalTalk, FDDI, ATM. NIC Drivers: Open Datalink Interface (ODI), Network Independent Interface Specification (NDIS)

1 Physical

NIC, Twisted Pair, Coax, Fiber Optic, Wireless Media, Repeater, Multiplexer, Hubs, (Passive/Active), TDR, Oscilloscope, Amplifier, Carrier pigeon

TCP LAYERS

4 Application (OSI - Layers 5 through 7)

HTTP, FTP, DNS

(Routing protocols like BGP and RIP, which for a variety of reasons run over TCP and UDP respectively, may also be considered part of the Internetwork layer)

3 Transport (OSI - Layers 4 and 5)

TCP, UDP, RTP, SCTP

(Routing protocols like OSPF, which run over IP, may also be considered part of the Internetwork layer)

2 Internetwork (OSI - Layer 3)

For TCP/IP this is the Internet Protocol (IP)

(Required protocols like ICMP and IGMP run over IP, but may still be considered part of the Internetwork layer; ARP does not run over IP)

1 Link (OSI - Layers 1 and 2)

Ethernet, Wi-Fi, MPLS, etc.

http://www.tomax7.com/aplus/osi_model.htm

QUESTION 199

Developing a network design according to layers such as core and distribution is an example of which type of design methodology?

- A. Flat design
- B. Top-down

- C. Hierarchical structured design
- D. PDIOO

Correct Answer: C

Section: (none)

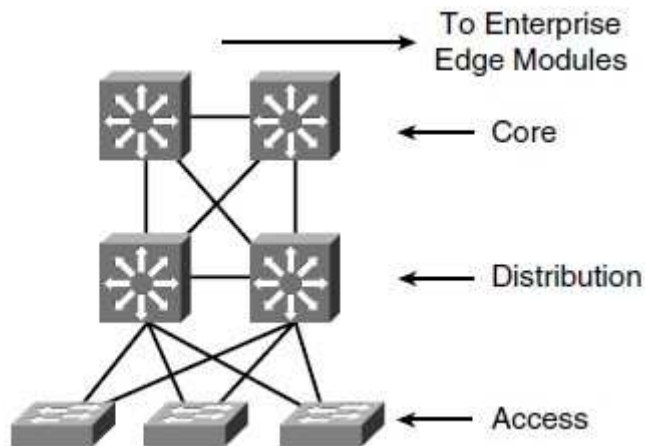
Explanation

Explanation/Reference:

Explanation: Explanation

Hierarchical Network Design

As shown in the figure, a traditional hierarchical LAN design has three layers:



Figure, Hierarchical Network Design Has Three Layers: Core, Distribution, and Access

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 2

QUESTION 200

Which parameters does the computation of the EIGRP composite metric use by default?

- A. Bandwidth and reliability
- B. Bandwidth and load
- C. Bandwidth and maximum transmission unit (MTU)
- D. Bandwidth and delay

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

EIGRP for IPv4 Summary

The characteristics of EIGRP for IPv4 networks follow:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 10

QUESTION 201

Which statement is true about WANs?

- A. Switches or concentrators often relay information through the WAN.
- B. WANs typically encompass broad geographic areas.
- C. In general, WAN technologies function at the middle three layers of the Open System Interconnection (OSI) model.
- D. Users of WANs do not typically own all transmission facilities.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

WAN Defined

Wide-area networks (WAN) are communications networks that are used to connect geographically dispersed network locations. Generally, WAN services are offered by service providers or telecommunication carriers. WANs can transport data, voice, and video traffic. Service providers charge fees, called tariffs, for providing WAN services or communications to their customers. Sometimes the term service is referred to as the WAN communications provided by the carrier.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 6

QUESTION 202

Which item is not a true disadvantage of the full-mesh topology?

- A. Central hub router represents a single point of failure in the network.
- B. High level of complexity to implement.
- C. Large number of packet replications required.
- D. High costs due to number of virtual circuits.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Full-Mesh Topology

With full-mesh topologies, each site has a connection to all other sites in the WAN cloud (any-to-any). As the numbers of sites grow, so does the number of spoke connections that are ultimately required. Consequently, the full-mesh topology is not viable in very large networks. However, a key advantage of this topology is that it has plenty of redundancy in the event of network failures. But redundancy implemented with this approach does have a high price associated with it.

Here are some issues inherent with full-mesh topologies:

The number of VCs required for a full mesh can be calculated using the formula $((N - 1) \times N / 2)$. For example if you have 4 sites, $((4 - 1) \times 4 / 2) = 6$ VCs are required.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition

QUESTION 203

Which IPv4 field are the precedence bits located in?

- A. IP destination address
- B. Type-of-service field
- C. IP options field

D. IP protocol field

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

ToS (Type of Service): This field is 8 bits in length. Quality of service (QoS) parameters such as IP precedence or DSCP are found in this field.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 8

QUESTION 204

Which hierarchical layer has functions such as High availability, port security, and rate limiting?

- A. Core
- B. Access
- C. Network
- D. Distribution

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Access Layer

The access layer provides user access to local segments on the network. The access layer is characterized by switched LAN segments in a campus environment. Microsegmentation using LAN switches provides high bandwidth to workgroups by reducing the number of devices on Ethernet segments. Functions of the access layer include the following:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 2

QUESTION 205

With which of the following capabilities does RIPv2 improve RIPv1?

- A. Multicast updates, authentication, variable-length subnet mask (VLSM)
- B. Authentication, VLSM, hop count
- C. Multicast updates, authentication, hop count
- D. Multicast updates, hop count

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

RIPv2 improves on RIPv1 with the ability to use VLSM, with support for route authentication, and with multicasting of route updates. RIPv2 supports CIDR. It still sends updates every 30 seconds and retains the 15-hop limit; it also uses triggered updates. RIPv2 still uses UDP port 520; the RIP process is responsible for checking the version number. It retains the loop-prevention strategies of poison reverse and counting to infinity. On Cisco routers, RIPv2 has the same administrative distance as RIPv1, which is 120. Finally, RIPv2 uses the IP address 224.0.0.9 when multicasting route updates to other RIP routers. As in RIPv1, RIPv2 by default

summarizes IP networks at network boundaries. You can disable autosummarization if required.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 10

QUESTION 206

Which is the maximum segment distance for Fast Ethernet over unshielded twisted-pair (UTP)?

- A. 285 feet
- B. 100 feet
- C. 500 feet
- D. 100 meters

Correct Answer: D

Section: (none)






Explanation

Explanation/Reference:

Explanation: Explanation

100BASE-TX

RJ-45 Wiring (TIA/EIA-568-B T568B)

Pin	Pair	Wire	Color
1	2	1	 white/orange
2	2	2	 orange
3	3	1	 white/green
4	1	2	 blue
5	1	1	 white/blue
6	3	2	 green
7	4	1	 white/brown
8	4	2	 brown

100BASE-TX is the predominant form of Fast Ethernet, and runs over two wire-pairs inside a category 5 or above cable (a typical category 5 cable contains 4 pairs and can therefore support two 100BASE-TX links). Like 10BASE-T, the proper pairs are the orange and green pairs (canonical second and third pairs) in TIA/EIA-568-B's termination standards, T568A or T568B.

These pairs use pins 1, 2, 3 and 6.

In T568A and T568B, wires are in the order 1, 2, 3, 6, 4, 5, 7, 8 on the modular jack at each end. The color-order would be green/white, green, orange/white, blue, blue/white, orange, brown/white, brown for T568A, and orange/white, orange, green/white, blue, blue/white, green, brown/white, brown for T568B.

Each network segment can have a maximum distance of 100 meters (328 ft). In its typical configuration,

100BASE-TX uses one pair of twisted wires in each direction, providing 100 Mbit/s of throughput in each direction (full-duplex). See IEEE 802.3 for more details. The configuration of 100BASE-TX networks is very similar to 10BASE-T. When used to build a local area network, the devices on the network (computers, printers etc.) are typically connected to a hub or switch, creating a star network. Alternatively it is possible to connect two devices directly using a crossover cable.

With 100BASE-TX hardware, the raw bits (4 bits wide clocked at 25 MHz at the MII) go through 4B5B binary encoding to generate a series of 0 and 1 symbols clocked at 125 MHz symbol rate. The 4B5B encoding provides DC equalization and spectrum shaping (see the standard for details). Just as in the 100BASE-FX case, the bits are then transferred to the physical medium attachment layer using NRZI encoding. However, 100BASE-TX introduces an additional, medium dependent sublayer, which employs MLT-3 as a final encoding of the data stream before transmission, resulting in a maximum "fundamental frequency" of 31.25 MHz. The procedure is borrowed from the ANSI X3.263 FDDI specifications, with minor discrepancies.

QUESTION 207

Which term accurately describes a specific measure of delay often used to describe voice and video networks?

- A. Jitter
- B. Flux
- C. Latency
- D. Reliability

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Table. Network Delays

Fixed Delay	Description
Propagation delay	6 ms per km. No solution
Serialization delay	Frame length/bit rate. A faster link and smaller packets help reduce.
Processing delay	Depends on codec used: coding, compression, and packetization. Add hardware DSPs.
Queuing delay	Variable packet sizes and number of packets. Use LLQ, CBWFQ, LFI.
Jitter	Caused by variable delay. Use dejitter buffers to make delay constant; design as much as possible for an uncongested network.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 14

QUESTION 208

Which layer is in charge of fast transport in the hierarchical network model?

- A. Network
- B. Distribution
- C. Access
- D. Core

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Table Cisco Enterprise Architecture Model

Explanation

Table Cisco Enterprise Architecture Mode

Cisco Enterprise Architecture Model	
Hierarchical Layer	Description
Core	<ul style="list-style-type: none"> • Fast transport • High reliability • Redundancy • Fault tolerance • Low latency and good manageability • Avoidance of slow packet manipulation caused by filters or other processes • Limited and consistent diameter • Quality of service (QoS)
Distribution	<ul style="list-style-type: none"> • Policy-based connectivity • Redundancy and load balancing • Aggregation of LAN wiring closets • Aggregation of WAN connections • QoS • Security filtering • Address or area aggregation or summarization • Departmental or workgroup access • Broadcast or multicast domain definition • Routing between virtual LANs (VLAN) • Media translations (for example, between Ethernet and Token Ring) • Redistribution between routing domains (for example, between two different routing protocols) • Demarcation between static and dynamic routing protocols

|

Access	<ul style="list-style-type: none"> • Layer 2 switching • High availability • Port security • Broadcast suppression • QoS • Rate limiting • Address Resolution Protocol (ARP) inspection • Virtual access control lists (VACL) • Spanning tree • Trust classification • Power over Ethernet (PoE) and auxiliary VLANs for VoIP
--------	--

QUESTION 209

SNMP is short for Simple Network Management Protocol. Which version or versions of SNMP specify security extensions as part of the protocol definition?

- A. SNMPv2
- B. SNMPv4
- C. SNMPv3
- D. SNMPv1

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Table SNMP Security LevelsVersion

Level

Authentication

Encryption

SNMPv1

NoAuthNoPriv

Community String

None

SNMPv2

NoAuthNoPriv

Community String

None

SNMPv3

NoAuthNoPriv

Username

None

SNMPv3

AuthNoPriv

MD5 or SHA

None

SNMPv3

AuthPriv

MD5 or SHA

DES, 3DES, AES

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 15

QUESTION 210

What is the reason for switching preferred on shared segments?

- A. Switched segments provide a collision domain for each host.
- B. Switched segments provide a broadcast domain for each host
- C. Shared segments provide a broadcast domain for each host.
- D. Shared segments provide a collision domain for each host.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Switches

Switches use specialized integrated circuits to reduce the latency common to regular bridges. Switches are the evolution of bridges. Some switches can run in cut-through mode, where the switch does not wait for the entire frame to enter its buffer; instead, it begins to forward the frame as soon as it finishes reading the destination MAC address. Cut-through operation increases the probability that frames with errors are propagated on the network, because it forwards the frame before the entire frame is buffered and checked for errors. Because of these problems, most switches today perform store-and-forward operation as bridges do. Switches are exactly the same as bridges with respect to collision-domain and broadcast-domain characteristics. Each port on a switch is a separate collision domain. By default, all ports in a switch are in the same broadcast domain. Assignment to different VLANs changes that behavior.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 3

QUESTION 211

Study the following options carefully. The corporate Internet is part of which functional area?

- A. Enterprise Edge
- B. Enterprise Campus
- C. Service Provider (SP) Edge
- D. Enterprise

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Enterprise WAN

The enterprise edge of the enterprise WAN includes access to WANs. WAN technologies include the following:

Use the following guidelines when designing the enterprise edge:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 2

QUESTION 212

Which H.323 protocol is in charge of call setup and signaling?

- A. RTCP
- B. H.245
- C. G.711
- D. H.225

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

H.323 terminals must support the following standards:

H.245 specifies messages for opening and closing channels for media streams and other commands, requests, and indications. It is a control channel protocol.

Q.931 is a standard for call signaling used by H.323 within the context of H.225. It is also used by PRI links.

H.225 performs registration, admission, and status (RAS) signaling for H.323 sessions.

RTP is the transport layer protocol used to transport VoIP packets. RTCP is also a transport layer protocol.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 14

QUESTION 213

How often does a RIPv1 router broadcast its routing table by default?

- A. Every 90 seconds.
- B. Every 30 seconds.
- C. Every 60 seconds.
- D. RIPv1 does not broadcast periodically.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Distance-Vector Routing Protocols

The first IGP routing protocols introduced were distance-vector routing protocols. They used the Bellman-Ford algorithm to build the routing tables. With distance-vector routing protocols, routes are advertised as vectors of distance and direction. The distance metric is usually router hop count. The direction is the next-hop router (IP address) toward which to forward the packet. For RIP, the maximum number of hops is 15, which can be a serious limitation, especially in large nonhierarchical internetworks.

Distance-vector algorithms call for each router to send its entire routing table to only its immediate neighbors. The table is sent periodically (30 seconds for RIP). In the period between advertisements, each router builds a new table to send to its neighbors at the end of the period. Because each router relies on its neighbors for route information, it is commonly said that distance-vector protocols "route by rumor."

Having to wait half a minute for a new routing table with new routes is too long for today's networks. This is why distance-vector routing protocols have slow convergence.

RIPv2 and RIPv6 can send triggered updates--full routing table updates sent before the update timer has expired. A router can receive a routing table with 500 routes with only one route change, which creates serious overhead on the network (another drawback). Furthermore, RFC 2091 updates RIP with triggered extensions to allow triggered updates with only route changes. Cisco routers support this on fixed point-to-point interfaces.

The following is a list of IP distance-vector routing protocols:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 10

QUESTION 214

For the following protocols, which one maps names to IPv6 addresses?

- A. Domain Name System (DNS)
- B. DNSv2
- C. Address Resolution Protocol (ARP)
- D. Neighbor discovery (ND)

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

DNS maps domain names to IP addresses, and ARP resolves IP addresses to MAC addresses. These protocols are important in TCP/IP networks because they simplify the methods of address assignment and resolution.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 8

QUESTION 215

What does CDP stand for ?

- A. Collection Device Protocol
- B. Campus Discovery Protocol
- C. Cisco Device Protocol
- D. Cisco Discovery Protocol

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

CDP

Cisco Discovery Protocol (CDP) is a Cisco-proprietary protocol that can be used to discover only Cisco network devices. CDP is media and protocol independent, so it works over Ethernet, Frame Relay, ATM, and other media. The requirement is that the media support Subnetwork Access Protocol (SNAP) encapsulation. CDP runs at the data link layer of the OSI model. CDP uses hello messages; packets are exchanged between neighbors, but CDP information is not forwarded. In addition to routers and switches, IP phones and Cisco Unified Communication Manager (CUCM) servers also advertise CDP information. Being protocol and media independent is CDP's biggest advantage over other network management technologies. CDP provides key information about neighbors, including platforms, capabilities, and IP addresses, which is significant for network discovery. It is useful when SNMP community strings are unknown when performing a network discovery.

When displaying CDP neighbors, you can obtain the following information:

Network management devices can obtain CDP information for data gathering. CDP should be disabled on untrusted interfaces, such as those that face the Internet, third-party networks, or other secure networks. CDP works only on Cisco devices.

Note: Disable CDP on interfaces for which you do not want devices to be discovered, such as Internet connections.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 15

QUESTION 216

For the following options, which International Telecommunication Union (ITU) standard provides a framework for multimedia protocols for the transport of voice, video, and data over packet-switched networks?

- A. Weighted fair queuing (WFQ)
- B. H.323
- C. Voice over IP (VoIP)
- D. Session Initiation Protocol (SIP)

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

VoIP Control and Transport Protocols

A number of different protocols are used in a VoIP environment for call control, device provisioning, and addressing.

Figure 14-15 shows those protocols focused on VoIP control and transport.

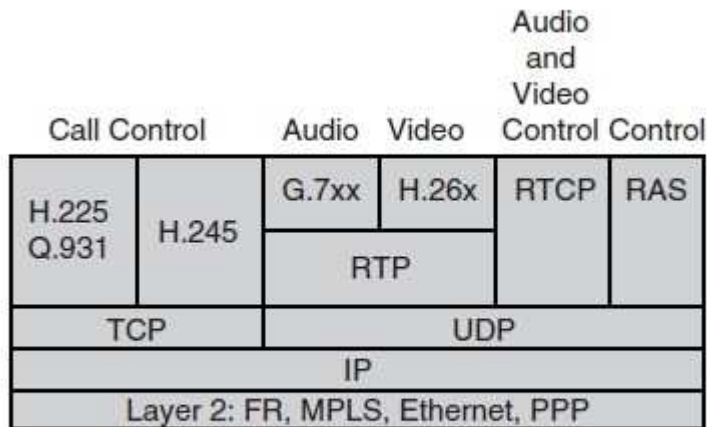


Figure 14-15 *VoIP Control and Transport Protocols*

Some of the most significant protocols are

Dynamic Host Configuration Protocol (DHCP): Used to provide device configuration parameters such as IP configuration (address, subnet mask, default gateway) and TFTP servers (via DHCP option 150).

TFTP: To obtain ring tones, backgrounds, configuration files, and firmware files. Skinny Client Control Protocol (SCCP): Used for call control for Cisco IP phones (Cisco proprietary).

Real-time Transport Protocol (RTP): For voice stream (VoIP) station-to-station traffic in an active call.

Real-time Transport Control Protocol (RTCP): For RTP control and reporting (accompanying stream to RTP between endpoints).

Media Gateway Control Protocol (MGCP): A client/server protocol for control of endpoints and gateways. In the MGCP model, intelligence resides on the call agent (server), and the device is controlled by the agent.

H.323: An ITU standard for VoIP networks that is a peer-to-peer system (call processing logic is local to each device) used for gateways and endpoints. Session Initiation Protocol (SIP): A standard for VoIP networks defined by the IETF and used for gateways and endpoints. SIP is feature rich (native IM, presence, and video support), lightweight, and designed for easy troubleshooting (ASCII-based messages).

QUESTION 217

Which feature will not transfer packets when there is silence?

- A. Ear and mouth (E&M)
- B. Voice Activity Detection (VAD)
- C. Digital Silence Suppressor (DSS)
- D. Dial peers

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

VAD

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 speech 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. Bandwidth savings are at least 35 percent in conservative estimates. VAD is enabled by default for all VoIP calls. In real-world practice, is it suggested that VAD be avoided because it creates quality issues and breaks applications such as fax and modem transmissions.

For G.729 bandwidth is reduced from 26.4 kbps to 17.2 kbps with VAD and to 7.3 kbps with VAD and cRTP enabled.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 14

QUESTION 218

What does the Cisco SLM define as the component used to specify expected performance between a pair of devices connected by a network?

- A. CM
- B. SLC
- C. SLA
- D. SAA

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

CiscoWorks Service Level Manager

Service Level Manager (SLM) version 2.0 is the server component of the CiscoWorks Service Management Solution (SMS). SLM allows administrators to define and validate service-level agreements in terms common to those written into their Service Provider contract. Through local and remote Collection Managers, SLM interacts with the Cisco IOS® Software to perform synthetic testing and monitoring of Layer 3 and 4 services according to the specified SLA parameters and thresholds. The synthetic testing approach ensures a common understanding between customer and service provider of the endpoints, characteristics, and thresholds of the tests.

NOTE: This product is no longer being sold and might not be supported. View the End-of-Life Notice to learn: <http://www.cisco.com/en/US/products/sw/cscowork/ps2144/index.html>

QUESTION 219

In a network with Enhanced Interior Gateway Routing Protocol (EIGRP) and IGRP using the same autonomous system number, what will happen on the router configured with both protocols?

- A. Redistribution occurs automatically.
- B. Redistribution is not necessary.
- C. EIGRP assumes IGRP is a less capable protocol and overtakes it.
- D. Redistribution does not occur automatically.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 220

What is the acronym PDIOO short for?

- A. Purpose, design, install, operation, optimization
- B. Purpose, design, implement, operate, optimize
- C. Plan, design, install, operation, optimization
- D. Plan, design, implement, operate, optimize

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

PDIOO has now been replaced with PPDIOO

Table: PPDIOO Network Life Cycle Phases	
PPDIOO Phase	Description
Prepare	Establishes organization and business requirements, develops a network strategy, and proposes a high-level architecture.
Plan	Identifies the network requirements by characterizing and assessing the network, performing a gap analysis.
Design	Provides high availability, reliability, security, scalability, and performance.
Implement	Installation and configuration of new equipment.
Operate	Day-to-day network operations.
Optimize	Proactive network management. Modifications to the design.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 1

QUESTION 221

Which item is not an SNMP operation?

- A. GetNext
- B. Community
- C. Trap
- D. Set

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

SNMP Operations

SNMP operations focus on retrieving or modifying the value of management information, and reporting an event. They occur through message exchange over a message transport service. Each SNMP operation has its own type of message. An SNMP message consists of a header and a protocol data unit (PDU) identifying the message type and containing further data necessary to complete the request. The following table shows the message types that are supported by Windows Embedded CE.

Message type	Description	From/To
GetRequest	Accesses and retrieves the value of one or more instances of management information.	Manager/agent
GetNextRequest	Accesses and retrieves the value of the next instance of management information in lexicographical order.	Manager/agent
GetBulk	Accesses multiple values at one time (SNMPv2c only).	Manager/agent
GetResponse	Reply to a GetRequest , GetNextRequest , and SetRequest operation.	Agent/manager
SetRequest	Stores and sets a value in a variable.	Manager/agent
Trap	An unsolicited message that is sent by an SNMP agent to an SNMP manager and indicates that some event has occurred.	Agent/manager

GetRequest

The SNMP manager uses the GetRequest message to retrieve data from the managed objects that are maintained by an SNMP agent. By using GetRequest, the manager can request the value of one or more MIB variables, provided that the MIBs that specify the variables are supported by the agent that receives the GetRequest message.

GetNextRequest

The GetNextRequest message, like the GetRequest message, is used by the SNMP service to retrieve data from a managed object that is maintained by an SNMP agent. GetNextRequest and GetRequest have the same format, but they use different operations. Unlike GetRequest, GetNextRequest does not require that the instance identifier of each variable be specified in its OID.

GetBulk

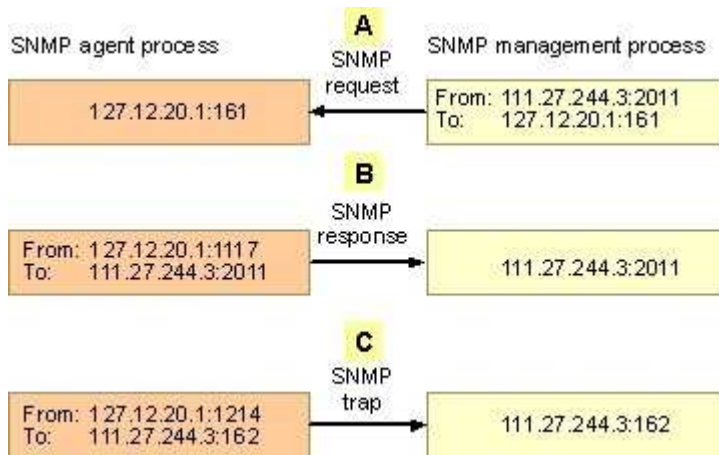
This operation is new for SNMPv2. It allows the SNMP manager to retrieve large amounts of information from the agent without initiating a GetNextRequest operation.

SetRequest

The SNMP manager uses the SetRequest message to request that management data that is maintained by an agent be modified. SetRequest has the same format as the GetRequest message, but it is used to write an object value, not to read one.

Trap

The SNMP service can handle requests and report network management information to one or more hosts in discrete blocks of data that are known as traps. Traps notify a network management device that an extraordinary event has occurred at an agent. When a trap condition occurs, the SNMP agent sends an SNMP-agent trap message to each of the network management stations, as specified in the trap receiver table. The following illustration shows how messages are exchanged between the SNMP agent and the SNMP service.



<http://msdn.microsoft.com/en-us/library/aa910027.aspx>

QUESTION 222

Which packet-switching topology approach typically requires the greatest level of expertise to implement?

- A. Hub and spoke
- B. Point-to-point
- C. Star
- D. Partial mesh

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Hub and spoke or star network creates a central point of failure and is a more complex network than a point to point to configuration. However, due to the level of redundant configurations the Partial Mesh configuration is more complex than any of the other choices listed

Packet and cell switched: Connections that use virtual circuits (PVC/SVC) established by the SP. Packet-switched technologies include Frame Relay and cell-switched technologies such as ATM. ATM uses cells and provides support for multiple quality of service (QoS) classes. The virtual circuits are part of the shared ATM/Frame Relay SP backbone network. This gives the SP greater flexibility with its service offerings.

Hub-and-Spoke Topology

A star or hub-and-spoke topology provides a hub router with connections to the spoke routers through the WAN cloud. Network communication between the sites flows through the hub router. Significant WAN cost savings, lower circuit counts, and simplified management are benefits of the hub-and-spoke topology. In addition, hub-and-spoke topologies provide WAN hierarchy and can provide high availability through the use of dual routers at the hub site.

A major disadvantage of this approach is that if you use a single hub router, it can represent a single point of failure. The hub-and-spoke topology can also limit the overall performance when resources are accessed through the central hub router from the spoke routers, such as with spoke-to-spoke network traffic.

QUESTION 223

The network-design process is limited by many external constraints. Which origins are of these constraints?

- A. Technological, worldwide standards, social, and managerial
- B. Technological, political, social, and economical

- C. Technological, cost, social, and economical
- D. Managerial, political, social, and economical

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Requirements and Constraints

Before delving into the typical topologies, it is wise to understand the overall network design process. As with any systems design effort, network design is an exercise in meeting new and old requirements while working within certain constraints. These constraints include money, labor, technology, space, and time. In addition, there may be social or political constraints, such as the mandated use of certain standards or vendors. Economic constraints play a major role in any network design. Unless you are very fortunate, you often must compromise in the capacity of WAN links, the switching capabilities of routers, the type of interfaces used, and the level of redundancy achieved. Achieving the "best possible service at the lowest possible cost" was a design paradigm invented--tongue-in-cheek, to some extent--by one network manager to satisfy both management and network users. This paradigm fails to explain how this task is achieved, other than through a carefully considered compromise, but neither does it say anything that is incorrect.

Labor effort should be of paramount concern in any network design. In this case, the first area of concern is the amount of effort and level of skill necessary to connect a new customer to the network or to expand the capacity of the network infrastructure. As a general rule, the more often a task must be executed, the more the design should focus on making that task simple and efficient--in other words, the goal involves optimizing the common case. In addition to prudent network design, labor costs can also be reduced through investment in network management tools. It is noteworthy that for many networks, the capital cost is dwarfed by the ongoing charges for highly skilled support personnel.

Processor speed doubles every 18 months. Nevertheless Internet traffic levels can increase at a far more rapid rate. Thus, computation is still a constraint of network design, particularly in the case of routers. Typical computational limitations that apply to network design are associated with processing of routing updates, accounting, security filtering and encryption, address translation, and even packet forwarding.

Space issues include the physically obvious, such as the cost of expensive air-conditioned points of presence (POPs) or co-location facilities. Space also includes subtler, but nonetheless important resources, such as the buffer capacity in a router or the bandwidth of a WAN link. One time constraint that affects the success of a design is the time-to-market. It is useless to design an extremely sophisticated network if the customers have gone elsewhere by the time it is operational. Time constraints also include packet forwarding and propagation delays, which have a fundamental impact on bandwidth (in a TCP/IP environment) and response time. Social constraints include those that may not seem sensible to achieve the major requirements of the network. These could include a mandated use of standards that are difficult to obtain, to use, or to understand. Thankfully, this has been less common since the demise of OSI. (At one time in the industry, a play on the OSI reference model included a "political" layer above the application layer--the so-called "eighth layer of networking.") Alternatively, you may be constrained to using a certain vendor's equipment because of a prearranged partnership agreement.

Cisco Network Topology and Design

By Khalid Raza, Mark Turner.

Sample Chapter is provided courtesy of Cisco Press.

Date: Feb 1, 2002

QUESTION 224

What does FCAPS stand for?

- A. Fault, caching, application, production, security
- B. Fault, configuration, accounting, performance, security
- C. Fiscal, communication, application, production, security
- D. Fault, consolidation, accounting, performance, security

Correct Answer: B

Section: (none)**Explanation****Explanation/Reference:**

Explanation:

Explanation

FCAPS is the ISO Telecommunications Management Network model and framework for network management. FCAPS is an acronym for Fault, Configuration, Accounting, Performance, Security, the management categories into which the ISO model defines network management tasks. In non-billing organizations Accounting is sometimes replaced with Administration.

Fault management

A fault is an event that has a negative significance. The goal of fault management is to recognize, isolate, correct and log faults that occur in the network. Furthermore, it uses trend analysis to predict errors so that the network is always available. This can be established by monitoring different things for abnormal behavior.

When a fault or event occurs, a network component will often send a notification to the network operator using a proprietary or open protocol such as SNMP, or at least write a message to its console for a console server to catch and log/page. This notification is supposed to trigger manual or automatic activities. For example, the gathering of more data to identify the nature and severity of the problem or to bring backup equipment on-line. Fault logs are one input used to compile statistics to determine the provided service level of individual network elements, as well as sub-networks or the whole network. They are also used to determine apparently fragile network components that require further attention. The leading Fault Management systems are EMC Smarts, CA Spectrum, HP Software, NetIQ, IBM Tivoli Netcool, TTI Telecom Netrac, CA Clarity, Objective Systems Integrators NETeXPERT etc. Fault Isolation tools like Delphi are also available, which are basically used to isolate the fault in any telecom network.

Configuration management

The goals of configuration management include:

Accounting management

Accounting is often referred to as billing management. The goal is to gather usage statistics for users.

Using the statistics the users can be billed and usage quota can be enforced.

Examples:

RADIUS, TACACS and Diameter are examples of protocols commonly used for accounting. For non-billed networks, "administration" replaces "accounting". The goals of administration are to administer the set of authorized users by establishing users, passwords, and permissions, and to administer the operations of the equipment such as by performing software backup and synchronization.

Performance management

Performance management enables the manager to prepare the network for the future, as well as to determine the efficiency of the current network, for example, in relation to the investments done to set it up. The network performance addresses the throughput, percentage utilization, error rates and response times areas.

By collecting and analysing performance data, the network health can be monitored. Trends can indicate capacity or reliability issues before they become service affecting. Performance thresholds can be set in order to trigger an alarm. The alarm would be handled by the normal fault management process (see above). Alarms vary depending upon the severity.

Security management

Security management is the process of controlling access to assets in the network. Data security can be achieved mainly with authentication and encryption. Authorization to it configured with OS and DBMS access control settings...

QUESTION 225

What is DHCP?

- A. Dynamic Host Configuration Protocol
- B. Dedicated Host Configuration Protocol
- C. Dynamic Host Control Protocol
- D. Predecessor to BOOTP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

DHCP (Dynamic Host Control Protocol) - Provides IP address, mask, gateway, DNS address, and TFTP address

QUESTION 226

Which answer is correct about routing metrics?

- A. If the metric is cost, the path with the highest cost is selected.
- B. If the metric is bandwidth, the path with the highest bandwidth is selected.
- C. If the metric is bandwidth, the path with the lowest bandwidth is selected.
- D. If the metric is bandwidth, the highest sum of the bandwidth is used to calculate the highest cost.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 227

Where do you put DNS and DHCP on Enterprise model? Select two.

- A. Enterprise campus Server Farm Module
- B. Enterprise edge
- C. SP Edge Premise
- D. Enterprise Branch

Correct Answer: AD

Section: (none)

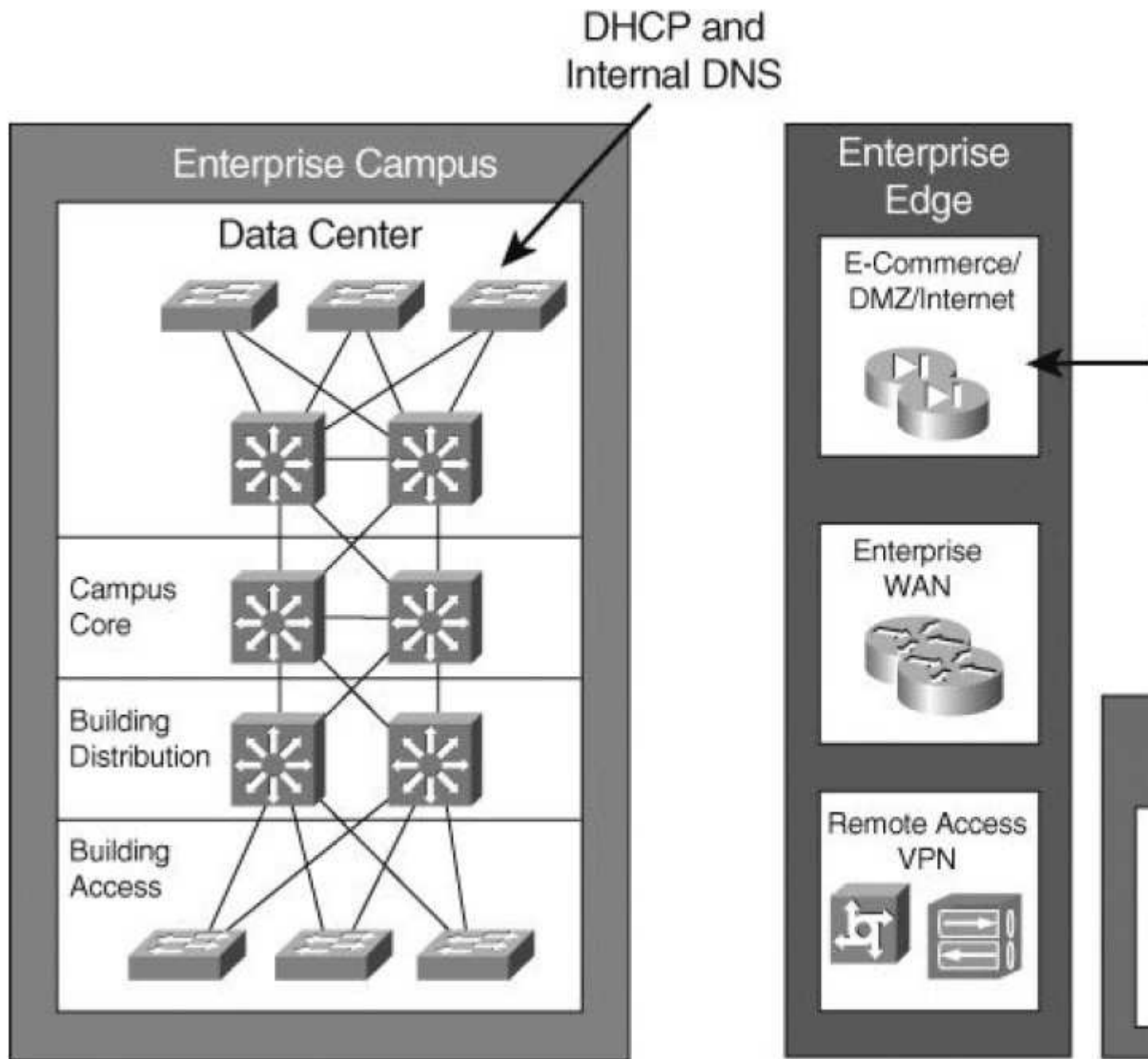
Explanation

Explanation/Reference:

Explanation: Explanation

One important note for the CCDA to remember is to place DNS servers in the Enterprise Campus Server Farm module and Enterprise Branch of the Enterprise Campus architecture (see Figure 8-7).

Figure. DHCP and DNS Servers in the Network



Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 8

QUESTION 228

Which two of these are functions of an access point in a Split MAC Network Architecture? (Choose two.)

- A. EAP Authentication
- B. MAC layer encryption or decryption
- C. 802.1Q encapsulation
- D. Process probe response

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Cisco Unified Wireless Network Split-MAC Architecture With the Cisco UWN split-MAC operation, the control and data messages are split. LWAPs communicate with the WLCs using control messages over the wired network. LWAPP or CAPWAP data messages are encapsulated and forwarded to and from wireless clients. The WLC manages multiple APs, providing configuration information and firmware updates as needed.

LWAP MAC functions are

Controller MAC functions are

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 5

QUESTION 229

Data link switching is typically used in which Enterprise Campus Module layer?

- A. Server Farm
- B. Campus Core
- C. Building Access
- D. Building Distribution
- E. Internet Connectivity

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

In the most general model, the Building Access layer uses Layer 2 switching (or Data link switching), and the Building Distribution layer uses multilayer switching.

QUESTION 230

Which three of these are components of the North American Numbering Plan? (Choose three.)

- A. Numbering Plan Area
- B. country code
- C. prefix
- D. zone
- E. line number
- F. trunk channel

Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

NANP has the address format of NXX-NXX-XXXX, where N is any number from 2 to 9 and X is any number from 0 to 9. The first three digits identify the numbering plan area and are commonly called the area code. The address is further divided into the office code (also known as prefix) and line number. The prefix is three digits, and the line number is four digits. The line number identifies the phone.

QUESTION 231

Which two statements about the Enterprise Data Center Aggregation submodule are correct? (Choose two.)

- A. it provides Layer 4-7 services
- B. it should never support STP
- C. it is the critical point for control and application services
- D. it typically provides Layer 2 connectivity from the data center to the core

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

This submodule provides Layer 4 through Layer 7 services through security and application service devices such as load-balancing devices, SSL offloading devices, firewalls, and IDS devices.

The Data Center Aggregation (distribution) layer aggregates the uplinks from the access layer to the Data Center Core layer and is the critical point for control and application services.

QUESTION 232

Which network management protocol allows a network device to have vendor-specific objects for management?

- A. SNMP v1
- B. SNMP v2
- C. SNMP v3
- D. MIB
- E. RMON1
- F. RMON2

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

MIB

A Management Information Base (MIB) is a collection of information that is stored on the local agent of the managed device. MIBs are organized hierarchically and are accessed by the NMS. MIBs are databases of objects organized in a tree-like structure, with each branch containing similar objects. Each object has a unique object identifier (number) that uniquely identifies the managed object of the MIB hierarchy. Read and write community strings are used to control access to MIB information.

The top-level MIB object IDs belong to different standards organizations and lower-level object IDs are allocated to associated organizations. Standard MIBs are defined by RFCs. Vendors define private branches that include managed objects for their products. RFC 1213 describes the MIBs for TCP/IP. Cisco defines the MIBs under the Cisco head object. For example, a Cisco MIB can be uniquely identified by either the object name, iso.org.dod.private.enterprise.cisco, or the equivalent object descriptor, 1.3.6.1.4.1.9.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 15

QUESTION 233

Which two solutions are parts of the Cisco Security Management Suite? (Choose two.)

- A. ASA

- B. Cisco Security Agent
- C. NAC Appliance
- D. csm
- E. pix
- F. Cisco Security MARS

Correct Answer: DF

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Solutions of the Cisco Security Management Suite are:

+ Cisco Security Manager (CSM) is an integrated solution for configuration management of firewall, VPN, router, switch module, and IPS devices.

+ Cisco Secure Access Control Server (ACS) provides centralized control for administrative access to Cisco devices and security applications.

+ Cisco Security Monitoring, Analysis, and Response System (MARS) is an appliance-based solution for network security administrators to monitor, identify, isolate, and respond to security threats.

+ Management Center for CSA (CSA MC) is an SSL web-based tool for managing Cisco Security Agent configurations.

+ Cisco Router and Security Device Manager (SDM) is a web-based tool for routers and supports a wide range of IOS software.

+ Cisco Adaptive Security Device Manager (ASDM) is a web-based tool for managing Cisco ASA 5500 series appliances, PIX 500 series appliances (version 7.0 or higher), and Cisco Catalyst 6500 Firewall Services Modules (FWSM version 3.1 or higher). + Cisco Intrusion Prevention System Device Manager (IDM) is a web-based application that configures and manages IPS sensors.

(Reference: CCDA Official Exam Certification Guide 3rd)

QUESTION 234

When monitoring voice traffic on a converged network, which are the three most important QoS characteristics to pay attention to? (Choose three.)

- A. delay
- B. jitter
- C. packet loss
- D. bit error rate
- E. CRTP hop configuration

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Packets might not arrive at a constant rate because they take different paths and have perhaps experienced congestion in the network.

Real-time applications such as voice and video are not very tolerant to jitter and delay.

Table identifies various application requirements for data, voice, and video traffic.

Table Application Requirements				
	Data File Transfer	Interactive Data Application	Real-Time Voice	Real-Time Video
Response Time	Reasonable	Within a second	Round Trip less than 250ms with the delay and low jitter	Minimum delay and jitter
Throughput and packet loss tolerance	High/Med	Low/Low	Low/Low	High/Med
Downtime (high reliability has low downtime)	Reasonable	Low	Low	Minimum

Packet Loss

Packet loss is another item that affects voice and video quality. It causes voice and video clipping and skips. It is caused by several factors: congested links, improper QoS configuration, bad packet buffer management, and routing issues. Packet loss is also caused by packets received outside of the dejitter buffer range, which are packets that are discarded.

Cisco VoIP uses 20-ms samples of voice payload per VoIP packet. Codec algorithms can then correct up to 30 ms of lost voice. For the codec correction to be effective, only 1 packet can be lost during any given time. When this occurs, the DSP interpolates the conversation with what it thinks the audio should be.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition

QUESTION 235

An internal network has servers with private IPv4 addresses that must be visible from the public network. Which kind of address translation should be used to ensure this?

- 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)

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Table. NAT Concepts	
Description	IPv4 Address Type
Commonly used to assign a network device with internal private IP address an unique public address so that they can be accessed from the Internet	Static NAT
Dynamically maps an unregistered or private IP address to a registered IP address from a pool (group) of registered addresses.	Dynamic NAT
Maps multiple unregistered or private IP addresses to a single registered IP address by using different ports	PAT
The real IP address of the device that resides in the internal network. This address is used in the stub domain.	Inside local address
The translated IP address of the device that resides in the internal network. This address is used in the public network	Inside global address
The real IP address of a device that resides in the Internet, outside the stub domain.	Outside Global address
The translated IP address of the device that resides in the Internet. This address is used inside the stub domain	Outside local address

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 8

QUESTION 236

Which two of these are the most accurate characteristics of EIGRP deployment? (Choose two.)

- A. Provides features for most Ethernet, Frame Relay, and dial-up network deployment types.
- B. Provides routing for IPv4, IPv6, Appletalk, and IPX.
- C. Provides default hierarchical routing and summarization of a VLSM IP address deployment.
- D. Provides quick convergence through neighbor relationships and topology backup routes.
- E. Provides the best route selection on combined default metrics of active bandwidth, delay, load, reliability, and MTU parameters.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

EIGRP for IPv4 Summary

The characteristics of EIGRP for IPv4 networks follow:

DUAL

EIGRP implements DUAL to select paths and guarantee freedom from routing loops. J. J. Garcia Luna-Aceves developed DUAL. It is mathematically proven to result in a loop-free topology, providing no need for periodic updates or route hold-down mechanisms that make convergence slower.

DUAL selects a best path and a second-best path to reach a destination. The best path selected by DUAL is the successor, and the second-best path (if available) is the feasible successor. The feasible distance is the lowest calculated metric of a path to reach the destination.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 10

QUESTION 237

Which of the following is a modular component within the Cisco Enterprise Campus module in the Cisco Enterprise Architecture framework?

- A. Teleworker
- B. E-Commerce
- C. Internet Connectivity
- D. Building Distribution
- E. WAN/MAN Site-to-Site VPN

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 238

A company is implementing an Identity Management solution with these characteristics:

existing Cisco ACS 4.0

Cisco Catalyst switches

minimal added investments

Which Cisco Trust and Identity solution would you recommend?

- A. NAC Appliance (Cisco Clean Access)
- B. Cisco IBNS
- C. NAC Framework
- D. Cisco Security Agent
- E. csm
- F. Cisco Security MARS

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Identity Based Networking Services

Cisco Identity Based Networking Services (IBNS) is an integrated solution consisting of several Cisco products that offer authentication, access control, and user policies to secure network connectivity and resources. IBNS helps enterprises with the ability to increase user productivity, reduce operating costs, increase visibility and enforce policy compliance.

IBNS focuses on wired Campus LAN infrastructures

http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html

Cisco ACS

Cisco® Secure Access Control Server (ACS) is a highly scalable, high-performance access control server that provides a comprehensive identity networking solution. As an important component of the Cisco Identity-Based Networking Services (IBNS) architecture, Cisco Secure ACS extends access security by combining authentication, user or administrator access, and policy control from a centralized identity networking framework. This allows enterprise networks to have greater flexibility and mobility, increased security, and user productivity gains. Cisco Secure ACS supports a wide array of access connection types, including wired and wireless LAN, dialup, broadband, content, storage, voice over IP (VoIP), firewalls, and VPNs. http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps2086/prod_bulletin0900aecd80388_2de.html

IBNS: Web Authentication Deployment and Configuration Guide The following hardware platforms and software releases are the minimum versions required to configure all the features described in this guide:

· Cisco Catalyst® 2960 Series Switches with Cisco IOS® Software Release 12.2(50)SE32 · Cisco Catalyst 3560 Series Switches with Cisco IOS Software Release 12.2(50)SE32 · Cisco Catalyst 3750 Series Switches with Cisco IOS Software Release 12.2(50)SE32 · Cisco Catalyst 4500 Series Switches with Cisco IOS Software Release 12.2(50)SG · Cisco Catalyst 6500 Series Switches with Cisco IOS Software Release 12.2(33)SXI · Cisco® Secure Access Control System (ACS) Version 5.0 (earlier versions of Cisco Secure ACS will also support the required functions with the appropriate configuration).

Although other platforms were not tested as part of this solution, the Cisco Catalyst 4948 Switch is expected to perform similarly with these software releases.

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/app_note_c27-577494.html

QUESTION 239

Which two design methodology steps relate, at least in part, to the implement phase of the PPDIOO process? (Choose two.)

- A. verifying the network
- B. testing design
- C. determining customer requirements
- D. characterizing the existing network
- E. establishing the organizational requirements

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

The Implement phase relates to implement new devices, including verifying and testing so A and B are the most suitable options.

"Determining customer requirements" occurs in the Prepare phase, which identifies requirements and builds a conceptual architecture.

"Characterizing the existing network" belongs to the Plan phase; this step is performed to determine the infrastructure necessary to meet the requirements. In the "establishing the organizational requirements" step, the network topology is designed to meet the requirements and close the network gaps identified in the previous steps. This step is related to the Design Phase of the PPDIOO process.

QUESTION 240

Which H.323 protocol monitors calls for factors such as packet counts, packet loss, and arrival jitter?

- A. H.225
- B. H.245
- C. RAS

D. RTCP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

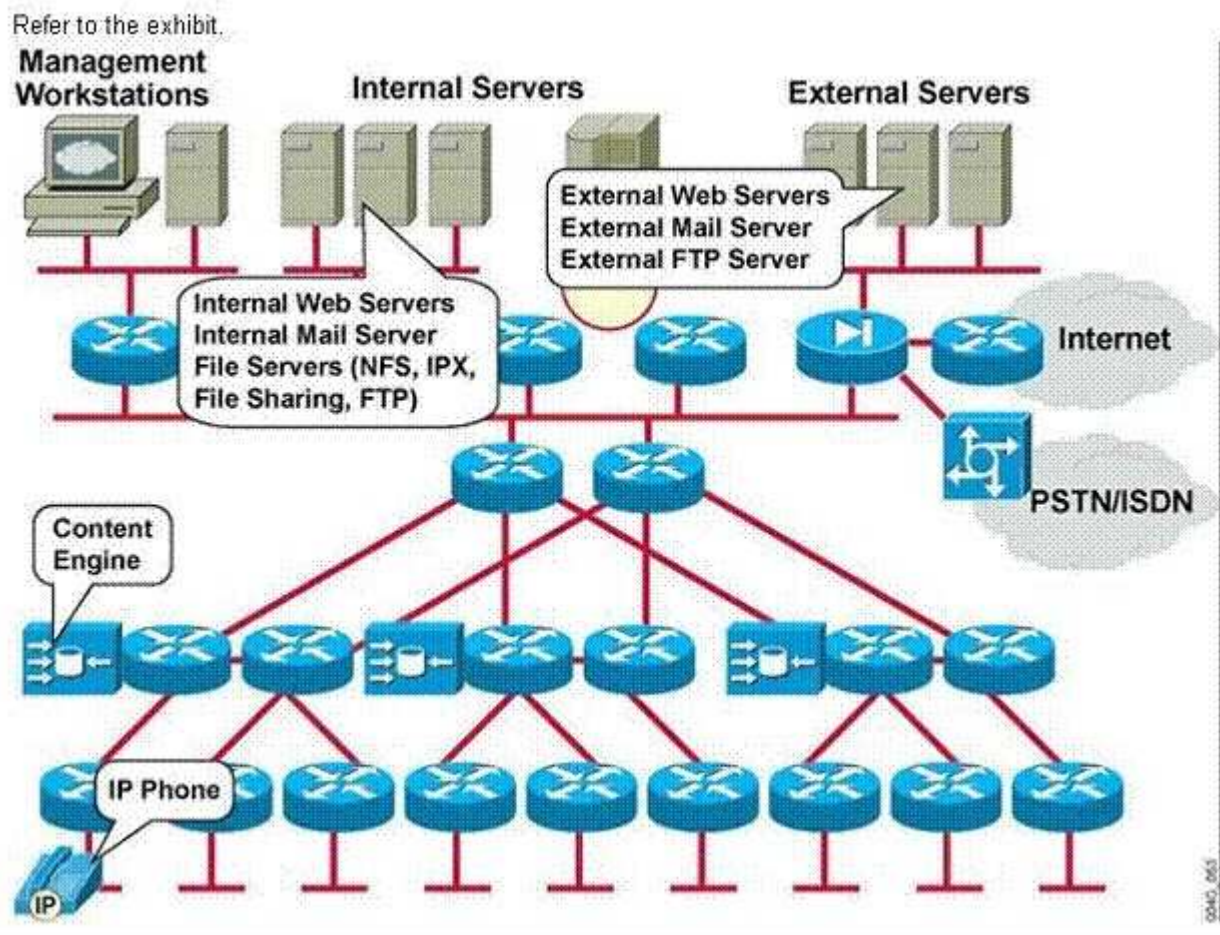
Explanation: Explanation

RTCP is also defined in RFC 3550. RTCP is a session layer protocol that monitors the delivery of data and provides control and identification functions.

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 14

QUESTION 241

Refer to the exhibit.



Which element or elements of the existing network infrastructure does this network map emphasize?

- A. network services
- B. network protocols
- C. the OSI data link layer
- D. network applications

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 242

The BodMech online fitness organization specializes in creating fitness plans for senior citizens. The company recently added a health-products retail inventory. Which E-Commerce module device will allow customers to interact with the company and purchase products?

- A. application server
- B. database server
- C. public server
- D. web server
- E. NIDS appliance
- F. SMTP mail server

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Web server can refer to either the hardware (the computer) or the software (the computer application) that helps to deliver content that can be accessed through the Internet. The most common use of Web servers is to host Web sites but there are other uses like data storage or for running enterprise applications.

The primary function of a web server is to deliver web pages on the request to clients. This means delivery of HTML documents and any additional content that may be included by a document, such as images, style sheets and scripts.

A client, commonly a web browser or web crawler, initiates communication by making a request for a specific resource using HTTP and the server responds with the content of that resource or an error message if unable to do so. The resource is typically a real file on the server's secondary memory, but this is not necessarily the case and depends on how the web server is implemented. While the primary function is to serve content, a full implementation of HTTP also includes ways of receiving content from clients. This feature is used for submitting web forms, including uploading of files.

Many generic web servers also support server-side scripting, e.g., Apache HTTP Server and PHP. This means that the behavior of the web server can be scripted in separate files, while the actual server software remains unchanged. Usually, this function is used to create HTML documents "on- the-fly" as opposed to returning fixed documents. This is referred to as dynamic and static content respectively. The former is primarily used for retrieving and/or modifying information from databases. The latter is, however, typically much faster and more easily cached. Web servers are not always used for serving the world wide web. They can also be found embedded in devices such as printers, routers, webcams and serving only a local network. The web server may then be used as a part of a system for monitoring and/or administrating the device in question. This usually means that no additional software has to be installed on the client computer, since only a web browser is required (which now is included with most operating systems).

QUESTION 243

Which two of the following are benefits of using a modular approach to network design? (Choose two.)

- A. improves flexibility
- B. facilitates implementation
- C. lowers implementation costs
- D. improves customer participation in the design process

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 244

Which statement describes the recommended deployment of DNS and DHCP servers in the Cisco Enterprise Architecture Model?

- A. Place the DHCP and DNS servers in the Enterprise Campus Access layer and Enterprise branch.
- B. Place the DHCP and DNS servers in the Enterprise Campus Server Farm layer and Enterprise branch.
- C. Place the DHCP server in the Enterprise Campus Core layer and Remote Access/VPN module with the DNS server in the Internet Connectivity module.
- D. Place the DHCP server in the Enterprise Campus Distribution layer with the DNS server in the Internet Connectivity module.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: For the Enterprise Campus, DHCP and internal DNS servers should be located in the Server Farm and they should be redundant. External DNS servers can be placed redundantly at the service provider facility and at the Enterprise branch.

QUESTION 245

Which two routing protocols usually converge most quickly? (Choose two.)

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

Correct Answer: EF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 246

Which two wireless attributes should be considered during a wireless site survey procedure? (Choose two.)

- A. encryption
- B. channel
- C. authentication
- D. power
- E. SSID

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

RF Site Survey

Similar to performing an assessment for a wired network design, RF site surveys are done to determine design parameters for WLANs and customer requirements. RF site surveys help determine the coverage areas and check for RF interference. This helps determine the appropriate placement of wireless APs.

The RF site survey has the following steps:

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 5

QUESTION 247

When designing using the Cisco Enterprise Architecture, in which Enterprise Campus layer does the Enterprise Teleworker module establish its connection?

- A. Building Core
- B. Building Access
- C. Enterprise Branch
- D. Enterprise Data Center
- E. WAN/Internet

Correct Answer: E

Section: (none)

Explanation

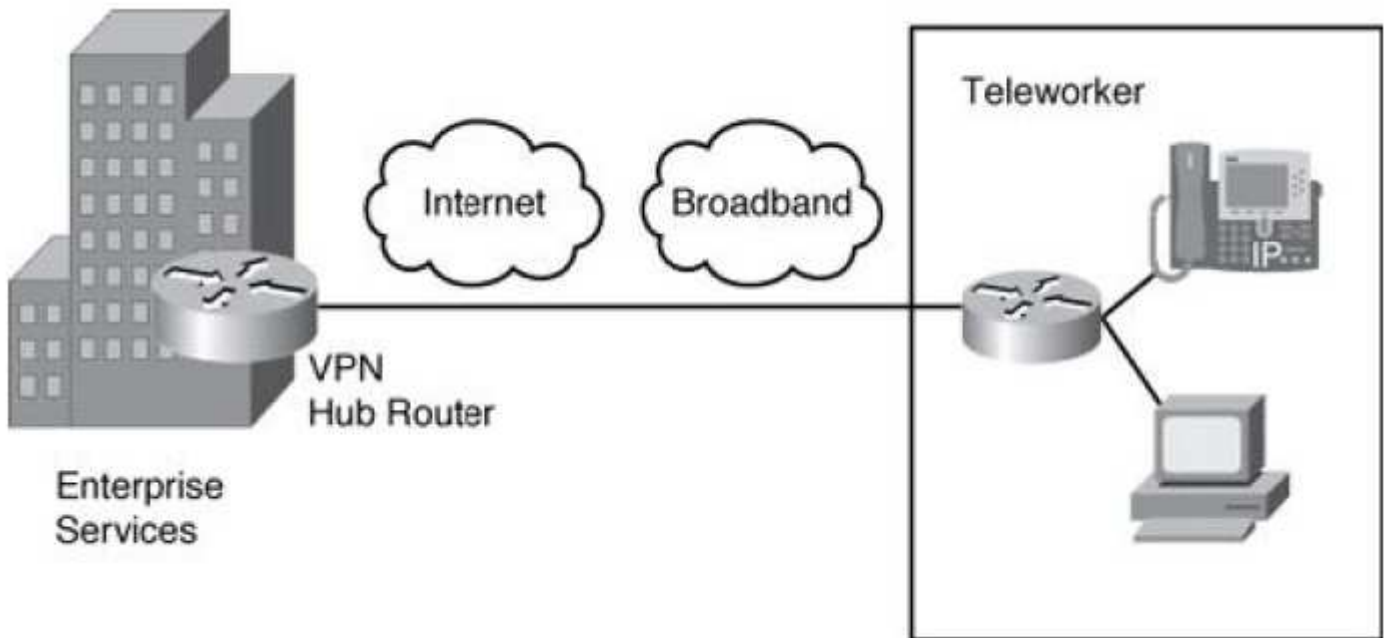
Explanation/Reference:

Explanation: Explanation

Enterprise Teleworker Module

The enterprise teleworker module consists of a small office or a mobile user who needs to access services of the enterprise campus. As shown in Figure 2-14, mobile users connect from their homes, hotels, or other locations using dialup or Internet access lines. VPN clients are used to allow mobile users to securely access enterprise applications. The Cisco Virtual Office solution provides a solution for teleworkers that is centrally managed using small integrated service routers (ISR) in the VPN solution. IP phone capabilities are also provided in the Cisco Virtual Office solution, providing corporate voice services for mobile users.

Figure 2-14. Enterprise Teleworker Solution



Internet Connectivity Module

The Internet submodule of the enterprise edge provides services such as public servers, email, and DNS. Connectivity to one or several Internet service providers (ISP) is also provided. Components of this submodule include

Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 2

QUESTION 248

Which three of these are layers in the Cisco SONA Architecture? (Choose three.)

- A. Application
- B. Physical
- C. Presentation
- D. Integrated Transport
- E. Interactive Services
- F. Networked Infrastructure

Correct Answer: AEF

Section: (none)

Explanation

Explanation/Reference:

Explanation: Explanation

Overview:

The Cisco Service-Oriented Network Architecture (SONA) framework outlines how enterprises can evolve their IT infrastructure into an Intelligent Information Network that accelerates applications, business processes and resources, and enables IT to have a greater impact on business. The architectural framework shows how integrated systems across a fully converged network allow flexibility, while standardization and virtualization of resources increases efficiency. SONA extends Cisco's tested and proven network designs in the Data Center, Campus, WAN/MAN, Teleworker and Branch, to securely and reliably enable business applications. It leverages the solutions, services and experience of Cisco and its partners.

Since SONA was announced in December 2005 Cisco has delivered several new solutions that support SONA, added to our portfolio of lifecycle services and worked with customers and partners to explore ways to enhance

SONA for global enterprises.

Three Layers of Cisco SONA

SONA Fact Sheet

Cisco Service-Oriented Network Architecture Update

http://newsroom.cisco.com/dlls/2006/eKits/sona_fact_sheet.pdf

QUESTION 249

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 route summarization
- C. reduces the routing table size by using manual route summarization
- D. allows the subnet mask and classful routing updates to be advertised
- E. secures the hosts on a subnet by using RFC 1918 addresses

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 250

You are performing an audit of a customer's existing network and need to obtain the following router information:

Interfaces

running processes

IOS image being executed

Which command should you use?

- A. show version
- B. show tech-support
- C. show startup-config
- D. show running-config
- E. show processes memory

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 251

What is the recommended spanning tree protocol to use for all Layer 2 deployments in a branch office environment?

- A. CST
- B. RSPT
- C. PVST
- D. MSTP

E. Rapid PVST +

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 252

Which Cisco device management feature is most suited to metering network traffic and providing data for billing network usage?

- A. BGP
- B. Cisco Discovery Protocol
- C. QoS
- D. RMON
- E. NetFlow

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 253

Which of these domain-of-trust security statements is correct?

- A. Segments within a network should have the same trust models.
- B. An administrator should apply consistent security controls between segments.
- C. Communication between trusted entities needs to be carefully managed and controlled.
- D. Segment security policy decisions are based on trust.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 254

When collecting information about a customer's existing network, which two sources will provide the most accurate data? (Choose two.)

- A. traffic analysis
- B. customer interview
- C. customer-supplied server list
- D. existing network topology diagram
- E. configurations obtained from network equipment

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 255

Which modules are found in the Enterprise Edge functional area of the Cisco Enterprise Architecture? Select all that apply.

- A. Teleworker
- B. WAN/MAN
- C. Server Farm
- D. E-Commerce
- E. Internet Connectivity
- F. Remote Access/VPN

Correct Answer: BDEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Enterprise Edge functional area is composed of Following modules:

- E-commerce module: The E-commerce module includes the devices and services necessary for an organization to provide e-commerce applications.
- Internet Connectivity module: The Internet Connectivity module provides enterprise users with Internet access.
- Remote Access and VPN module: This module terminates VPN traffic and dial-in connections from external users.
- WAN and MAN and Site-to-Site VPN module: This module provides connectivity between remote sites and the central site over various WAN technologies.

QUESTION 256

A campus network needs end-to-end QoS tools to manage traffic and ensure voice quality. Which three types of QoS tools are needed? (Choose three.)

- A. interface queuing and scheduling
- B. congestion management
- C. compression and fragmentation
- D. bandwidth provisioning
- E. traffic classification
- F. buffer management

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 257

Which H.323 protocol is responsible for the exchanging of capabilities and the opening and closing of logical channels?

- A. H.225
- B. H.245
- C. RAS
- D. RTCP

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:



<http://www.gratisexam.com/>