

**Cisco.Actualtests.640-864.v2014-06-24.by.LISA.160q**

Number: 640-864  
Passing Score: 800  
Time Limit: 120 min  
File Version: 24.5



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

**Exam Code: 640-864**

**Exam Name: Cisco Designing for Cisco Internetwork Solutions 2011**



## Exam A

### QUESTION 1

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 2

Characterizing an existing network requires gathering as much information about the network as possible. Which of these choices describes the preferred order for the information-gathering process?

- A. Site and network audits, traffic analysis, existing documentation and organizational input
- B. Existing documentation and organizational input, site and network audits, traffic analysis
- C. Traffic analysis, existing documentation and organizational input, site and network audits
- D. Site and network audits, existing documentation and organizational input, traffic analysis

**Correct Answer:** B

**Section:** (none)

**Explanation**

#### **Explanation/Reference:**

Explanation:

This section describes the steps necessary to characterize the existing network infrastructure and all sites. This process requires three steps:

- Step 1. Gather existing documentation about the network, and query the organization to discover additional information. Organization input, a network audit, and traffic analysis provide the key information you need. (Note that existing documentation may be inaccurate.) Step 2. Perform a network audit that adds detail to the description of the network. If possible, use traffic-analysis information to augment organizational input when you are describing the applications and protocols used in the network.
- Step 3. Based on your network characterization, write a summary report that describes the health of the network. With this information, you can propose hardware and software upgrades to support the network requirements and the organizational requirements.

### QUESTION 3

You want to gather as much detail as possible during a network audit with a minimal impact on the network devices themselves.

Which tool would you use to include data time stamping across a large number of interfaces while being customized according to each interface?

- A. RMON
- B. SNMPv3
- C. NetFlow
- D. Cisco Discovery Protocol

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 4

Which three are considered as technical constraints when identifying network requirements? (Choose three.)

- A. Support for legacy applications
- B. Bandwidth support for new applications
- C. Limited budget allocation
- D. Policy limitations
- E. Limited support staff to complete assessment
- F. Support for existing legacy equipment
- G. Limited timeframe to implement

**Correct Answer:** ABF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Network design might be constrained by parameters that limit the solution. Legacy applications might still exist that must be supported going forward, and these applications might require a legacy protocol that may limit a design. Technical constraints include the following:

Existing wiring does not support new technology.

Bandwidth might not support new applications.

The network must support exiting legacy equipment.

Legacy applications must be supported (application compatibility).

### QUESTION 5

In which phase of PPDIOO are the network requirements identified?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

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

Plan Phase

The Plan phase identifies the network requirements based on goals, facilities, and user needs. This phase characterizes sites and assesses the network, performs a gap analysis against best- practice architectures, and looks at the operational environment. A project plan is developed to manage the tasks, responsible parties, milestones, and resources to do the design and implementation. The project plan aligns with the scope, cost, and resource parameters established with the original business requirements. This project plan is followed (and updated) during all phases of the cycle.

#### QUESTION 6

Which is part of the Prepare phase of PPDIOO?

- A. Obtain site contact information
- B. Perform network audit
- C. Identify customer requirements



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

- D. Perform gap analysis

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

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

#### Prepare Phase

The Prepare phase establishes organization and business requirements, develops a network strategy, and proposes a high-level conceptual architecture to support the strategy. Technologies that support the architecture are identified. This phase creates a business case to establish a financial justification for a network strategy.

#### QUESTION 7

During which phase of the PPDIOO model would you conduct interviews with supporting staff to develop and propose a viable solution?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

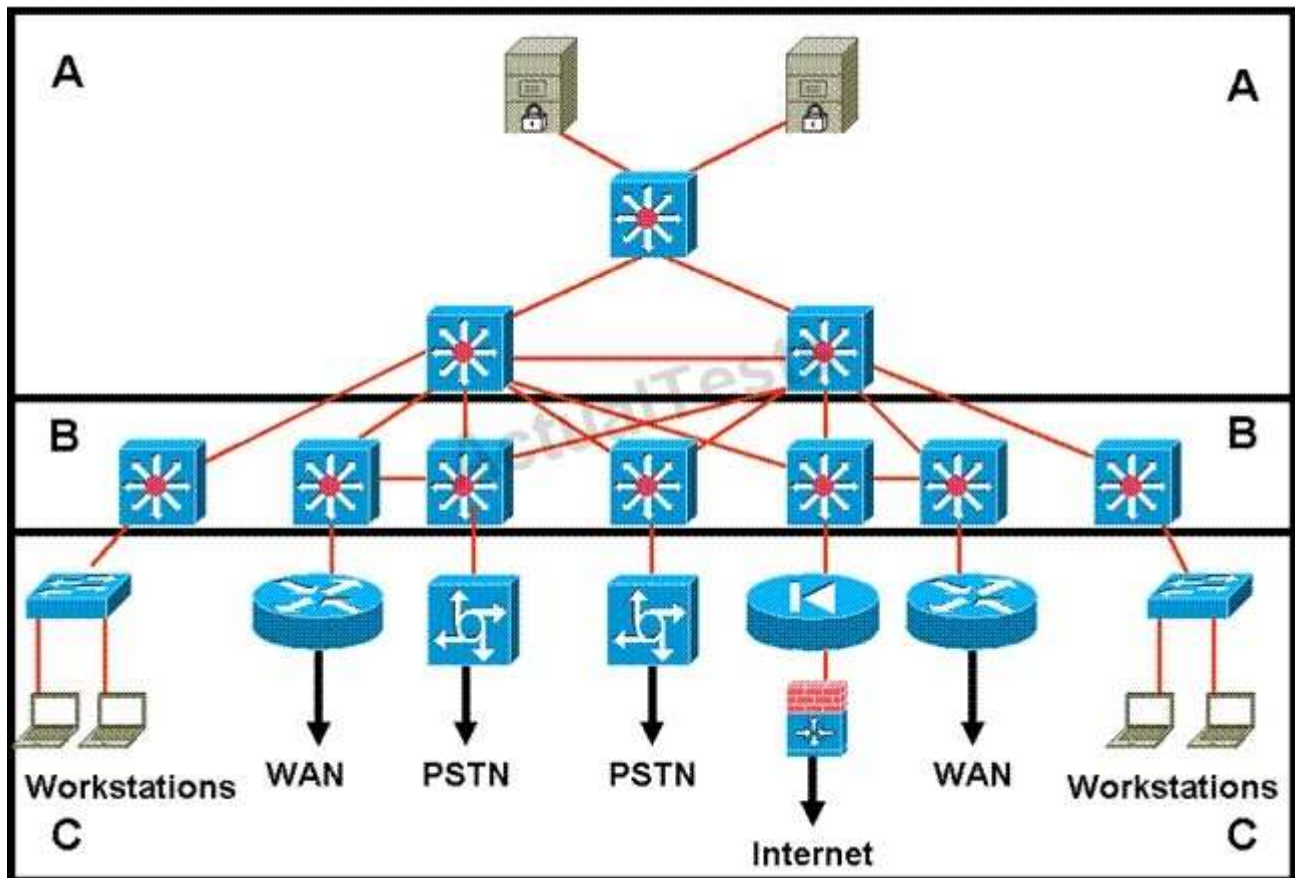
PPDIOO Phase	Description
Prepare	Establishes organization and business requirements, develops a network strategy, and proposes a high-level architecture
Plan	Identifies the network requirements by characterizing and assessing the network, performing a gap analysis
Design	Provides high availability, reliability, 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

### Prepare Phase

The Prepare phase establishes organization and business requirements, develops a network strategy, and proposes a high-level conceptual architecture to support the strategy. Technologies that support the architecture are identified. This phase creates a business case to establish a financial justification for a network strategy.

### QUESTION 8

Refer to the exhibit.



Which statement accurately represents the characteristics of the core layer in this design?

- A. QoS should only be performed only in the core.
- B. Load balancing should never be implemented or used.
- C. Access lists should be used in the core to perform packet manipulation.
- D. Partial mesh should be used as long as it is connected to each device by multiple paths.
- E. Policy-based traffic control should be implemented to enable prioritization and ensure the best performance for all time-critical applications.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 9

What are the three primary functions of the distribution layer of the campus network design hierarchy? (Choose three.)

- A. provide end-user connectivity
- B. provide high speed transport
- C. provide QoS services
- D. enforce security policies
- E. provide WAN connections
- F. connect access devices to the core backbone

**Correct Answer:** CDF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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

#### **QUESTION 10**

Which of the following is a component within the Cisco Enterprise Campus module?

- 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 11**

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 12**

Which three solutions are part of the Borderless Network Services? (Choose three.)

- A. Wireless
- B. Routing
- C. TrustSec

- D. MediaNet
- E. Switching
- F. EnergyWise
- G. Next-Gen WAN

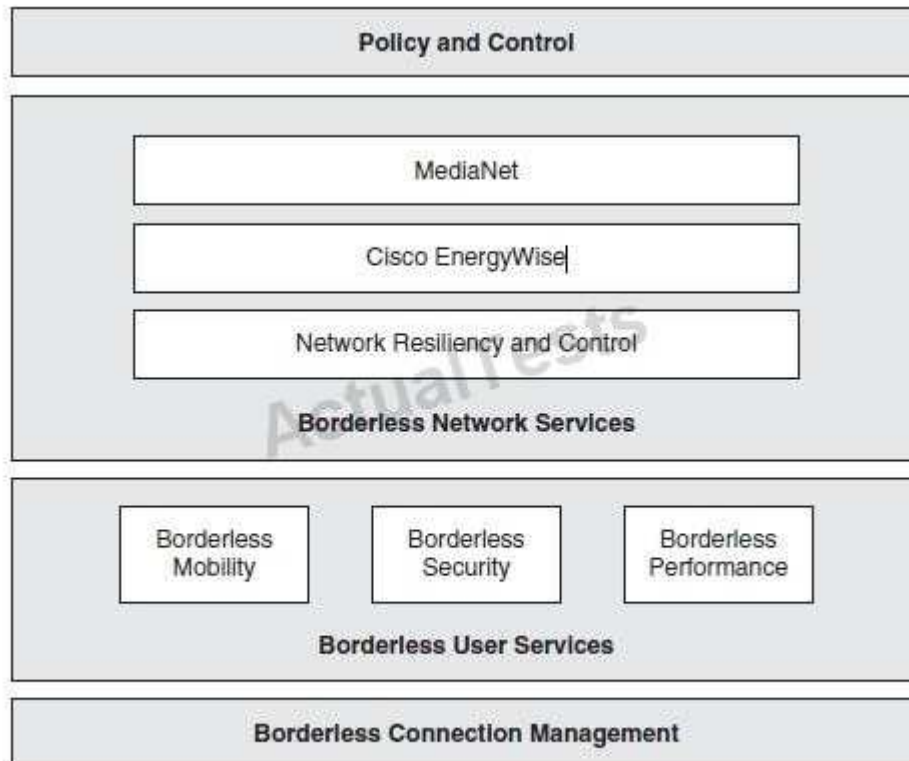
**Correct Answer:** CDF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:



**Figure 1-2** *Borderless Architecture*

### QUESTION 13

Which three modular components are part of the Cisco Enterprise Edge Architecture? (Choose three.)

- A. e-commerce module
- B. Internet connectivity module
- C. server farm module
- D. remote access and VPN module
- E. PSTN services module
- F. enterprise branch module
- G. building distribution module

**Correct Answer:** ABD

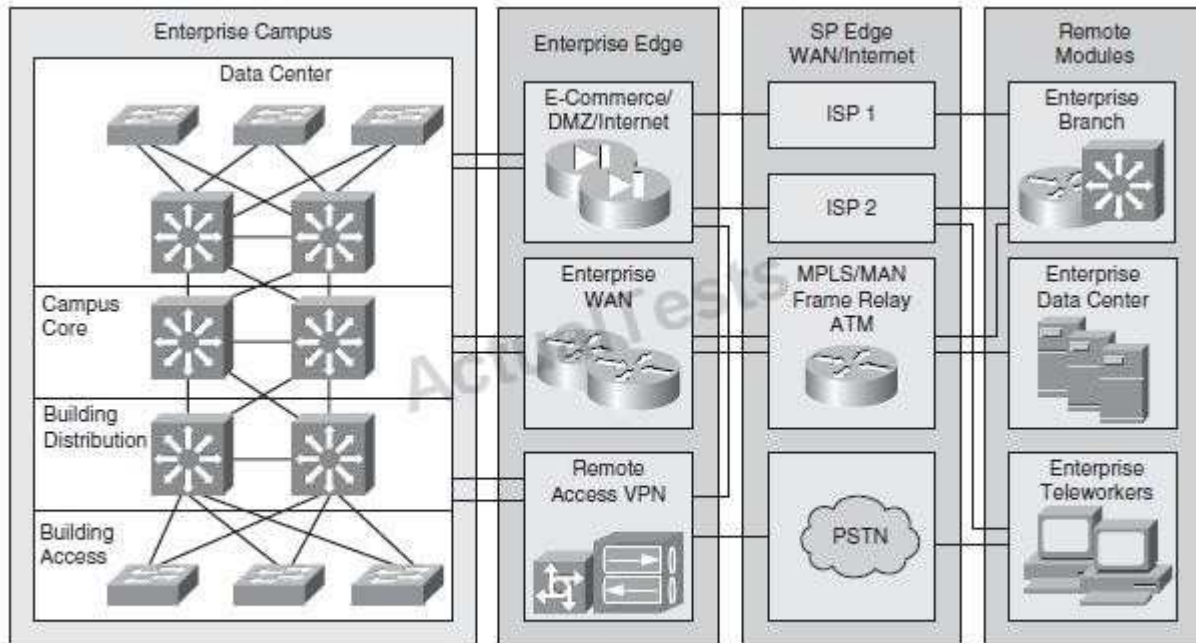
**Section:** (none)

**Explanation**



**Explanation/Reference:**

Explanation:



**Figure 2-5** *Cisco Enterprise Architecture Model*

**QUESTION 14**

Where in the Cisco Enterprise Architecture model does network management reside?

- A. Enterprise data center module
- B. Enterprise campus module
- C. Enterprise edge module
- D. Service Provider edge module
- E. Service Provider data center module

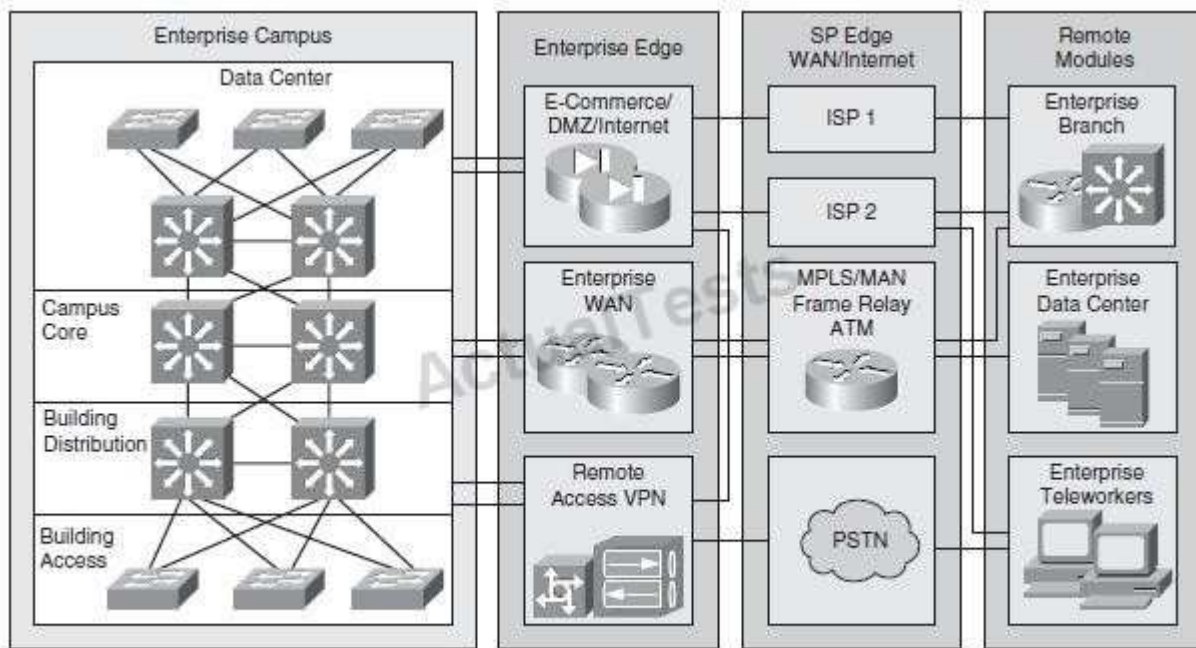
**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:



**Figure 2-5** *Cisco Enterprise Architecture Model*

The network management servers reside in the campus infrastructure but have tie-ins to all the components in the enterprise network for monitoring and management.

#### QUESTION 15

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

- 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

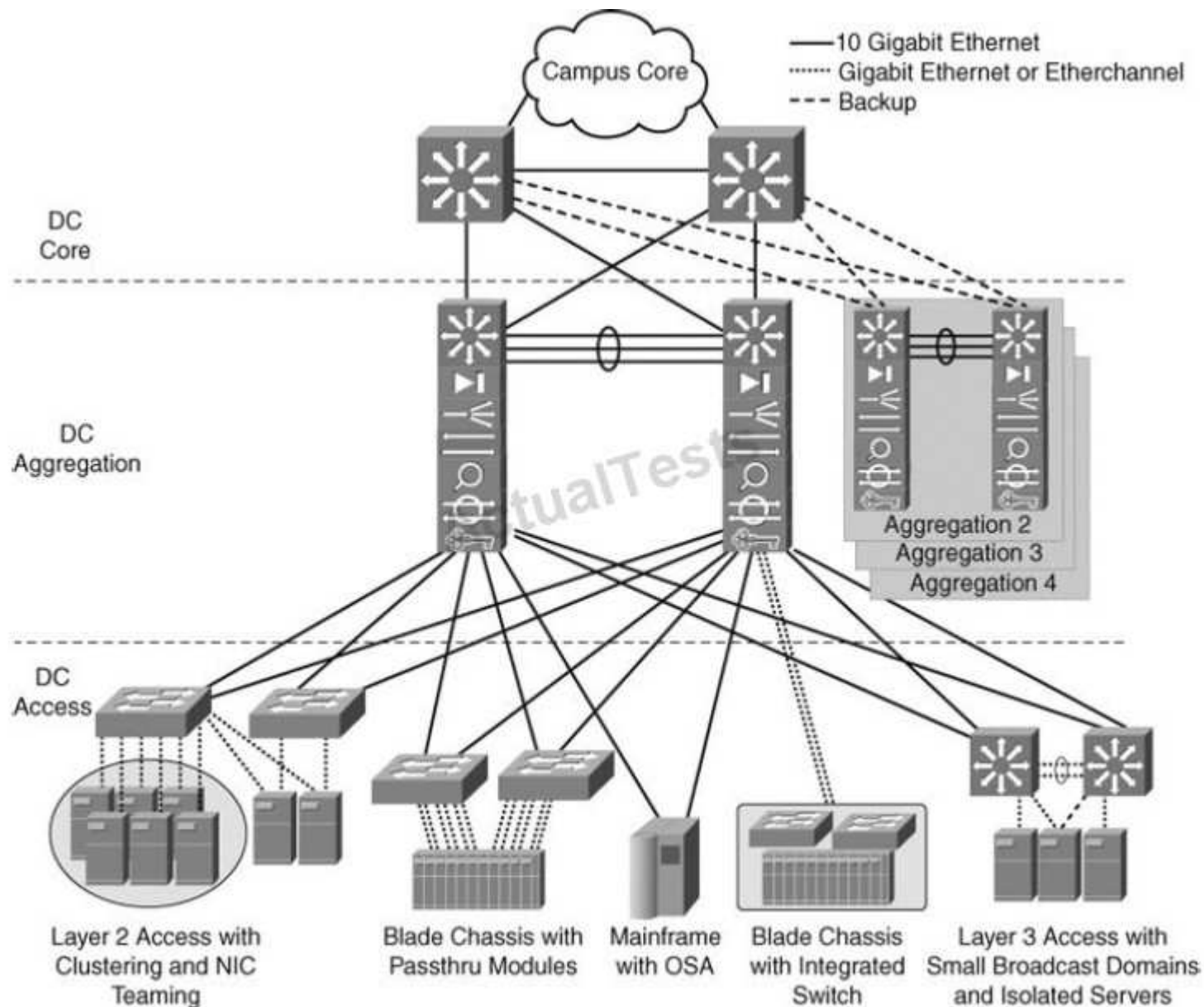
**Section:** (none)

**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



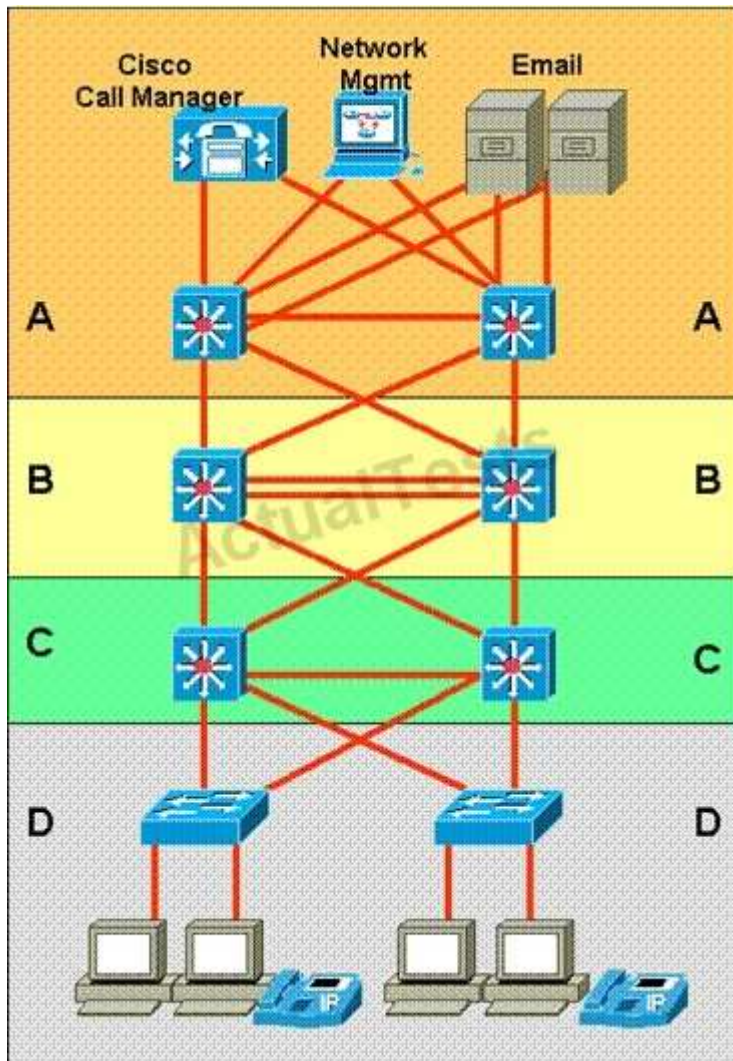
#### Defining the DC Access Layer

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 16

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 17

What is the 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 choiceE.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 18

The evolution of the Data Center is best represented by the 3.0 architecture component of virtualization.Which of the following is not an example of the virtualization taking place in the Data Center?

- A. Virtualized media access utilizing Fibre Channel over Ethernet
- B. VLANs and virtual storage area networks (VSANs) provide for virtualized LAN and SAN connectivity, separating physical networks and equipment into virtual entities
- C. Virtual Machines that run an application within the client operating system, which is further virtualized and running on common hardware
- D. Storage devices virtualized into storage pools, and network devices are virtualized using device contexts

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 19

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 upon 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 20

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 interfaces 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 21

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 22**

When there is a need for immunity to EMI for connecting locations that are greater than 100 meters apart, which two solutions can be utilized? (Choose two.)

- A. multimode fiber
- B. Fibre Channel
- C. HVDC transmission lines
- D. single-mode fiber
- E. serial RS-232
- F. Gigabit Ethernet 1000BASE-CX

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 23**

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

- A. The access layer in the data center is typically built at Layer 3, which allows for better sharing of services across multiple servers.
- B. With Layer 2 access, the default gateway for the servers can be configured at the access or aggregation layer.
- C. A dual-homing NIC requires a VLAN or trunk between the two access switches to support the dual IP addresses on the two server links to two separate switches.
- D. 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](http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a00805fcc bf.pdf)

**QUESTION 24**

Which layer of the OSI model does Cisco recommend to place the enterprise network core layer, when designing a network based on its switched hierarchical design?

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 25**

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 26**

Your supervisor wants you to recommend a management protocol that will allow you to track overall bandwidth utilization, utilization by traffic type, and utilization by source and destination. Which is ideally suited for this function?

- A. MRTG
- B. NetFlow
- C. RRD
- D. SNMP

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

NetFlow

Cisco NetFlow allows the tracking of IP flows as they are passed through routers and multilayer switches. IP flows are a set of IP packets within a specific timeslot that share a number of properties, such as the same source address, destination address, type of service, and protocol number. NetFlow information is forwarded to a network data analyzer, network planning tools, RMON applications, or accounting and billing applications. Net-Flow allows for network planning, traffic engineering, billing, accounting, and application monitoring. The most recent version of NetFlow is NetFlow Version 9, which is defined in RFC 3954. NetFlow consists of three major components:

#### **QUESTION 27**

Which of the following three options represents the components of the Teleworker Solution? (Choose three.)

- A. Cisco Unified IP Phone
- B. Cisco 880 Series Router
- C. Aironet Office Extend Access Point
- D. Catalyst 3560 Series Switch
- E. Cisco 2900 Series Router
- F. MPLS Layer 3 VPN
- G. Leased lines

**Correct Answer: ABE**



**Section: (none)**  
**Explanation**

**Explanation/Reference:**

Explanation:

A Cisco ASR is used to terminate Teleworker solutions, not a 2900 series router.

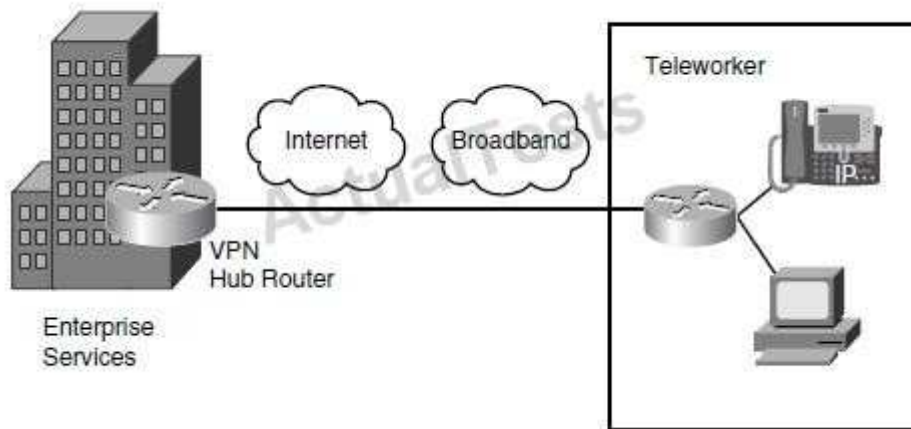
Hybrid teleworker uses Aironet, Advanced teleworker uses 880, both use IP phones.

google: "at\_a\_glance\_c45-652500.pdf" for details

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.

**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.



**QUESTION 28**

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?

- A. Dynamic load balancing, or salt-and-pepper access point design, avoids the potential impact of oversubscription on aggregate network performance.
- B. N+N redundancy configuration allows logically grouping access points on controllers to minimize intercontroller roaming events.
- C. N+N+1 redundancy configuration has the least impact to system management because all of the controllers are colocated in an NOC or data center.
- D. 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.

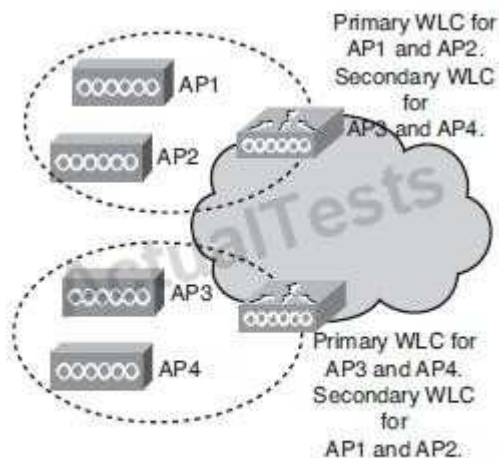
Link: <http://www.cisco.com/web/learning/le31/le46/cln/qlm/CCDA/design/understanding-wireless-network-controller-technology-3/player.html>

**N+N WLC Redundancy**

With N+N redundancy, shown in Figure 5-14, an equal number of controllers back up each other. For example, a pair of WLCs on one floor serves as a backup to a second pair on another floor. The top WLC is primary for AP1 and AP2 and secondary for AP3 and AP4. The bottom WLC is primary for AP3 and AP4 and secondary for AP1 and AP2. There should be enough capacity on

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 70  
Cisco 640-864 Exam

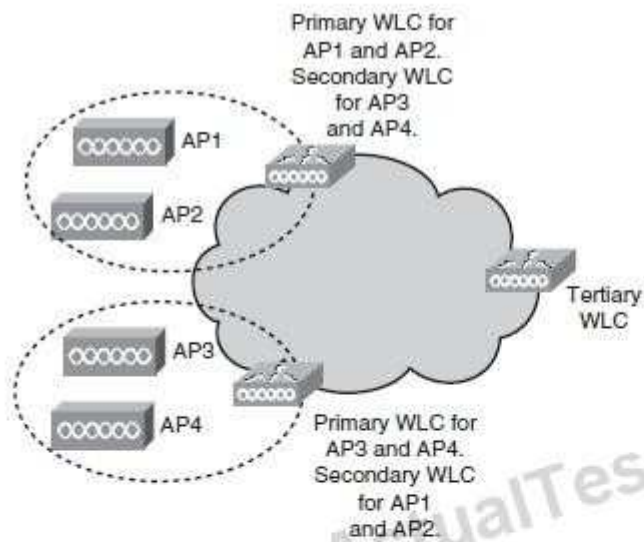
each controller to manage a failover situation.



**Figure 5-14** N+N Controller Redundancy

**N+N+1 WLC Redundancy**

With N+N+1 redundancy, shown in Figure 5-15, an equal number of controllers back up each other (as with N+N), plus a backup WLC is configured as the tertiary WLC for the APs. N+N+1 redundancy functions the same as N+N redundancy plus a tertiary controller that backs up the secondary controllers. The tertiary WLC is placed in the data center or network operations center



**Figure 5-15** *N+N+1 Controller Redundancy*

Table 5-9 covers WLC redundancy.

**Table 5-9** *WLC Redundancy*

WLC Redundancy	Description
N+1	A single WLC acts as the backup for multiple WLCs. The backup WLC is configured as the secondary on APs.
N+N	An equal number of controllers back up each other.
N+N+1	An equal number of controllers back up each other. The backup WLC is configured as the tertiary on APs.

## Exam B

### QUESTION 1

Which factor would be most influential in choosing multimode fiber optic connections over UTP?

- A. signal attenuation
- B. required bandwidth
- C. required distance
- D. electromagnetic interference
- E. cost

**Correct Answer:** C

**Section:** (none)

**Explanation**

#### **Explanation/Reference:**

Explanation:

Cabling has several key characteristics, such as the physical connector, media type, and cable length. Copper and fiber-optic cables are commonly used today. Fiber-optic cabling allows for longer distances and is less prone to interference than copper cabling. The two main types of optical fiber are single-mode and multi-mode. Copper cabling is widely available, costs less, and generally covers shorter distances (up to 100 meters, about 328 feet). Typical copper cabling found in the data center is CAT 5e/CAT 6 with RJ-45 connectors.

### QUESTION 2

Which three are associated with the distribution layer within the campus design? (Choose three.)

- A. access layer aggregation
- B. route summarization
- C. network trust boundary
- D. next-hop redundancy
- E. layer 2 switching
- F. port security
- G. broadcast suppression

**Correct Answer:** ABD

**Section:** (none)

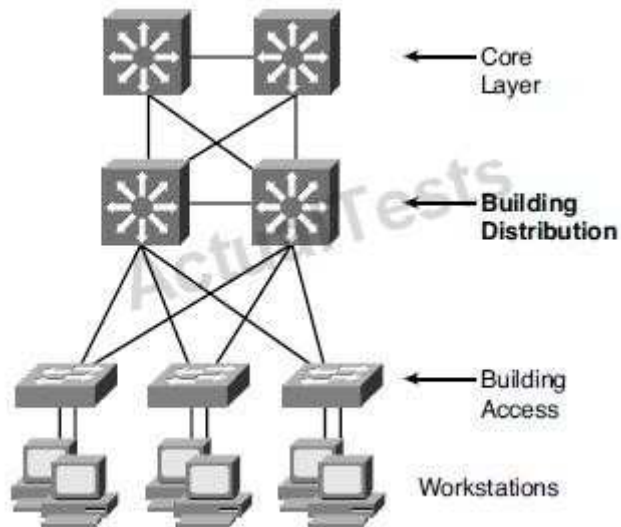
**Explanation**

#### **Explanation/Reference:**

Explanation:

Distribution Layer Best Practices

As shown in Figure 3-6, the distribution layer aggregates all closet switches and connects to the core layer. Design considerations for the distribution layer include providing wirespeed performance on all ports, link redundancy, and infrastructure services. The distribution layer should not be limited on performance. Links to the core must be able to support the bandwidth used by the aggregate access layer switches. Redundant links from the access switches to the distribution layer and from the distribution layer to the core layer allow for high availability in the event of a link failure. Infrastructure services include quality of service (QoS) configuration, security, and policy enforcement. Access lists are configured in the distribution layer.



The following are recommended best practices at the distribution layer:

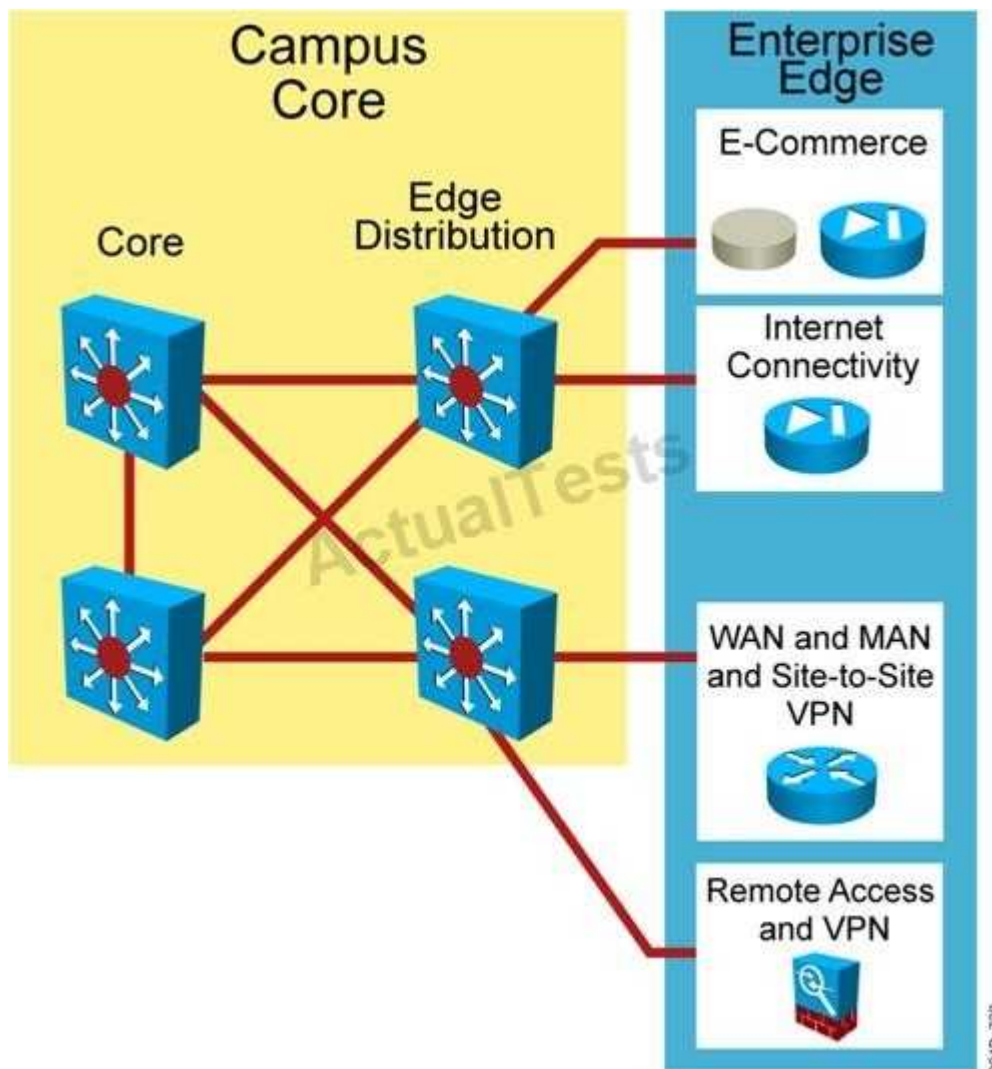
Use first-hop redundancy protocols. Hot Standby Router Protocol (HSRP) or Gateway Load Balancing Protocol (GLBP) should be used if you implement Layer 2 links between the Layer 2 access switches and the distribution layer.

Use Layer 3 routing protocols between the distribution and core switches to allow for fast convergence and load balancing.

Only peer on links that you intend to use as transit.

### QUESTION 3

Refer to the exhibit.



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 4

OSPF will be used as the IGP within a campus network. Which two things should you consider before deployment? (Choose two.)

- A. All areas need to connect back to area 0.
- B. The OSPF process number on each router should match.
- C. NSSA areas should be used when an area cannot connect directly to area 0.

- D. Stub areas should be connected together using virtual links.
- E. ECMP may cause undesired results depending on the environment.

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 5**

High availability is a key design consideration in the enterprise campus network. In a fully redundant topology, which is likely to provide faster IGP convergence during a failure?

- A. redundant supervisors
- B. redundant supervisors with Cisco Nonstop Forwarding (NSF) and Stateful Switchover (SSO)
- C. single supervisors with tuned IGP timers
- D. single supervisors

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

In a fully redundant topology with tuned IGP timers, adding redundant supervisors with Cisco nonstop forwarding (NSF) and stateful switchover (SSO) may cause longer convergence times than single supervisors with tuned IGP timers. NSF attempts to maintain the flow of traffic through a router that has experienced a failure. NSF with SSO is designed to maintain a link-up Layer 3 up

state during a routing convergence event. However, because an interaction occurs between the IGP timers and the NSF timers, the tuned IGP timers can cause NSF-aware neighbors to reset the neighbor relationships.

#### **QUESTION 6**

Which Cisco technology using Nexus NX-OS infrastructure allows the network architect to create up to four separate control and data plane instances of the Nexus chassis?

- A. virtual port-channel
- B. virtual routing and forwarding
- C. virtual switching system
- D. virtual device context

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Virtualization

Virtual local-area network (VLAN), virtual storage-area network (VSAN), and virtual device contexts (VDC) help to segment the LAN, SAN, and network devices instances. Cisco Nexus 1000V virtual switch for VMware ESX and ESXi help to deliver visibility and policy control for virtual machines (VM).

Flexible networking options with support for all server form factors and vendors, including support for blade servers from Cisco, Dell, IBM, and HP with integrated Ethernet and Fibre Channel switches.

**QUESTION 7**

An enterprise campus module is typically made up of four submodules, as described by the Cisco Enterprise Architecture Model. Which two submodules are part of this module?

- A. DMZ
- B. enterprise branch
- C. building distribution
- D. server farm/data center
- E. MAN

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 8**

Which three options are valid Cisco STP tools used to ensure best-practice access layer design for the enterprise campus? (Choose three.)

- A. Portfast
- B. UDLD
- C. Root Guard
- D. BPDU Guard
- E. Flex Links
- F. SPAN
- G. EtherChannel

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

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

Use RPVST+ if STP is required. It provides the best convergence.

Set trunks to ON and ON with no-negotiate

Manually prune unused VLANs to avoid broadcast propagation. Use 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 Cisco STP Toolkit, which provides PortFast, Loop Guard, Root Guard, and BPDU Guard.

**QUESTION 9**

Which is a factor in enterprise campus design decisions?

- A. network application characteristics
- B. routing protocol characteristics
- C. switching latency characteristics
- D. packet filtering characteristics



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Campus LAN Design and Best Practices

LANs can be classified as large-building LANs, campus LANs, or small and remote LANs. The large-building LAN typically contains a major data center with high-speed access and floor communications closets; the large-building LAN is usually the headquarters in larger companies. Campus LANs provide connectivity between buildings on a campus. Redundancy is usually a requirement in large-building and campus LAN deployments. Small and remote LANs provide connectivity to remote offices with a relatively small number of nodes. Campus design factors include the following categories:

Network application characteristics: Different application types  
Infrastructure device characteristics: Layer 2 and Layer 3 switching, hierarchy  
Environmental characteristics: Geography, wiring, distance, space, power, number of nodes

Applications are defined by the business, and the network must be able to support them. Applications may require high bandwidth or be time sensitive. The infrastructure devices influence the design. Decisions on switched or routed architectures and port limitations influence the design. The actual physical distances affect the design. The selection of copper or fiber media may be influenced by the environmental or distance requirements. The following sections show some sample LAN types. Table 3-8 summarizes the different application types.

#### **QUESTION 10**

Spanning Layer 2 across geographically separate data centers is a key consideration for current data center designs. Which is the name of the NX-OS technology that facilitates MAC in IP transport for Layer 2 VLANs across any IP network?

- A. Overlay Transport Virtualization
- B. Virtual Private LAN Services
- C. Generic Routing Encapsulation
- D. QinQ tunneling

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 11**

Which network virtualization technology involves creating virtual routers with its own individual routing tables on a physical router?

- A. VSS
- B. vPC
- C. VRF
- D. VLAN

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

VRF Virtual routing and forwarding. A routing virtualization technology that creates multiple logical Layer 3 routing and forwarding instances (route tables) that can function on the same physical router.

#### QUESTION 12

In the enterprise data center, which are the three main components? (Choose three.)

- A. Network Infrastructure
- B. Interactive services
- C. Data Center Management
- D. Internet services
- E. WAN services
- F. VPN and remote access

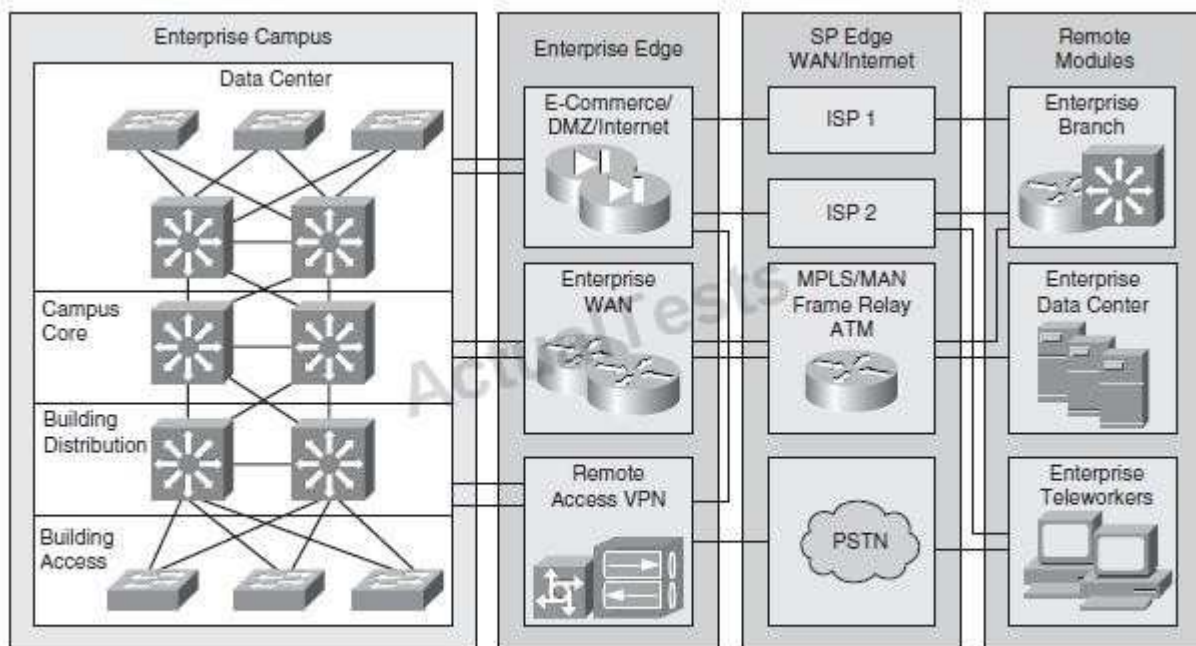
**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:



**Figure 2-5** Cisco Enterprise Architecture Model

Network infrastructure: Gigabit and 10 Gigabit Ethernet, InfiniBand, optical transport and storage switching

Interactive services: Computer infrastructure services, storage services, security, application optimization

DC management: Cisco Fabric Manager and Cisco VFrame for server and service management

#### QUESTION 13

Which one of these statements describes why, from a design perspective, a managed VPN approach for enterprise teleworkers is 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 hotel, 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 14**

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

#### **QUESTION 15**

What are three key areas that need to be considered when designing a remote data center? (Choose three.)

- A. power diversity
- B. active directory services
- C. Cisco IOS versions
- D. data storage
- E. applications
- F. user access
- G. packet routing

**Correct Answer:** ADE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 16

If a teleworker is required to access the branch office via a secure IPSEC VPN connection, which technology is recommended to provide the underlying transport?

- A. ISDN
- B. Metro Ethernet
- C. Frame Relay
- D. ADSL
- E. ATM

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Enterprise Teleworker Design

All the remote edges of the network is another branch office known as enterprise teleworkers. Cisco developed a solution called Cisco Virtual Office Solution, which was designed with the enterprise teleworker in mind. As organizations continually try to reduce costs and improve employee productivity, working from home is becoming an increasingly popular option for businesses and organizations. This approach allows employees to manage their work schedules more effectively and increase their productivity. This also results in greater job satisfaction and flexibility in the work schedules. The work-from-home teleworker is an extension of the enterprise and serves as the basis for the enterprise teleworker solution.

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.

#### QUESTION 17

Which three describe challenges that are faced when deploying an environment for teleworkers? (Choose three.)

- A. supporting a mix of technically knowledgeable and nontechnical users
- B. simplifying router installation and configuration
- C. verifying available power at employee's house for necessary equipment
- D. avoiding situations where employees might use nonstandard hardware or configurations
- E. reducing daily commuting time to main office location
- F. providing access to FTP servers located in main office location
- G. implementing leased line connectivity between main office and employee's home location

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 18**

Which model of ISR is utilized for the teleworker design profile?

- A. Cisco 1900 Series
- B. Cisco 1800 Series
- C. Cisco 800 Series
- D. Cisco 500 Series

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

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.

#### **QUESTION 19**

You need to connect to a remote branch office via an Internet connection. The remote office does not use Cisco equipment. This connection must be secure and must support OSPF.

Which of the following can be used to transport data to the branch office?

- A. GRE over IPsec
- B. IPsec
- C. GRE
- D. IPsec VTI

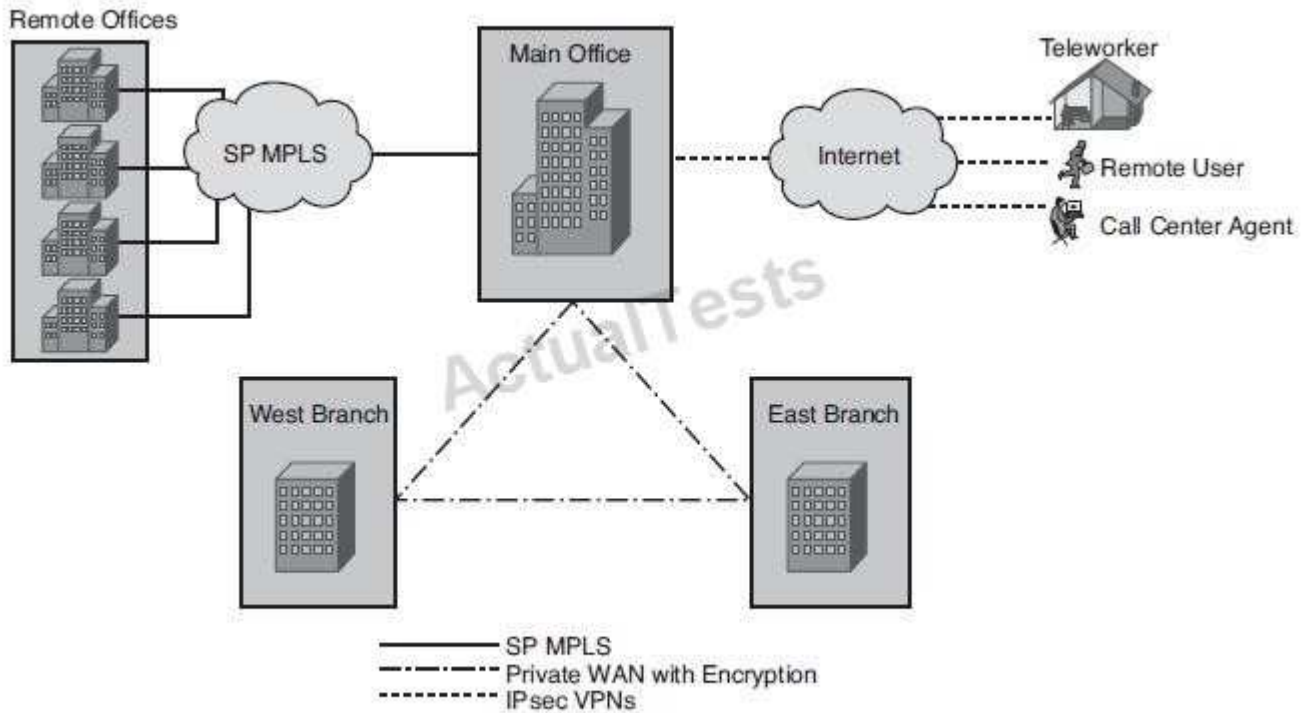
**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:



**Figure 7-6** WAN Architectures

**QUESTION 20**

When designing a WAN backup for voice and video applications, what three types of connections should be used? (Choose three.)

- A. Private WAN
- B. internet
- C. ISDN
- D. MPLS
- E. dial-up
- F. ATM
- G. DSL

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Critical thing here is voice/video backup for which we need at least 768 KB/s (CCDP)

**QUESTION 21**

Which two are characteristics of a Lightweight Access Point? (Choose two.)

- A. managed via a central wireless LAN controller
- B. code upgrade performed via a TFTP server
- C. CAPWAP tunnels
- D. managed directly via CLI or web interface
- E. facilitates the creation of its own WLANs and port mappings

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Cisco Unified Wireless Network (UWN) architecture, Control and Provisioning for Wireless Access Point (CAPWAP), WLAN controller components, roaming, and mobility groups. Cisco UWN components provide scalable WLAN solutions using WLAN controllers to manage LWAPs. The CCDA must understand how these components work with each other, how they scale, and how roaming and mobility groups work.

**QUESTION 22**

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

**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](http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.shtml)

#### QUESTION 24

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

- A. One-way route redistribution avoids the requirement for static 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:

Routing Protocols on the Hierarchical Network Infrastructure The selected routing protocol should be used based on the network design goals and the network

module being used. As shown in Figure 11-23, high-speed routing is recommended for the network core and distribution layers. These routing protocols react fast to network changes. It is a best practice that the same routing protocol be used in the three layers (core, distribution, access) of the enterprise network.

The enterprise edge connects the campus network with external connectivity including WAN, Internet, VPN, remote-access modules. Routing protocols in the enterprise edge may be EIGRP, OSPF, BGP, and static routes. Specifically in the Internet module you will find BGP/static routes.

Table 11-9 shows a summary of the recommended routing protocols in the network infrastructure.

**Table 11-9** *Routing Protocols on the Hierarchical Network Infrastructure*

Network Module	Routing Protocols
Campus core	EIGRP, OSPF
Campus distribution	EIGRP, OSPF
Enterprise edge	EIGRP, OSPF, BGP, Static
Internet and VPN modules	BGP, Static

#### QUESTION 25

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:

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

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

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 34

Cisco 640-864 Exam

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](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 26

Which three types of WAN topologies can be deployed in the Service Provider Module? (Choose three.)

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

**Correct Answer:** BCF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 27

Which statement describes the recommended deployment of DNS and DHCP servers in the Cisco Network Architecture for the Enterprise?

- 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.

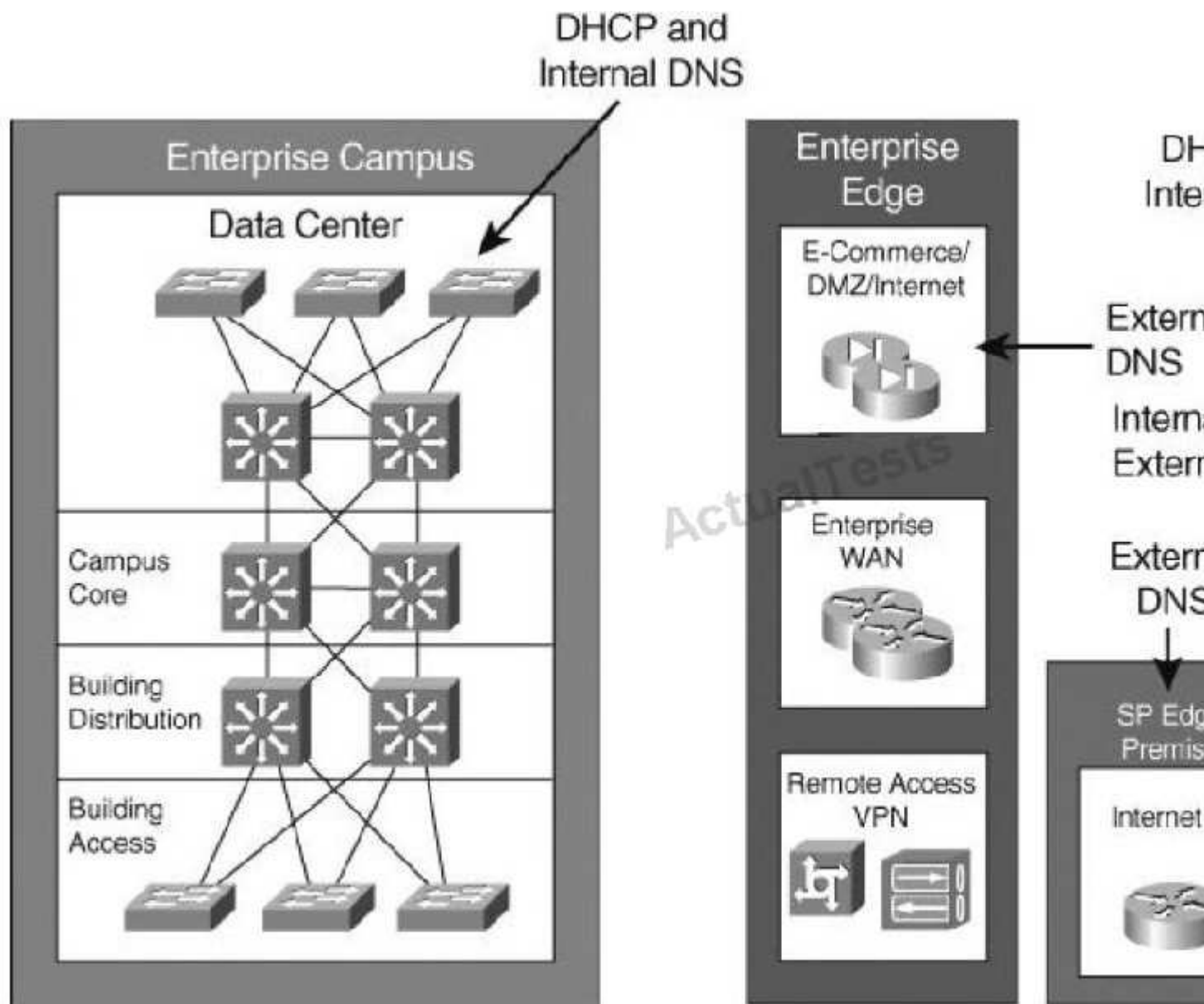
**Correct Answer:** B

**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.



"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 67  
Cisco 640-864 Exam

#### QUESTION 28

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:

## Exam C

### QUESTION 1

When designing an EIGRP network, which two things should you take into consideration? (Choose two.)

- A. ASN and K values must match.
- B. The neighbor command can be used to enable unicast communication.
- C. The neighbor diameter cannot exceed a 15-hops limit.
- D. NSSA areas can be used to redistribute external routes.
- E. Neighbor relationship can be established with non-Cisco routers.

**Correct Answer:** AB

**Section:** (none)

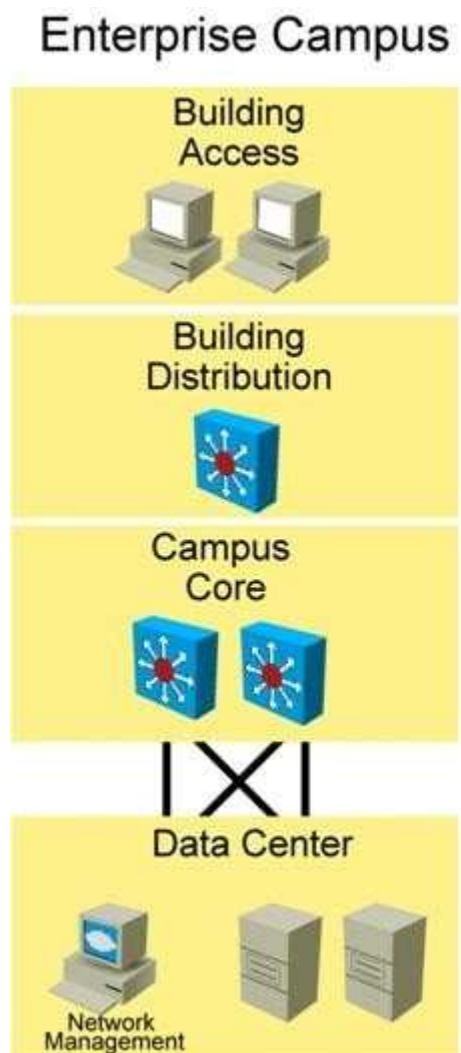
**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 2

Refer to the exhibit.



Which three modules would typically utilize public IPv4 addressing?(Choose three.)

- A. Access
- B. Distribution
- C. Core
- D. Data Center
- E. E-Commerce
- F. Internet Connectivity
- G. Remote Access/VPN
- H. WAN/MAN
- I. Branch
- J. Branch Data Center

**Correct Answer:** EFG

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 3

Which is the North American RIR for IPv4 addresses?

- A. RIPE
- B. ARIN
- C. IANA
- D. IEEE
- E. APNIC

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 4

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 5

What is the most compact representation of the following IPv6 address?

2001:db8:0000:0000:cafe:0000:0000:1234

- A. 2001:db8::cafe::1234
- B. 2001:db8::cafe:0000:0000:1234
- C. 2001:db8:0:0:cafe::1234
- D. 2001:db8::cafe:0:1234

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 6

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 7

Which subnet address and mask would you use for all Class D multicast addresses to be matched within an access list?

- A. 224.0.0.0/20
- B. 224.0.0.0/4
- C. 239.0.0.0/24
- D. 239.0.0.0/8
- E. 225.0.0.0/8

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 8

Which three items pertain to EIGRP? (Choose three.)

- A. Can use multiple unequal paths.
- B. Routes are redistributed as type 2 by default.
- C. ASN and K values must match to form neighbors.
- D. Uses multicast address 224.0.0.9 for updates.
- E. Exchanges full routing table every 30 seconds.
- F. Summary routes have AD of 90.
- G. External routes have AD of 170.

**Correct Answer:** ACG

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 9

Which type of area should you use in an enterprise OSPF deployment if you want to prevent propagation of type 5 LSAs but still allow the redistribution of external routes?

- A. stub
- B. totally stubby
- C. backbone
- D. NSSA
- E. virtual link

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

NSSAs

Notice that Area 2 in Figure 11-5 has an ASBR. If this area is configured as an NSSA, it generates the external LSAs (Type 7) into the OSPF system while retaining the characteristics of a stub area to the rest of the autonomous system. There are two options for the ABR. First, the ABR for Area 2 can translate the NSSA external LSAs (Type 7) to autonomous system external LSAs (Type 5) and flood the rest of the internetwork. Second, the ABR is not configured to convert the NSSA external LSAs to Type 5 external LSAs, and therefore the NSSA external LSAs remain within the NSSA.

There is also an NSSA totally stub area. The difference is that the default NSSA has no default route unless the ABR is explicitly configured to advertise one. The NSSA totally stub area does receive a default route.

#### QUESTION 10

Your supervisor has asked you to deploy a routing protocol within the lab environment that will allow for unequal cost multipath routing. Which should you choose?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**



**Explanation/Reference:**

Explanation:

**QUESTION 11**

A hierarchical design of the EIGRP domain facilitates which two of the following? (Choose two.)

- A. route summarization
- B. faster convergence
- C. unequal cost load balancing
- D. redistribution
- E. virtual links

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Hierarchical Versus Flat Routing Protocols

Some routing protocols require a network topology that must have a backbone network defined. This network contains some, or all, of the routers in the internetwork. When the internetwork is defined hierarchically, the backbone consists of only some devices. Backbone routers service and coordinate the routes and traffic to or from routers not in the local internetwork. The supported hierarchy is relatively shallow. Two levels of hierarchy are generally sufficient to provide scalability.

Selected routers forward routes into the backbone.

OSPF and IS-IS are hierarchical routing protocols. By default, EIGRP is a flat routing protocol, but it can be configured with manual summarization to support hierarchical designs. Flat routing protocols do not allow a hierarchical network organization. They propagate all routing information throughout the network without dividing or summarizing large networks into smaller areas. Carefully designing network addressing to naturally support aggregation within routing-protocol advertisements can provide many of the benefits offered by hierarchical routing protocols. Every router is a peer of every other router in flat routing protocols; no router has a special role in the internetwork. EIGRP, RIPv1, and RIPv2 are flat routing protocols.

**QUESTION 12**

Which two methods are used to reduce the mesh links required between iBGP peers in the same AS? (Choose two.)

- A. community
- B. router reflectors
- C. local preference
- D. confederations
- E. atomic aggregate
- F. MED

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Route Reflectors

iBGP requires that all routers be configured to establish a logical connection with all other iBGP routers. The logical connection is a TCP link between all iBGP-speaking routers. The routers in each TCP link become BGP peers. In large networks, the number of iBGP-meshed peers can become very large. Network administrators can use route reflectors to reduce the number of required mesh links between iBGP peers. Some routers are

selected to become the route reflectors to serve several other routers that act as route-reflector clients. Route reflectors allow a router to advertise or reflect routes to clients. The route reflector and its clients form a cluster. All client routers in the cluster peer with the route reflectors within the cluster. The route reflectors also peer with all other route reflectors in the internetwork. A cluster can have more than one route reflector.

#### Confederations

Another method to reduce the iBGP mesh within an autonomous system is BGP confederations. With confederations, the autonomous system is divided into smaller, sub autonomous systems, and the whole group is assigned a confederation ID. The sub-ASNs or identifiers are not advertised to the Internet but are contained within the iBGP networks. The routers within each private autonomous system are configured with the full iBGP mesh. Each sub-autonomous system is configured with eBGP to communicate with other sub-autonomous systems in the confederation. External autonomous systems see only the ASN of the confederation, and this number is configured with the BGP confederation identifier.

#### QUESTION 13

Which is usually used to connect to an upstream ISP?

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

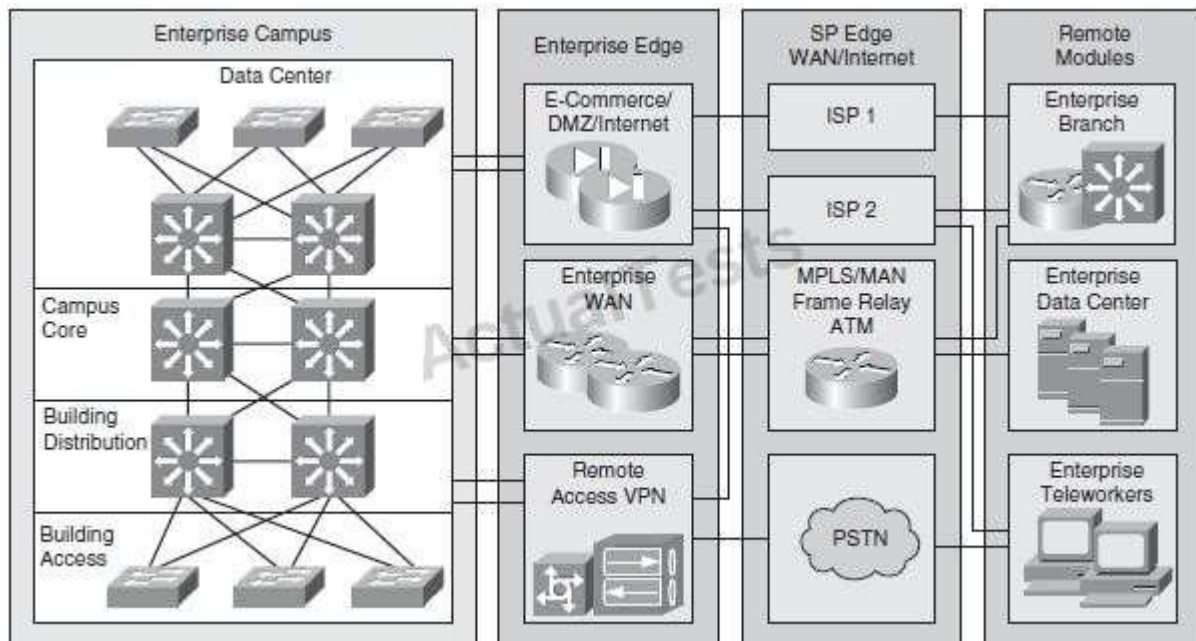
**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:



#### QUESTION 14

A company wants to use private IP addresses for all its internal hosts. Which technology can the company use to provide access to the Internet using a single public IP address?

- A. static NAT

- B. source routing
- C. ACL
- D. PAT

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 15**

You are designing a network that requires a routing protocol that will use minimal network bandwidth. Which would satisfy this requirement?

- A. RIPv2
- B. RIPv6
- C. OSPF
- D. ARP
- E. EGP

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 16**

At which layer of the network is route summarization recommended?

- A. data link layer
- B. core layer
- C. distribution layer
- D. access layer

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Distribution

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 VLANs

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

#### QUESTION 17

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:

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 18

A company is implementing an Identity Management solution with these characteristics:

- Existing AAA Server
- Cisco Catalyst switches
- minimal added investments

Which Cisco Trust and Identity Management solution would you recommend?

- A. NAC Appliance
- B. Cisco IBNS
- C. CSM
- D. Cisco Security MARS

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 19**

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:

Campus LAN QoS Considerations

For the access layer of the campus LAN, you can classify and mark frames or packets to apply quality of service (QoS) policies in the distribution or at the enterprise edge. Classification is a fundamental building block of QoS and involves recognizing and distinguishing between different traffic streams. For example, you distinguish between HTTP/HTTPS, FTP, and VoIP traffic. Without classification, all traffic is treated the same.

**QUESTION 20**

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 21**

Which three statements are true regarding the virtual interface on a Cisco Wireless LAN Controller? (Choose three.)

- A. supports mobility management
- B. serves as a DHCP relay
- C. used for all controller to AP communication
- D. supports embedded Layer 3 security

- E. default for out-of-band management
- F. default for in-band management
- G. provides connectivity to AAA servers

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Virtual interface (static, configured at setup, mandatory) is used for Layer 3 security authentication, DHCP relay support, and mobility management.

#### QUESTION 22

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 23

Which is the purpose of the Cisco NAC Profiler?

- A. automates discovery and inventory of all LAN attached devices
- B. generates a profile based on username and group
- C. learns and creates a database of virus definitions based on LAN traffic
- D. a database used to map user VPN accounts

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Cisco NAC Profiler: Enables network administrators to keep a real-time, contextual inventory of all devices in a network. It greatly facilitates the deployment and management of Cisco Network Admission Control (NAC) systems by discovering and tracking the location and type of all LAN- attached endpoints, including those that are not capable of authenticating. It also uses the information about the device to determine the correct policies for NAC to apply.

#### QUESTION 24

Which protocol is used for voice bearer traffic?

- A. MGCP
- B. RTP
- C. SCCP
- D. CDP
- E. ICMP

**Correct Answer:** B

**Section:** (none)

**Explanation**

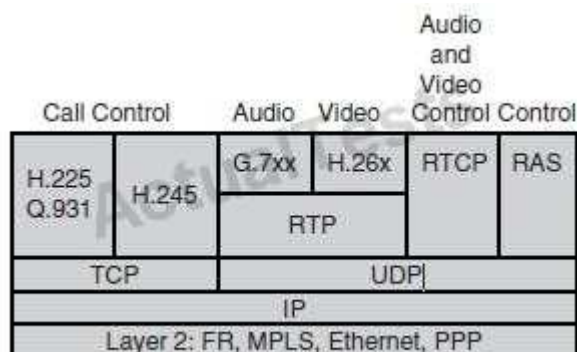
**Explanation/Reference:**

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.



#### QUESTION 25

Cisco Identity-Based Networking Services relies heavily on the 802.1X protocol. Which other authentication solution is used hand-in-hand with 802.1X to authenticate users for network access?

- A. RADIUS
- B. LEAP
- C. IPsec
- D. TACACS
- E. ISAKMP

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Cisco Identity-Based Network Services

The Cisco Identity-Based Network Services solution is a way to authenticate host access based on policy for admission to the network. IBNS supports identity authentication, dynamic provisioning of VLANs on a per-user basis, guest VLANs, and 802.1X with port security. The 802.1 X protocol is a standards-based protocol for authenticating network clients by permitting or denying access to the network. The 802.1 X protocol operates between the end-user client seeking access and an Ethernet switch or wireless access point (AP) providing the connection to the network. In 802.1 X terminology, clients are called supplicants, and switches and APs are called authenticates. A back-end RADIUS server such as a Cisco Access Control Server (ACS) provides the user account database used to apply authentication and authorization. With an IBNS solution, the host uses 802.1X and Extensible Authentication Protocol over LANs (EAPoL) to send the credentials and initiate a session to the network. After the host and switch establish LAN connectivity, username and password credentials are requested. The client host then sends the credentials to the switch, which forwards them to the RADIUS ACS. The RADIUS ACS performs a lookup on the username and password to determine the credentials' validity. If the username and password are correct, an accept message is sent to the switch or AP to allow access to the client host. If the username and password are incorrect, the server sends a message to the switch or AP to block the host port.

Figure 13-4 illustrates the communication flow of two hosts using 802.1X and KAPoL with the switch, AP, and back-end RADIUS server.

#### QUESTION 26

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](http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a008009487e.shtml)

#### QUESTION 27

Which two routing protocols converge most quickly? (Choose two.)

- A. RIPv1
- B. RIPv2
- C. BGP
- D. OSPF
- E. EIGRP

**Correct Answer:** DE



**Section: (none)**  
**Explanation**

**Explanation/Reference:**  
Explanation:

## Exam D

### QUESTION 1

Which two devices would you place in your DMZ to ensure enterprise edge security? (Choose two.)

- A. IPS
- B. NAC
- C. ASA
- D. ACS
- E. WCS

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

### QUESTION 2

Which three are security services offered through Cisco Router Security? (Choose three.)

- A. Trust and Identity
- B. Integrated Threat Control
- C. Unified Wireless Network Security Solution
- D. Secure Connectivity
- E. Voice-Messaging Security
- F. Endpoint Security
- G. Virtual Security Gateway

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation: Threat Defense

Enabling integrated security in routers, switches, and appliances: Security techniques enabled throughout the network, not just in point products or locations

Secure Connectivity

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

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

Simplifies hub-and-spoke VPNs; need to reduce VPN management Cisco Easy VPN Trust

Trust is the relationship between two or more network entities that are permitted to communicate.

Security policy decisions are largely based on this premise of trust. If you are trusted, you are allowed to communicate as needed. However, sometimes security controls need to apply restraint to trust relationships by limiting or preventing access to the designated privilege level. Trust relationships can be explicit or implied by the organization. Some trust relationships can be inherited or passed down from one system to another.

However, keep in mind that these trust relationships can also be abused.

#### Identity

Identity is the "who" of a trust relationship. These can be users, devices, organizations, or all of the above.

Network entities are validated by credentials. Authentication of the identity is based on the following attributes:

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 50

Cisco 640-864 Exam

Something the subject knows: Knowledge of a secret, password, PIN, or private key  
Something the subject has: Possession of an item such as a token card, smartcard, or hardware key

Something the subject is: Human characteristics, such as a fingerprint, retina scan, or voice recognition

Generally, identity credentials are checked and authorized by requiring passwords, pins, tokens, or certificates.

#### QUESTION 3

Which protocol is used to reserve bandwidth for the transport of a particular application data flow across the network?

- A. cRTP
- B. IEEE 802.1P
- C. RSVP
- D. LFI
- E. Auto QOS

**Correct Answer: C**

**Section: (none)**

**Explanation**

#### Explanation/Reference:

Explanation:

RSVP Signaling protocol that enables end stations or applications to obtain guaranteed bandwidth and low delays for their data flows.

#### QUESTION 4

Which voice codec should you use in order to provide toll quality calls?

- A. G.711
- B. G.718
- C. G.722
- D. G.729

**Correct Answer: A**

**Section: (none)**

**Explanation**

#### Explanation/Reference:

Explanation:

#### QUESTION 5

Which two features are supported by single wireless controller deployments? (Choose two.)

- A. automatic detection and configuration of LWAPPs
- B. LWAPP support across multiple floors and buildings
- C. automatic detection and configuration of RF parameters
- D. Layer 2 and Layer 3 roaming

- E. controller redundancy
- F. mobility groups

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 6**

Which three are features of LWAPP? (Choose three.)

- A. firmware synchronization
- B. local management of APs
- C. configuration changes manually synced
- D. encryption of control channel
- E. configuration data only on the WLC
- F. wireless control free operation
- G. replaces 802.1x for authentication in wireless connections

**Correct Answer:** ADE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Cisco Unified Wireless Network Split-MAC Architecture With the Cisco UWN split-M AC 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.

#### **QUESTION 7**

Which four services does the architecture for Media Services contain? (Choose four.)

- A. access services
- B. transport services
- C. storage services
- D. forwarding services
- E. session control services
- F. security services
- G. filtering services
- H. remote access services

**Correct Answer:** ABCE

**Section:** (none)

**Explanation**

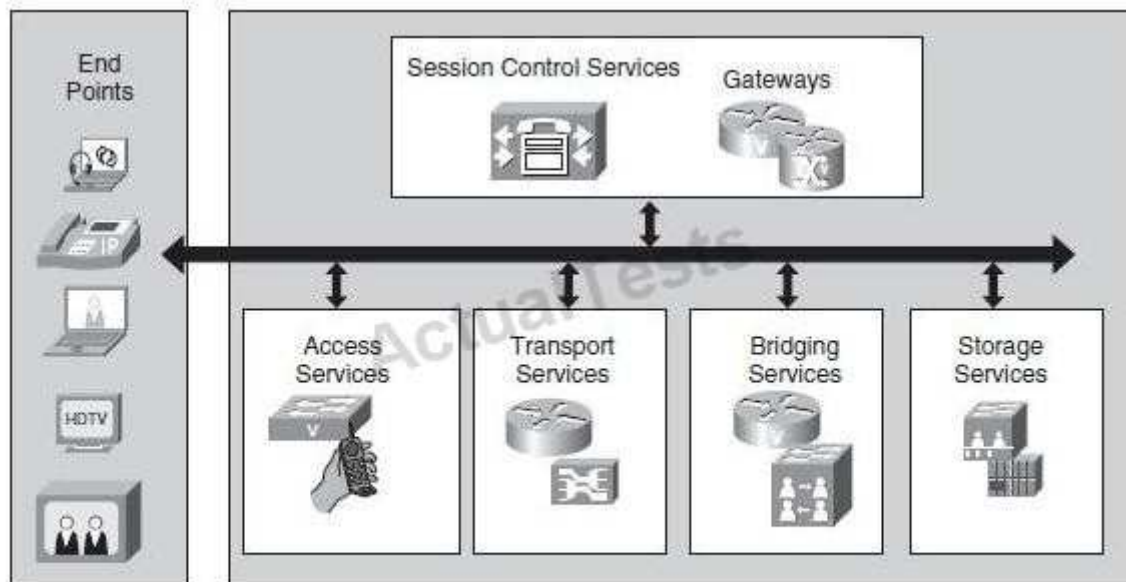
**Explanation/Reference:**

Explanation:

An architecture framework for media services supports different models of video models. As shown in Figure 14-13, the network provides service to video media in the Media Services Framework. Those services are access services, transport services, bridging services, storage servers, and session control services, which are provided to endpoints.

Access services provide identity of end devices, mobility, and location services. Transport services provide QoS for reliable packet delivery. Bridging services provide transcoding, conferencing, and recording services of media streams. Storage services provide capture and storage of media streams and content management and distribution.

Session control services provide session signaling and control and gateway services.



**Figure 14-13** *Media Services Architectural Framework*

#### QUESTION 8

Which Cisco device has the sole function at looking at threat detection and mitigation at the Enterprise edge?

- A. Cisco IOS router
- B. Cisco ASA
- C. Cisco Catalyst FWSM
- D. Cisco IPS

**Correct Answer:** D

**Section:** (none)

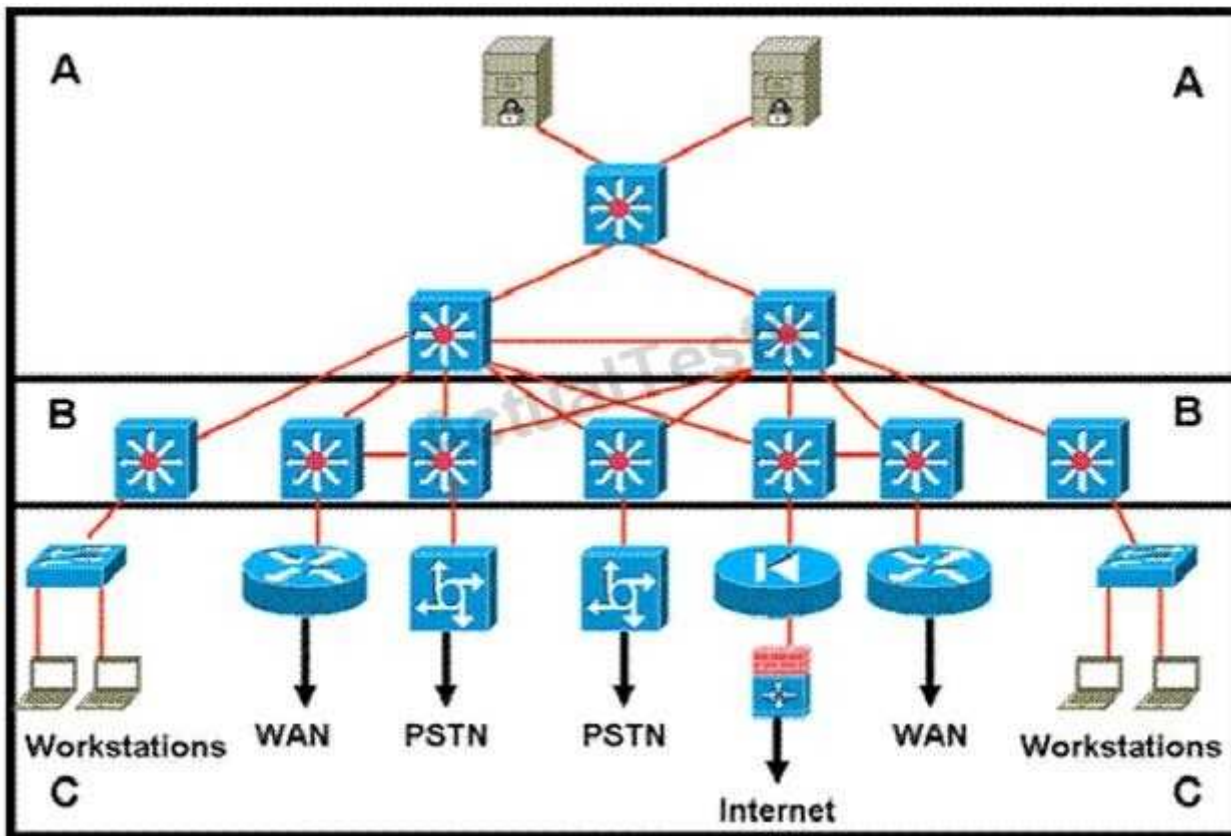
**Explanation**

**Explanation/Reference:**

Explanation:

#### QUESTION 9

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 10

You have a campus network that consists of only Cisco devices. You have been tasked to discover the device platforms, the IOS versions, and an IP address of each device to map the network. Which proprietary protocol will assist you with this task?

- A. SNMP
- B. TCP
- C. CDP



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

- D. ICMP
- E. LLDP

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**  
Explanation:

**QUESTION 11**

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 12**

Which three technologies are recommended to be used for WAN connectivity in today's Enterprise Edge designs? (Choose three.)

- A. DWDM
- B. Metro Ethernet
- C. Frame Relay
- D. MPLS VPN
- E. ISDN
- F. DSL
- G. Wireless

**Correct Answer:** ABD  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**  
Explanation:

There is some discussion about whether ISDN not DWDM should be the answer but it does say TODAY'S network

**QUESTION 13**

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. MISTP
- E. Rapid PVST +

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 14**

Which WAN technology is a cost-effective method to deliver 100Mb of bandwidth to multiple branch offices?

- A. DSL
- B. DWDM
- C. ISDN
- D. Metro Ethernet

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

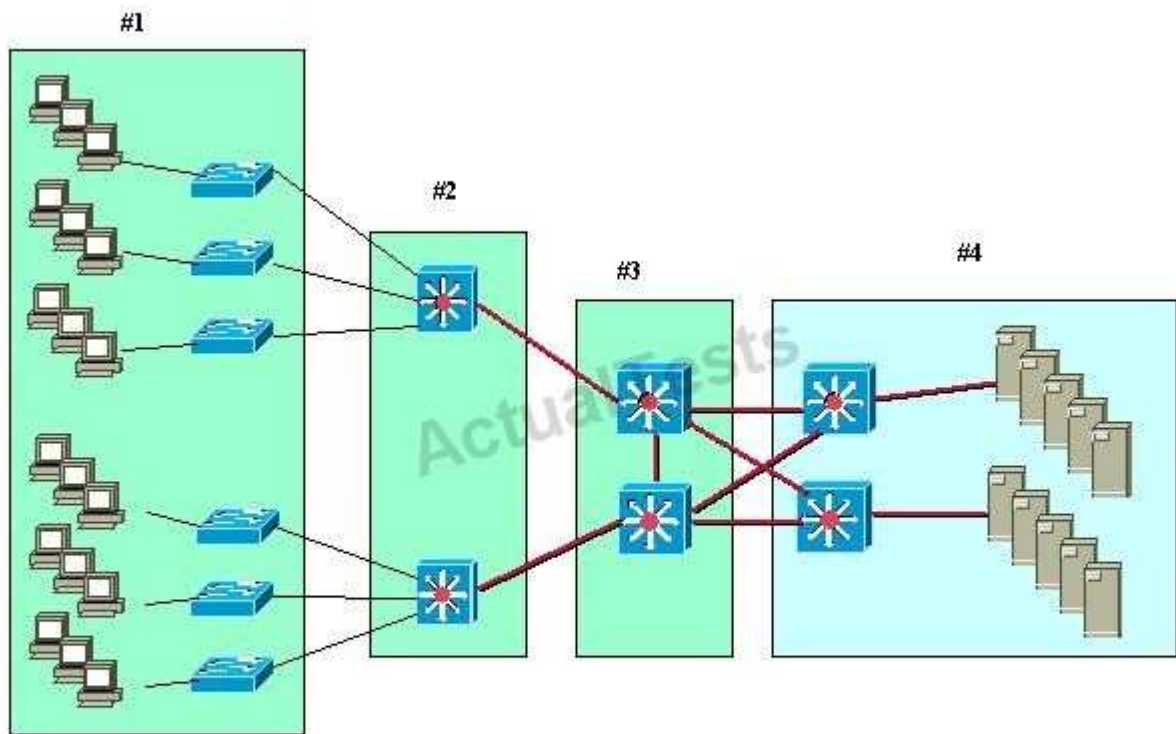
Metro Ethernet

Metro Ethernet uses well-known "Ethernet" to deliver low-cost and high-speed MAN/WAN connectivity for organizations. Many service providers now offer Metro Ethernet solutions to deliver a wide range of converged network services such as data, voice, and video on the same wire. Metro Ethernet provides enterprise LAN type functionality out in the MAN and WAN, increasing the throughput available for applications. Metro Ethernet bandwidths can range from 10Mbps to 1 Gbps, and even higher in some cases, allowing for support for higher performance and increased QoS requirements. In contrast to the rigid nature of traditional TDM provisioning, Metro Ethernet services are much easier to deploy and scale due to the flexible bandwidth increments. Metro Ethernet technology is appealing to many customers because they are already comfortable using Ethernet throughout their LAN environments.

**QUESTION 15**

Refer to the exhibit.





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

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

**Correct Answer:** B

**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 16**

WAN backup over the Internet is often used to provide primary connection redundancy. Which is the most important consideration when passing corporate traffic over the public Internet?

- A. security
- B. static versus dynamic routing
- C. bandwidth
- D. QoS
- E. latency

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

WAN Backup over the Internet

Another alternative for WAN backup is to use the Internet as the connectivity transport between sites. However, keep in mind that this type of connection does not support bandwidth guarantees. The enterprise also needs to work closely with the ISP to set up the tunnels and advertise the company's networks internally so that remote offices have reachable IP destinations. Security is of great importance when you rely on the Internet for network connectivity, so a secure tunnel using IPsec needs to be deployed to protect the data during transport.

**QUESTION 17**

Which two are types of network virtualization? (Choose two.)

- A. VSS: Virtual Switching System
- B. VRF: virtual routing and forwarding
- C. VCI: virtual channel identifier
- D. VLSM: variable length subnet masking
- E. VM: virtual machine
- F. VMP: Virtual Memory Pool

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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:

VLAN: Virtual local-area network  
VSAN: Virtual storage-area network  
VRF: Virtual routing and forwarding  
VPN: Virtual private network  
vPC: Virtual Port Channel

**QUESTION 18**

To provide Layer 2 connectivity between the primary and remote data centers, given that the two data centers are using Layer 3 routed DCIs, which NX-OS technology can be used to facilitate this requirement?

- A. VRF
- B. OTV
- C. MPLS
- D. SPT
- E. vPC

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

#### **QUESTION 19**

You are tasked with designing a new branch office that will support 75 users with possible expansion in the future and will need a highly available network. Which of the branch design profiles should be implemented?

- A. large branch design
- B. medium branch design
- C. teleworker design
- D. small branch design

**Correct Answer:** B

**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.

#### **QUESTION 20**

Which WLC interface is dedicated for WLAN client data?

- A. virtual interface
- B. dynamic interface
- C. management interface
- D. AP manager interface
- E. service port interface

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

WLC Interface Types

A WLC has five interface types:

Management interface (static, configured at setup, mandatory) is used for in-band management, connectivity to AAA, and Layer 2 discovery and association. Service-port interface (static, configured at setup, optional) is used for out-of-band management. It is an optional interface that is statically configured. AP manager interface

(static, configured at setup, mandatory except for 5508 WLC) is used for Layer 3 discovery and association. It has the source IP address of the AP that is statically configured.

Dynamic interface (dynamic) is analogous to VLANs and is designated for WLAN client data. Virtual interface (static, configured at setup, mandatory) is used for layer 3 security authentication, DHCP relay support, and mobility management.

#### **QUESTION 21**

Which two can be used as a branch office WAN solution? (Choose two.)

- A. frame relay
- B. MPLS
- C. Metro Ethernet
- D. GPRS
- E. dial-up modem
- F. 3G USB modems

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation: Explanation

Frame relay is old 'shared' technology today's sites use some flavor of Metro E or MPLS/VPN

#### **QUESTION 22**

When designing for a remote worker, which two are typical requirements? (Choose two.)

- A. best-effort interactive and low-volume traffic patterns
- B. connections to the enterprise edge using Layer 2 WAN technologies
- C. always-on connection with SLA from ISP
- D. voice and IPsec VPN support
- E. high-end security devices with stateful firewall filtering
- F. dual or multihoming to ISPs

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Teleworker: The teleworker module allows enterprises to securely deliver voice and data services to a remote small office/home office (SOHO) over a standard broadband access service, providing a business-resiliency solution for the enterprise and a flexible work environment for employees. Centralized management minimizes the IT support costs, and robust integrated security mitigates the unique security challenges of this environment. Integrated security- and identity-based networking services enable the enterprise to help extend campus security policies to the teleworker.

Staff can securely log in to the network over an "always-on" VPN and gain access to authorized applications and services from a single cost-effective platform. The productivity can be further enhanced by adding a Cisco IP phone, providing cost-effective access to a centralized IP communications system with voice and unified messaging services.

#### **QUESTION 23**

You are asked to design a new branch office that will need to support 25 users. These users will be using an ISP connection and will need to connect to the main office for network services.

Which two Cisco devices are the most appropriate to fulfill all of these requirements? (Choose two.)

- A. Cisco IPS
- B. Cisco ISR G2
- C. Cisco ASA
- D. Cisco 2960
- E. Cisco CRS-1
- F. Cisco ACS

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

## 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 access router can connect the Layer 2 switch ports in one of three ways:

- Integrated Layer 2 switching using an optional EtherSwitch module that provides 16 to 48 Ethernet ports for client connections. Some modules support PoE.
- External Layer 2 switching using a trunk connection to an access switch that aggregates the Ethernet connections. The access switch can also include PoE to support IP phones and wireless APs.
- Logical EtherChannel interface between the ISR and the access switches using the EtherSwitch module. The access switches can also provide PoE as needed.

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.

The ISR can support the default gateway function and other Layer 3 services such as DHCP, NAT, IPsec VPN, and IOS Firewall.

Layer 2 services can be provided by the Cisco ISR using switch modules or the Cisco Catalyst 2960, 3560 or 3750 series-based access switches. It is recommended that you use Rapid Per VLAN Spanning Tree Plus (PVST+) for all Layer 2 branch offices where loops are present. Rapid PVST+ ensures a loop-free topology when multiple Layer 2 connections are used for redundancy purposes.

Both the Cisco 2921 and the 2951 ISRs support three integrated 10/100/1000 Ethernet interfaces, which support Layer 3 routing, and one slot for a network module. There are 16, 24, and 48 port Cisco EtherSwitch network modules available.

Figure 7-8 illustrates the small branch design connecting back to the corporate office where the corporate resources are located.

### QUESTION 24

What is the acceptable amount of one-way network delay for voice and video applications?

- A. 300 bytes
- B. 1 sec
- C. 150 ms
- D. 500 ms

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Delay Components in VoIP Networks

The ITU's G.114 recommendation specifies that the one-way delay between endpoints should not exceed 150 ms to be acceptable, commercial voice quality. In private networks, somewhat longer delays might be acceptable for economic reasons. The ITU G.114 recommendation specifies that 151-ms to 400-ms one-way delay might be acceptable provided that organizations are aware that the transmission time will affect the quality of user applications. One-way delays of above 400 ms are unacceptable for general network planning purposes.

#### QUESTION 25

Which mode is used to exclusively look for unauthorized access points?

- A. monitor mode
- B. sniffer mode
- C. rogue detector mode
- D. local mode

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

AP Mode	Description
Monitor mode	
Rogue Detector mode	
Sniffer mode	
Bridge mode	

Interference detection and avoidance: As Cisco LWAPs monitor all channels, interference is detected by a predefined threshold (10 percent by default). Interference can be generated by rogue APs, microwaves, cordless telephones, Bluetooth devices, neighboring WLANs, or other electronic devices.

#### QUESTION 26

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 27

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



Exam E

QUESTION 1

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

High Level of Availability, scalability, and fast convergence

Enforces Policy within the network

Routing boundary (Dynamic, summarization, static)

Provides security, QoS, and IP Multicast to the network

Provides a limited set of services

The most feature-rich part of the campus network

Access

Distribution

Core

Select and Place:

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

High Level of Availability, scalability, and fast convergence

Enforces Policy within the network

Routing boundary (Dynamic, summarization, static)

Provides security, QoS, and IP Multicast to the network

Provides a limited set of services

The most feature-rich part of the campus network

**Access**

**Distribution**

**Core**

Correct Answer:

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

**Access**

Provides security, QoS, and IP Multicast to the network

The most feature-rich part of the campus network

**Distribution**

Enforces Policy within the network

Routing boundary (Dynamic, summarization, static)

**Core**

High Level of Availability, scalability, and fast convergence

Provides a limited set of services

**Section:**  
**Explanation**

**Explanation/Reference:**  
**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 2**

Drag the WAN technology on the left to the most appropriate category on the right.

	Leased
Frame-Relay	
TDM	
SONET	
MPLS	

Shared

Select and Place:

Drag the WAN technology on the left to the most appropriate category on the right.

	Leased
Frame-Relay	
TDM	
SONET	
MPLS	

Shared

Correct Answer:

Drag the WAN technology on the left to the most appropriate category on the right.

**Leased**

TDM

SONET

**Shared**

Frame-Relay

MPLS

**Section:**  
**Explanation**

**Explanation/Reference:**

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

**CCDA 640-864 Official Cert Guide Chapter 6**

**QUESTION 3**



Drag the data center properly on the left to the design aspect on the right it is most apt to affect.

variability of computing load, computing power and memory requirements

Space

disasters, fire suppression and alarm system

Weight Load

abundant, variable, well organized and easy to maintain

Power

amount of racks, equipment, cabling, people

Cooling

arranging equipment racks face-to-face or back-to-back

Cabling

rack servers vs blade servers

Security

Select and Place:

Drag the data center properly on the left to the design aspect on the right it is most apt to affect.

variability of computing load, computing power and memory requirements

Space

disasters, fire suppression and alarm system

Weight Load

abundant, variable, well organized and easy to maintain

Power

amount of racks, equipment, cabling, people

Cooling

arranging equipment racks face-to-face or back-to-back

Cabling

rack servers vs blade servers

Security

Correct Answer:

Drag the data center properly on the left to the design aspect on the right it is most apt to affect.

amount of racks, equipment, cabling, people

rack servers vs blade servers

variability of computing load, computing power and memory requirements

arranging equipment racks face-to-face or back-to-back

abundant, variable, well organized and easy to maintain

disasters, fire suppression and alarm system

**Section:**

**Explanation**

**Explanation/Reference:**

**Space:** amount of racks, equipment, cabling, people

**Weight load:** rack servers vs blade servers

**Power:** variability of computing load, computing power and memory requirements

**Cooling:** arranging equipment racks face-to-face or back-to-back

**Cabling:** abundant, variable, well organized and easy to maintain

**Security:** disasters, fire suppression and alarm systems

please refer to the link below.

**Link:**

[http://www.cisco.com/application/pdf/en/us/guest/netsol/ns107/c649/ccmigration\\_09186a008073377d.pdf](http://www.cisco.com/application/pdf/en/us/guest/netsol/ns107/c649/ccmigration_09186a008073377d.pdf)

**QUESTION 4**

Drag the WAN characteristics on the left to the branch office model where it would most likely be used on the right.

Redundant Devices

MPLS Deployment Model

Redundant Links

Redundant Links and Devices

Private WAN Deployment

Internet Deployment Model

**Small Office**

**Medium Office**

**Large Office**

**Select and Place:**

Drag the WAN characteristics on the left to the branch office model where it would most likely be used on the right.

Redundant Devices

MPLS Deployment Model

Redundant Links

Redundant Links and Devices

Private WAN Deployment

Internet Deployment Model

**Small Office**

**Medium Office**

**Large Office**

**Correct Answer:**



Drag the WAN characteristics on the left to the branch office model where it would most likely be used on the right.

**Small Office**

Redundant Links

Internet Deployment Model

**Medium Office**

Redundant Devices

Private WAN Deployment

**Large Office**

MPLS Deployment Model

Redundant Links and Devices

**Section:**

**Explanation**

**Explanation/Reference:**

**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.

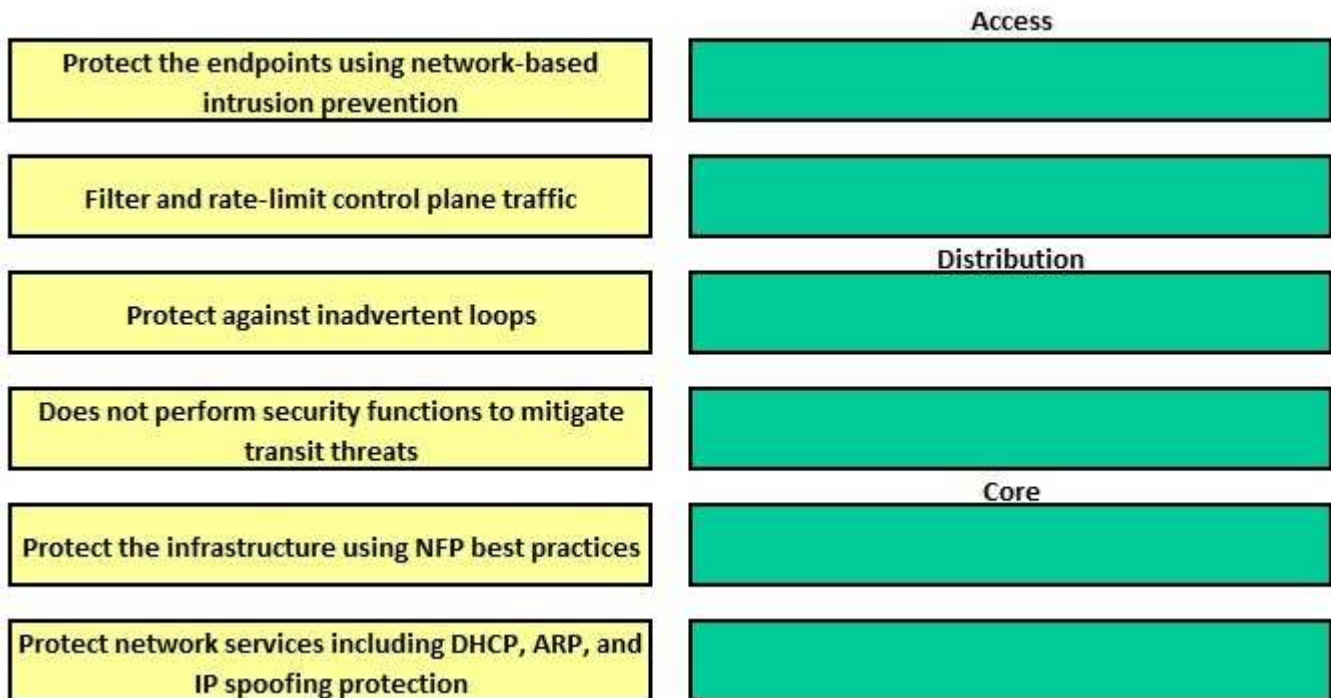
Cisco Press CCDA 640-864 Official Certification Guide Fourth Edition, Chapter 7

#### QUESTION 5

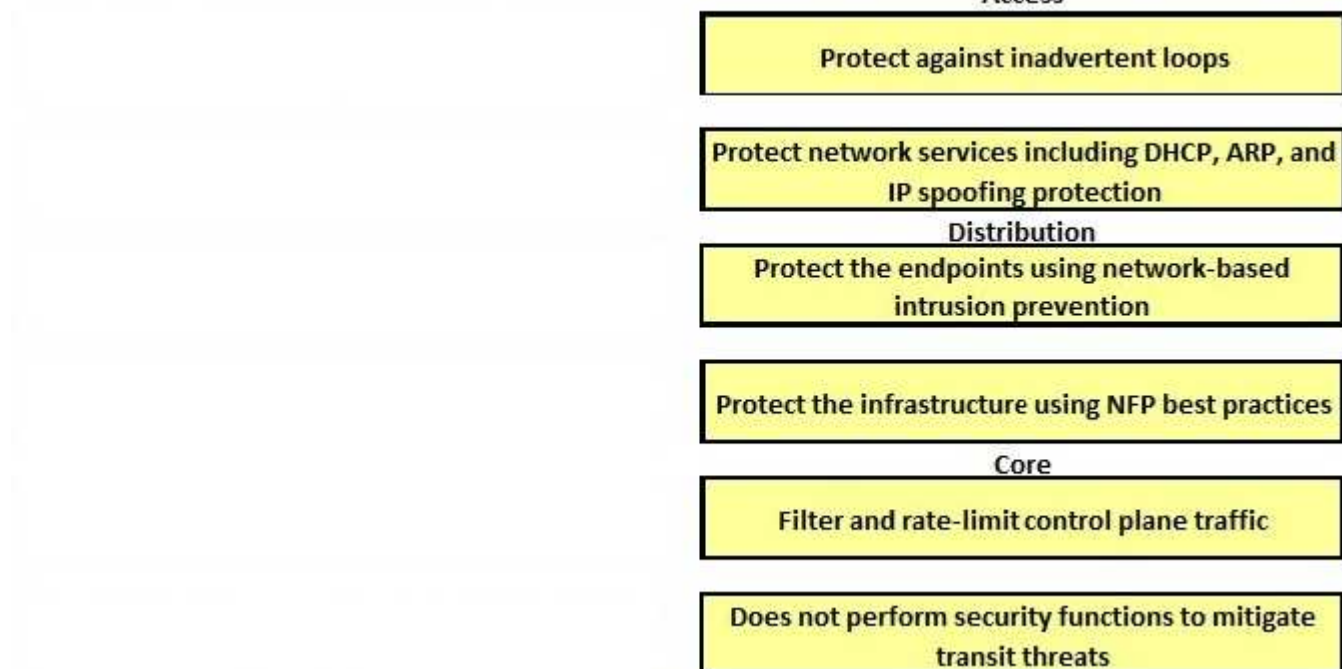
Drag the security provision on the left to the appropriate Network module on the right.

	Access
Protect the endpoints using network-based intrusion prevention	
Filter and rate-limit control plane traffic	
	Distribution
Protect against inadvertent loops	
Does not perform security functions to mitigate transit threats	
	Core
Protect the infrastructure using NFP best practices	
Protect network services including DHCP, ARP, and IP spoofing protection	

Select and Place:



Correct Answer:



Section:  
Explanation

Explanation/Reference:  
Changed this one to Jolly Frogs suggestion from Actual Tests:

Access:

Protect against inadvertent loops  
Protect network services including DHCP, ARP, and IP spoofing protection

**Distribution:**

Protect the endpoints using network-based intrusion prevention  
Protect the infrastructure using NFP best practices

**Core:**

Filter and rate-limit control plane traffic  
Does not perform security functions to mitigate transit threats

Explanation:

[http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE\\_RG/chap5.html#wp1090913](http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap5.html#wp1090913)

[http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE\\_RG/chap3.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap3.html)

**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 6**

Drag the technology on the left to the type of enterprise virtualization where it is most likely to be found on the right.

ASA firewall context
IPS
vPC
VLAN
VDC
VRF

Network Virtualization
Device Virtualization

**Select and Place:**

Drag the technology on the left to the type of enterprise virtualization where it is most likely to be found on the right.

ASA firewall context
IPS
vPC
VLAN
VDC
VRF

**Network Virtualization**


**Device Virtualization**


Correct Answer:

Drag the technology on the left to the type of enterprise virtualization where it is most likely to be found on the right.


**Network Virtualization**

vPC
VLAN
VRF

**Device Virtualization**

ASA firewall context
IPS
VDC

Section:

## **Explanation**

### **Explanation/Reference:**

Network Virtualization

- \* VPC
- \* VLAN
- \* VRF

Device Virtualization

- \*ASA firewall context
- \*IPS
- \*VDC

**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.

**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.

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

## **QUESTION 7**

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

provides internal users with external HTTP, FTP, SMTP, and DNS connectivity

enables service-oriented architectures, virtualization, and secure computing with load balancing, redundancy

enables intelligent route and switch, high availability resilient multilayer design and integrated security

supports application traffic through the internet, initiated outside the enterprise network

terminates traffic that is forwarded by the internet connectivity module

Enterprise Campus

Enterprise Edge

E-Commerce

Internet Connectivity

Remote Access and VPN

Data Center

Select and Place:



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

provides internal users with external HTTP, FTP, SMTP, and DNS connectivity

enables service-oriented architectures, virtualization, and secure computing with load balancing, redundancy

enables intelligent route and switch, high availability resilient multilayer design and integrated security

supports application traffic through the internet, initiated outside the enterprise network

terminates traffic that is forwarded by the internet connectivity module

Enterprise Campus

Enterprise Edge

E-Commerce

Internet Connectivity

Remote Access and VPN

Data Center

Correct Answer:



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

enables intelligent route and switch, high availability resilient multilayer design and integrated security

aggregates connectivity to voice, video, and data outside the enterprise with QoS and security

supports application traffic through the internet, initiated outside the enterprise network

provides internal users with external HTTP, FTP, SMTP, and DNS connectivity

terminates traffic that is forwarded by the internet connectivity module

enables service-oriented architectures, virtualization, and secure computing with load balancing, redundancy

Section:  
Explanation

Explanation/Reference:

- 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 8**

Drag the network characteristics on the left to the design method on the right which will best ensure redundancy at the building distribution layer.

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

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

Convergence (FHRP) is not an issue

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

Select and Place:

Drag the network characteristics on the left to the design method on the right which will best ensure redundancy at the building distribution layer.

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

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

Convergence (FHRP) is not an issue

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

Correct Answer:

Drag the network characteristics on the left to the design method on the right which will best ensure redundancy at the building distribution layer.

FHRP for convergence. No VLANs span between access layer switches across the distribution switches

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

Convergence (FHRP) is not an issue

**Section:**  
**Explanation**

**Explanation/Reference:**  
**I changed the answer on this to:**

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

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

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

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

VSS -> Convergence (FHRP) is not an issue

**Original Answer was**

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 9**

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

WRED

classification and marking

CAR

congestion avoidance

ACLs

traffic conditioners

LFI

congestion management

LLQ

link efficiency

Select and Place:

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

WRED

classification and marking

CAR

congestion avoidance

ACLs

traffic conditioners

LFI

congestion management

LLQ

link efficiency

Correct Answer:

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

ACLs

WRED

CAR

LLQ

LFI

#### Section:

#### Explanation

##### Explanation/Reference:

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

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 bandwidth. 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 10

Click and drag the Cisco Self-Defending Network term on the left to the SDN description on the right. Not all terms will be used.

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

Select and Place:

Click and drag the Cisco Self-Defending Network term on the left to the SDN description on the right.  
Not all terms will be used.

Threat Defense

provides secure network access, isolates and controls infected devices attempting access

Secure Remote Access

uses encryption and authentication to provide secure transport across untrusted networks

Cisco Self-Defending Network

uses security integrated into routers, switches, and appliances to defend against attacks

Secure Connectivity

integrates security into the network to identify, prevent and adapt to threats

Trust and Identity Management

**Correct Answer:**

Click and drag the Cisco Self-Defending Network term on the left to the SDN description on the right.  
Not all terms will be used.

Secure Remote Access

Trust and Identity Management

Secure Connectivity

Threat Defense

Cisco Self-Defending Network

**Section:**  
**Explanation**

**Explanation/Reference:**

- + 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

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 11

Match the Cisco security solution on the left to its function on the right	
Anomaly Guard and Detector	protects the endpoints (desktop, laptops and servers)
Cisco Security Agent	provides multiple functions as a high performance security appliance
IPS Appliance	prevents DDoS attacks
ASA	provides Web-Based VPN services
SSL Service Module	prevents attacks inline

Select and Place:



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

Anomaly Guard and Detector

protects the endpoints (desktop, laptops and servers)

Cisco Security Agent

provides multiple functions as a high performance security appliance

IPS Appliance

prevents DDoS attacks

ASA

provides Web-Based VPN services

SSL Service Module

prevents attacks inline

**Correct Answer:**

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

Cisco Security Agent

ASA

Anomaly Guard and Detector

SSL Service Module

IPS Appliance

**Section:**  
**Explanation**

**Explanation/Reference:**

+ 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

#### QUESTION 12

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

queuing	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
traffic policing	allows network administrator to manage the varying demands generated by applications
data compression	discards packets or modifies some aspect of them (such as IP precedence)

Select and Place:

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

queuing	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
traffic policing	allows network administrator to manage the varying demands generated by applications
data compression	discards packets or modifies some aspect of them (such as IP precedence)

Correct Answer:

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

window size

data compression

queuing

traffic policing

Section:  
Explanation

**Explanation/Reference:**

- + 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 IPprecedence): traffic policing

**QUESTION 13**

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

Select and Place:

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

**Correct Answer:**

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

**Section:**

**Explanation**

**Explanation/Reference:**

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.

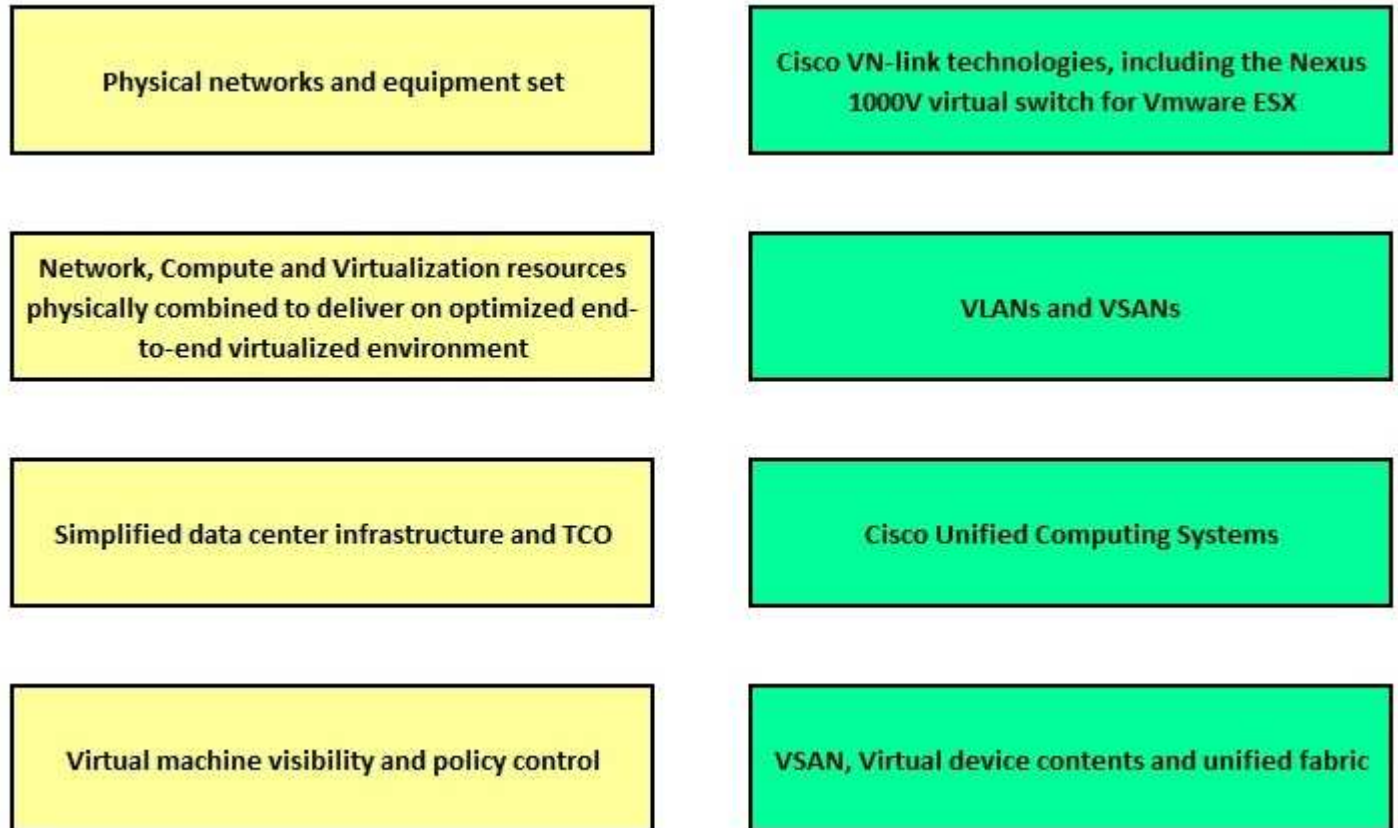
b. SNMP ( Simple Network Management Protocol)

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 14

Data Center Design 3.0

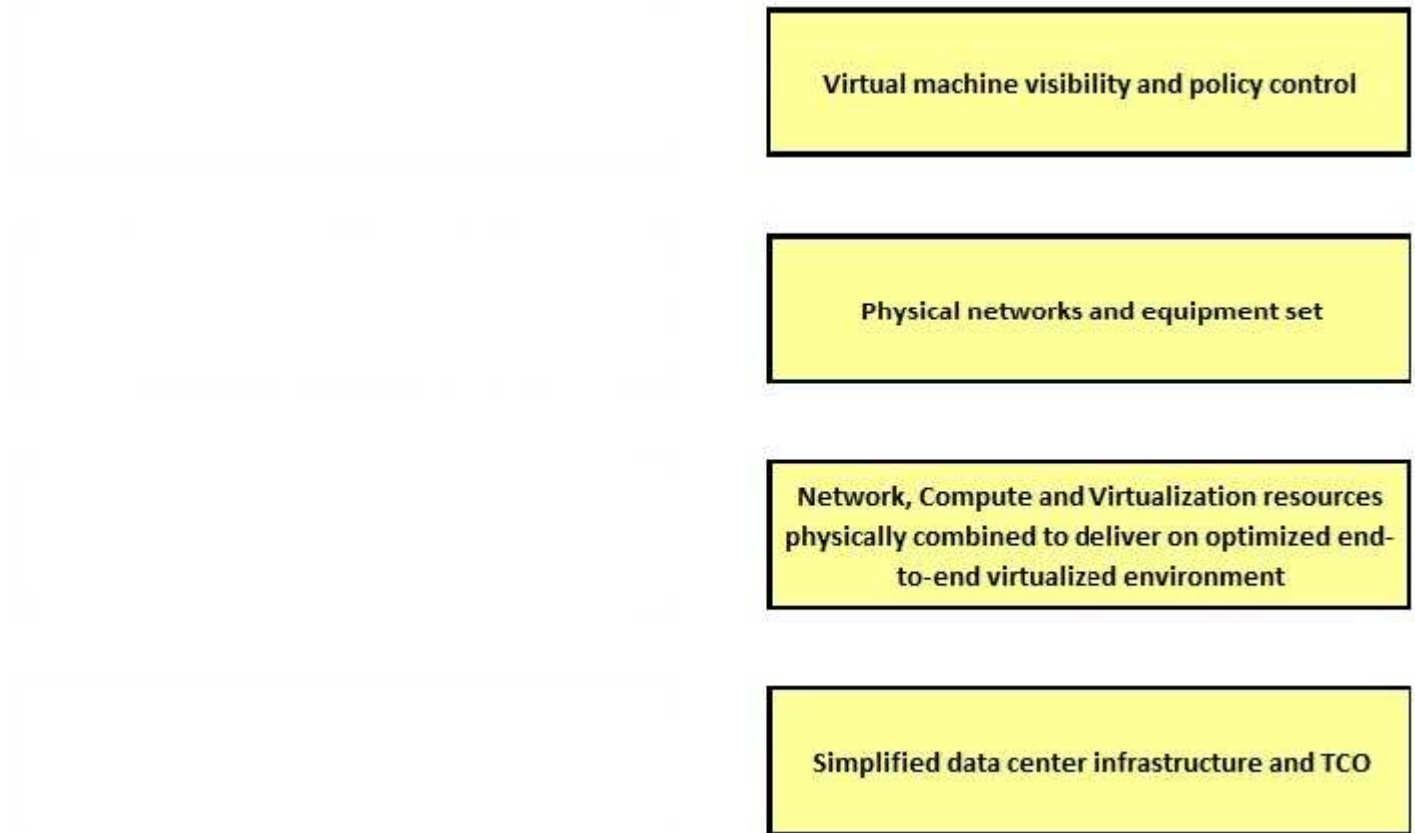


Select and Place:



Physical networks and equipment set	Cisco VN-link technologies, including the Nexus 1000V virtual switch for Vmware ESX
Network, Compute and Virtualization resources physically combined to deliver an optimized end-to-end virtualized environment	VLANs and VSANs
Simplified data center infrastructure and TCO	Cisco Unified Computing Systems
Virtual machine visibility and policy control	VSAN, Virtual device contents and unified fabric

Correct Answer:

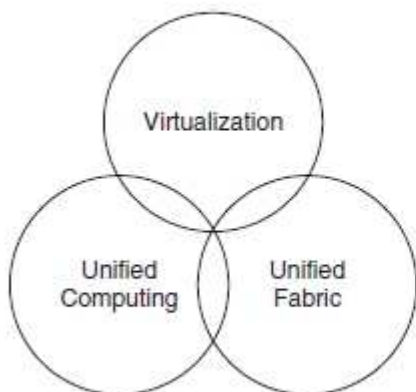


Section:  
Explanation

Explanation/Reference:

### Data Center 3.0 Components

Figure 4-2 highlights the Cisco Data Center 3.0 components.



**Figure 4-2** *Cisco Data Center 3.0 Architecture Framework*

- **Unified computing**
- Cisco Unified Computing System (UCS) is an innovative next-generation data center platform that converges

computing, network, storage, and virtualization together into one system.

- Integrates lossless 10GE unified network fabric with x86 architecture-based servers.
- Allows for Cisco Virtual Interface Card to virtualize your network interfaces on your server.
- Offers Cisco VN-Link virtualization.
- Supports Extended Memory Technology patented by Cisco.
- Increases productivity with just-in-time provisioning using service profiles.

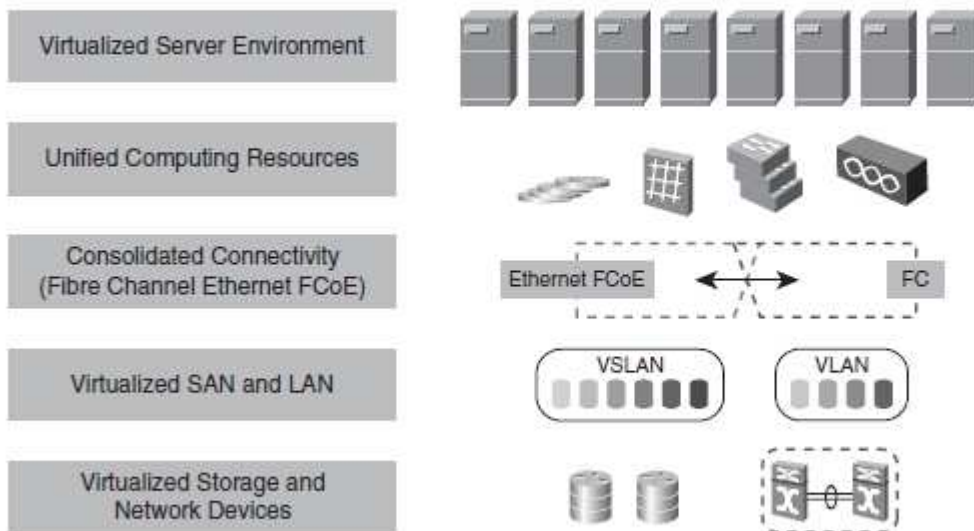
In addition, the newer Data Center 3.0 architecture increases the overall return on investment (ROI) and lowers the total cost of ownership (TCO).

#### ■ Virtualization

- Virtual local-area network (VLAN), virtual storage-area network (VSAN), and virtual device contexts (VDC) help to segment the LAN, SAN, and network devices instances.
- Cisco Nexus 1000V virtual switch for VMware ESX and ESXi help to deliver **visibility and policy control** for virtual machines (VM).
- Flexible networking options with support for all server form factors and vendors, including support for blade servers from Cisco, Dell, IBM, and HP with integrated Ethernet and Fibre Channel switches.

### Data Center 3.0 Topology Components

Figure 4-3 shows the Cisco Data Center 3.0 topology.



**Figure 4-3** Cisco Data Center 3.0 Topology

Virtualization technologies such as **VLANS and VSANs** provide for virtualized LAN and SAN connectivity by **logically segmenting multiple LANs and SANs on the same physical equipment**. Each VLAN and VSAN operates independently from one another.



Exam F

QUESTION 1

Drag the function on the left with the option most closely paired on the right	
NetFlow	Complete Monitor of all OSI Layers
RMON	Communication between devices and monitoring
CDP	Data Link, Multicast
SNMP	Process ACLs, packet analysis for security

Select and Place:

Drag the function on the left with the option most closely paired on the right	
NetFlow	Complete Monitor of all OSI Layers
RMON	Communication between devices and monitoring
CDP	Data Link, Multicast
SNMP	Process ACLs, packet analysis for security

Correct Answer:

Drag the function on the left with the option most closely paired on the right

RMON

SNMP

CDP

NetFlow

**Section:**

**Explanation**

**Explanation/Reference:**

RMON -> complete monitor of all OSI layers

SNMP -> communication between devices and monitoring

CDP -> data link, multicast

NetFlow -> processes ACLs, packet analysis for security

## QUESTION 2

Drag the function on the left with the option most closely paired on the right

VSAN / VLAN

Cisco Nexus 1000 and enforcing VM Security

Cisco Unified Communication System

Network and Server Virtualization

Data Center Virtualization

Unified Application for IPT

**Select and Place:**

Drag the function on the left with the option most closely paired on the right

VSAN / VLAN	Cisco Nexus 1000 and enforcing VM Security
Cisco Unified Communication System	Network and Server Virtualization
Data Center Virtualization	Unified Application for IPT

Correct Answer:

Drag the function on the left with the option most closely paired on the right

	Data Center Virtualization
	VSAN / VLAN
	Cisco Unified Communication System

Section:  
Explanation

Explanation/Reference:

Added a different D & D based on Secur Tut CCDA V2.1 Experience **SO IGNORE THIS ONE EXAM F Q14**

Cisco Unified Communication System
VSAN/VLAN
Data Center Virtualization

Original answer was:

Cisco Unified Communication System -> Cisco Nexus1000 and Enforcing vm Security  
VSAN/VLAN -> Network and Server Virtualization  
Data Center Virtualization -> Pending

ARCH guide shows for 1000V:

**Virtualization:** The Cisco VN-Link technology provides virtual machine-aware network services. This technology is used in the Cisco Nexus 1000V Distributed Virtual Switch, which integrates into the VMware vSphere virtualization platform.

Other virtualization technologies that are supported in the Cisco Nexus family of switches are virtual port channels (vPC) and virtual device contexts (VDC).

### QUESTION 3

Drag the function on the left with the option most closely paired on the right

Http / Email	Application
Budget	Network Services
IP Phone / Voice	Business Constraints
Security	Technical Goals

Select and Place:

Drag the function on the left with the option most closely paired on the right

Http / Email	Application
Budget	Network Services
IP Phone / Voice	Business Constraints
Security	Technical Goals

Correct Answer:

Drag the function on the left with the option most closely paired on the right

Http / Email

IP Phone / Voice

Budget

Security

Section:  
Explanation

Explanation/Reference:

#### QUESTION 4

Match each infrastructure service with its description

Identity

Access from a remote location

Mobility

Improved computational resources

Storage

Unified messaging

Compute

AAA, NAC

Security

Storage of critical data

Voice / Collaboration

Secure communications

Select and Place:

Match each infrastructure service with its description	
Identity	Access from a remote location
Mobility	Improved computational resources
Storage	Unified messaging
Compute	AAA, NAC
Security	Storage of critical data
Voice / Collaboration	Secure communications

Correct Answer:

Match each infrastructure service with its description	
	Mobility
	Compute
	Voice / Collaboration
	Identity
	Storage
	Security

Section:  
Explanation

Explanation/Reference:



### QUESTION 5

Match each access point mode with its description.

Local	For location-based services
REAP	Captures packets
Monitor	For point-to-point connections
Rogue detector	Default mode
Sniffer	Management across the WAN
Bridge	Monitors rogue Aps

Select and Place:

Match each access point mode with its description.

Local	For location-based services
REAP	Captures packets
Monitor	For point-to-point connections
Rogue detector	Default mode
Sniffer	Management across the WAN
Bridge	Monitors rogue Aps

Correct Answer:

Match each access point mode with its description.

Monitor

Sniffer

Bridge

Local

REAP

Rogue detector

Section:  
Explanation

Explanation/Reference:

#### QUESTION 6

Match each protocol, mechanism, or feature with its security grouping.

CSM

Identity and access control

IGP / EGP MD5

Threat detection and mitigation

NetFlow

Infrastructure protection

NAC

Security management

Select and Place:



Match each protocol, mechanism, or feature with its security grouping.

CSM

Identity and access control

IGP / EGP MD5

Threat detection and mitigation

NetFlow

Infrastructure protection

NAC

Security management

**Correct Answer:**

Match each protocol, mechanism, or feature with its security grouping.

NAC

NetFlow

IGP / EGP MD5

CSM

**Section:**

**Explanation**

**Explanation/Reference:**

NetFlow facilitates solutions to many common problems encountered by IT professionals.

- Analyze new applications and their network impact

Identify new application network loads such as VoIP or remote site additions.

- Reduction in peak WAN traffic

Use NetFlow statistics to measure WAN traffic improvement from application-policy changes; understand who is utilizing the network and the network top talkers.

- Troubleshooting and understanding network pain points

Diagnose slow network performance, bandwidth hogs and bandwidth utilization quickly with command line interface or reporting tools.

- Detection of unauthorized WAN traffic

Avoid costly upgrades by identifying the applications causing congestion.

- **Security and anomaly detection**

NetFlow can be used for anomaly detection and worm diagnosis along with applications such as Cisco CS-Mars.

- Validation of QoS parameters

Confirm that appropriate bandwidth has been allocated to each Class of Service (CoS) and that no CoS is over- or under-subscribed.

#### QUESTION 7

**Match each protocol with its description**

**DHCP**

**Transports coded voice streams**

**SCCP**

**Controls Cisco IOS gateways**

**RTP**

**Provides call signalling between Cisco IP Phones and CUCM**

**H.323**

**Provides IP address**

**TFTP**

**Provides phone registration**

**Select and Place:**

Match each protocol with its description

DHCP

Transports coded voice streams

SCCP

Controls Cisco IOS gateways

RTP

Provides call signalling between Cisco IP Phones and CUCM

H.323

Provides IP address

TFTP

Provides phone registration

Correct Answer:

Match each protocol with its description

RTP

H.323

SCCP

DHCP

TFTP

Section:  
Explanation

Explanation/Reference:

QUESTION 8

Match each component with its Cisco IPT functional area.

CUCM

Service applications

Layer 3 switch

Call processing

Digital gateway

Client endpoint

Unity

Infrastructure

Select and Place:

Match each component with its Cisco IPT functional area.

CUCM

Service applications

Layer 3 switch

Call processing

Digital gateway

Client endpoint

Unity

Infrastructure

Correct Answer:

Match each component with its Cisco IPT functional area.

Unity

CUCM

Digital gateway

Layer 3 switch

Section:  
Explanation

Explanation/Reference:

#### QUESTION 9

Match the routing protocol with the description

EIGRP

Distance-vector protocol used in the edge  
of the network

OSPFv2

IETF link-state protocol used in the  
network core

RIPv2

Hybrid protocol used in the network core

BGP

Path-vector protocol

Select and Place:

Match the routing protocol with the description

EIGRP

Distance-vector protocol used in the edge of the network

OSPFv2

IETF link-state protocol used in the network core

RIPv2

Hybrid protocol used in the network core

BGP

Path-vector protocol

Correct Answer:

Match the routing protocol with the description

RIPv2

OSPFv2

EIGRP

BGP

Section:  
Explanation

Explanation/Reference:

QUESTION 10

Place the PPDIOO Methodology in the correct order.

Optimize

Step 1

Design

Step 2

Prepare

Step 3

Implement

Step 4

Operate

Step 5

Plan

Step 6

Select and Place:

Place the PPDIOO Methodology in the correct order.

Optimize

Step 1

Design

Step 2

Prepare

Step 3

Implement

Step 4

Operate

Step 5

Plan

Step 6

Correct Answer:



Place the PPDIOO Methodology in the correct order.

Prepare

Plan

Design

Implement

Operate

Optimize

Section:  
Explanation

Explanation/Reference:

#### QUESTION 11

Drag the network characteristics on the left to the appropriate Access-Distribution block design on the right.

Fastest network convergence using routing

Loop-free topology

Uses FHRP

VLANs span multiple access layer switches

Layer 2 between Access and Distribution with  
Layer 2 link between the Distribution switches

Layer 2 between Access and Distribution with  
Layer 3 link between the Distribution switches

Layer 2 between Access and Distribution with  
Layer VSS link between the Distribution switches

Layer 3 between Access and Distribution with  
Layer 3 link between the Distribution switches

Select and Place:



Drag the network characteristics on the left to the appropriate Access-Distribution block design on the right.

Fastest network convergence using routing

Layer 2 between Access and Distribution with Layer 2 link between the Distribution switches

Loop-free topology

Layer 2 between Access and Distribution with Layer 3 link between the Distribution switches

Uses FHRP

Layer 2 between Access and Distribution with Layer VSS link between the Distribution switches

VLANs span multiple access layer switches

Layer 3 between Access and Distribution with Layer 3 link between the Distribution switches

**Correct Answer:**

Drag the network characteristics on the left to the appropriate Access-Distribution block design on the right.

VLANs span multiple access layer switches

Uses FHRP

Loop-free topology

Fastest network convergence using routing

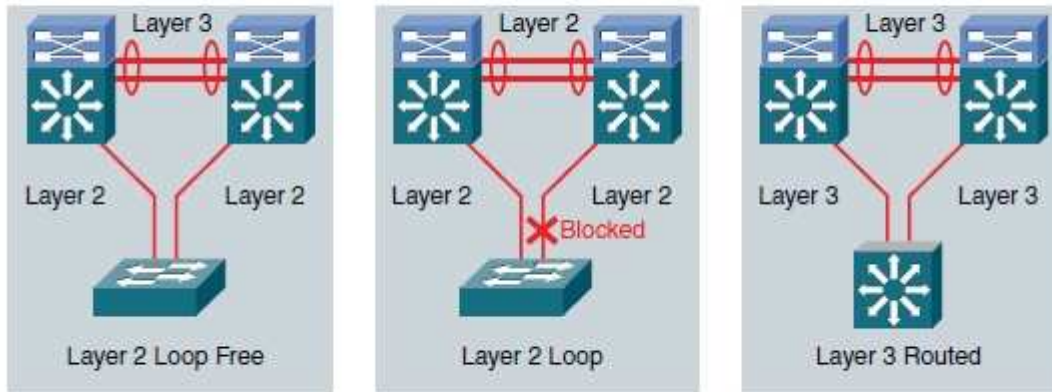
**Section:**  
**Explanation**

**Explanation/Reference:**

I changed this answer to reflect CCDP explanation:

## Common Access-Distribution Block Designs

Figure 2-15 shows the most common access-distribution block designs: Layer 2 loop free, Layer 2 looped, and Layer 3 routed.

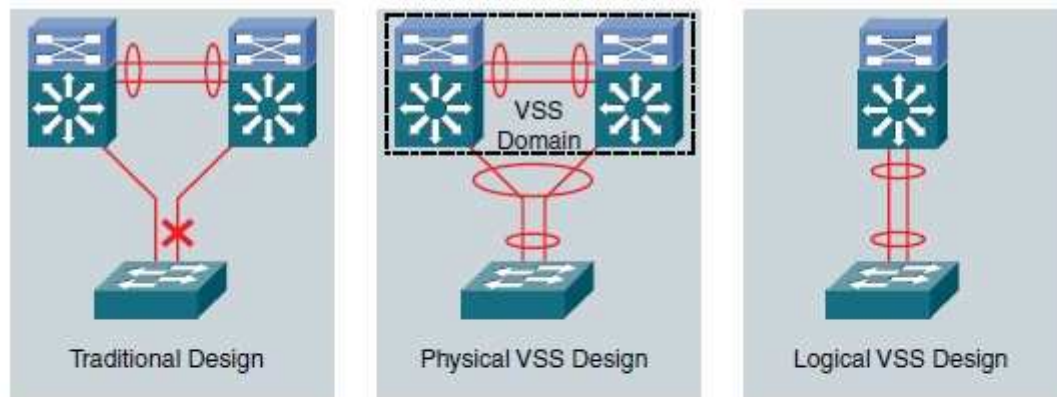


**Figure 2-15** *Access-Distribution Block Designs*

■ **Layer 2 loop-free design:** In this design, the access switches use Layer 2 switching. The links between the access and distribution layers are configured as Layer 2 trunks. The link between the distribution switches is configured as a Layer 3 routed link. An EtherChannel is typically used for this link to increase availability. In this design, there are no Layer 2 loops in the access-distribution block, which means that the Spanning Tree Protocol is not involved in network convergence and load balancing. All the ports are in the spanning-tree Forwarding state. Load balancing of the traffic from the access to the distribution layer is based on the First Hop Router Protocol (FHRP) that is used in this design. Reconvergence time in the case of failure is driven primarily by FHRP reconvergence. A limitation of this solution is that it is optimal for networks where each access layer VLAN can be constrained to a single access switch. Stretching VLANs across multiple access switches is not recommended in this design.

■ **Layer 2 looped design:** The Layer 2 looped design also uses Layer 2 switching on the access layer, and the links between the access and distribution switches are also configured as Layer 2 trunks. However, unlike the Layer 2 loop-free design, the link between the distribution switches is configured here as a Layer 2 trunk. This configuration introduces a Layer 2 loop between the distribution switches and the access switches. To eliminate this loop from the topology, the Spanning Tree Protocol blocks one of the uplinks from the access switch to the distribution switches. This design is recommended for networks that require an extension of VLANs across multiple access switches. A drawback is that network convergence in the case of failure is now dependent on spanning-tree convergence that is combined with FHRP convergence. Another downside is limited load balancing. PVST root election tuning can be used to balance traffic on a VLAN-by-VLAN basis. However, within each VLAN, spanning tree always blocks one of the access switch uplinks.

■ **Layer 3 routed design:** The Layer 3 routed design uses Layer 3 routing on the access switches. All links between switches are configured as Layer 3 routed links. The advantage of this design is that it eliminates the Spanning Tree Protocol from the interswitch links. It is still enabled on edge ports to protect against user-induced loops, but it does not play a role in the network reconvergence in the access-distribution block. FHRPs are also eliminated from the design, because the default gateway for the end hosts now resides on the access switch instead of on the distribution switch. Network reconvergence behavior is determined solely by the routing protocol being used. Like the Layer 2 loop-free design, the Layer 3 routed design constrains VLANs to a single access switch. Also, this design does not allow VLANs to be extended across multiple access switches, and it requires more sophisticated hardware for the access switches.

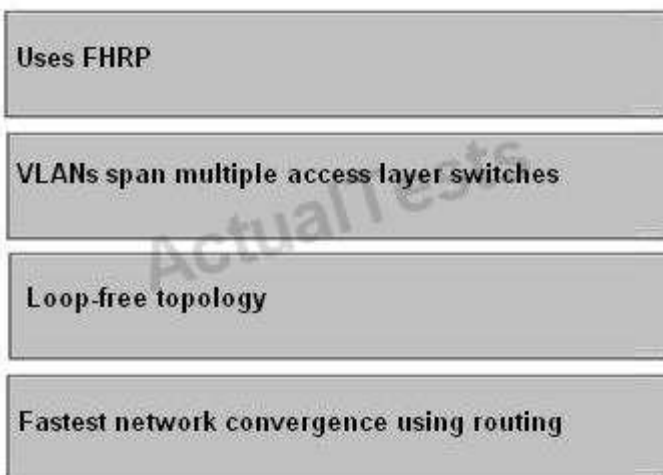


**Figure 2-16** VSS and MEC

Because the Spanning Tree Protocol recognizes the EtherChannel link as a single logical link, spanning tree is effectively removed from the network topology. Like the Layer 2 loop-free design, spanning tree is still enabled to guard against loops that are caused by miswiring or other human errors. It no longer plays a role in network convergence, however. A primary advantage of designs that are based on the MEC is that all links between the access and distribution layers are used in forwarding. Traffic is load balanced across the links through the EtherChannel hashing mechanisms.

Another advantage is that this design allows VLANs to extend across multiple access switches if necessary, without introducing Layer 2 loops into the topology.

This WAS 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:**

**QUESTION 12**

Drag the description or characteristics on the left to the appropriate technology or protocol on the right

provides complete network visibility from the physical layer to the application layer

SNMP

processes larger ACLs efficiently for packet filtering and security services

RMON

defines how information is exchanged between network management applications and agents

CDP

runs over the data link layer using a multicast address

NetFlow

**Select and Place:**

Drag the description or characteristics on the left to the appropriate technology or protocol on the right

provides complete network visibility from the physical layer to the application layer

SNMP

processes larger ACLs efficiently for packet filtering and security services

RMON

defines how information is exchanged between network management applications and agents

CDP

runs over the data link layer using a multicast address

NetFlow

**Correct Answer:**



Drag the description or characteristics on the left to the appropriate technology or protocol on the right

defines how information is exchanged between network management applications and agents

provides complete network visibility from the physical layer to the application layer

runs over the data link layer using a multicast address

processes larger ACLs efficiently for packet filtering and security services

**Section:**  
**Explanation**

**Explanation/Reference:**

#### QUESTION 13

The first phase of PPDIOO entails identifying customer requirements. Drag the example on the left to the associated requirement on the right.

Budget

Identify existing and planned network applications

Email and HTTP

Identify existing and planned network resources

Application compatibility

Define organizational constraints

IP telephone and video

Define the technical goals

Security

Define the technical constraints

**Select and Place:**

The first phase of PPDIOO entails identifying customer requirements. Drag the example on the left to the associated requirement on the right.

Budget

Identify existing and planned network applications

Email and HTTP

Identify existing and planned network resources

Application compatibility

Define organizational constraints

IP telephone and video

Define the technical goals

Security

Define the technical constraints

**Correct Answer:**

The first phase of PPDIOO entails identifying customer requirements. Drag the example on the left to the associated requirement on the right.

Email and HTTP

IP telephone and video

Budget

Security

Application compatibility

**Section:**  
**Explanation**

**Explanation/Reference:**

**QUESTION 14**

Drag the associated virtualization tool or solution on the left to the appropriate design requirement on the right.

VLANs and VSANs	virtual-machine
Cisco Unified Computing System	simplified data c
Cisco VN-Link technologies, including the Nexus 1000V Virtual Switch for Vmware ESX	network, compute, and virtual deliver and optimized
VSAN, virtual device contents, and unified fabric	physical networks and ec

Select and Place:

Drag the associated virtualization tool or solution on the left to the appropriate design requirement on the right.

VLANs and VSANs	virtual-machine
Cisco Unified Computing System	simplified data c
Cisco VN-Link technologies, including the Nexus 1000V Virtual Switch for Vmware ESX	network, compute, and virtual deliver and optimized
VSAN, virtual device contents, and unified fabric	physical networks and ec

Correct Answer:

Drag the associated virtualization tool or solution on the left to the appropriate design requirement on the

Cisco VN-Link technologies,  
for

VSAN, virtual dev

Cisco Unifi

VLA

Section:

Explanation

Explanation/Reference:



## **Exam G**

### **QUESTION 1**

Which two common cable management strategies are used in high-density server deployments in the data center? (Choose two.)

- A. top-of-rack
- B. middle-of-rack
- C. bottom-of-rack
- D. beginning-of-row
- E. middle-of-row
- F. end-of-row

**Correct Answer:** AF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 2**

Which protocol is the recommended first-hop redundancy protocol for an existing infrastructure that contains multiple vendors and platforms?

- A. HSRP
- B. VRRP
- C. IGRP
- D. OSPF

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 3**

Which IGP provides the fastest convergence by default?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 4**

Which three are valid Layer 2 access designs? (Choose three.)






- A. Looped Triangle
- B. Looped Square
- C. Looped U
- D. Loop-Free Triangle
- E. Loop-Free Square
- F. Loop-Free U

**Correct Answer:** ABF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

		Uplinks on Agg Switch in Blocking or Standby State	VLAN Extension Supported Across Access	Service Module Black-Holing on Uplink Failure (5)	Single Attached Server Black- Holing on Uplink Failure	Access Switch Density per Agg Module	Must Consider Inter-Switch Link Scaling
	Looped Triangle	-	+	+	+	-	(3) +
	Looped Square	+	+	+	+	+	-
	Loop-free U	+	-	(4) -	+	+	+
	Loop-free Inverted U	+	+	+	(1, 2) +/-	+	-
	FlexLinks	-	+	+	+	-	+

1. Use of Distributed EtherChannel Greatly Reduces Chances of Black Holing Condition
2. NIC Teaming Can Eliminate Black Holing Condition
3. When Service Modules Are Used and Active Service Modules Are Aligned to Agg1
4. ACE Module Permits L2 Loopfree Access with per Context Switchover on Uplink failure
5. Applies to when using CSM or FWSM in active/standby arrangement

15/30/46

Comparison Chart of Access Layer Designs

**QUESTION 5**

Which two enterprise campus layers are combined in a medium-sized LAN? (Choose two.)

- A. core
- B. distribution
- C. access
- D. backbone

E. aggregation

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

***Distribution Layer:***

The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. The distribution layer controls the flow of network traffic using policies and delineates broadcast domains by performing routing functions between virtual LANs (VLANs) defined at the access layer.

VLANs allow you to segment the traffic on a switch into separate subnetworks. For example, in a university you might separate traffic according to faculty, students, and guests. Distribution layer switches are typically high-performance devices that have high availability and redundancy to ensure reliability. You will learn more about VLANs, broadcast domains, and inter-VLAN routing later in this book.

***Core Layer***

The core layer of the hierarchical design is the high-speed backbone of the internetwork.

The core layer is critical for interconnectivity between distribution layer devices, so it is important for the core to be highly available and redundant. The core area can also connect to Internet resources. The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly.

***Note***

***In small networks, it is not unusual to implement a collapsed core model, where the distribution layer and core layer are combined into one layer.***

**QUESTION 6**

What is a characteristic of campus core designs?

- A. fast transport
- B. security
- C. summarization
- D. redistribution

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The campus core is in some ways the simplest yet most critical part of the campus. It provides a very limited set of services and is designed to be highly available and operate in an always-on mode. In the modern business world, the core of the network must operate as a non-stop 7x24x365 service. The key design objectives for the campus core are based on providing the appropriate level of redundancy to allow for near immediate data-flow recovery in the event of any component (switch, supervisor, line card, or fiber) failure. The network design must also permit the occasional, but necessary, hardware and software upgrade/change to be made without disrupting any network applications. The core of the network should not implement any complex policy services, nor should it have any directly attached user/server connections. The core should also have the minimal control plane configuration combined with highly available devices configured with the correct amount of physical redundancy to provide for this non-stop service capability.

**QUESTION 7**

Which servers that reside in the data center require direct links to all other enterprise modules?

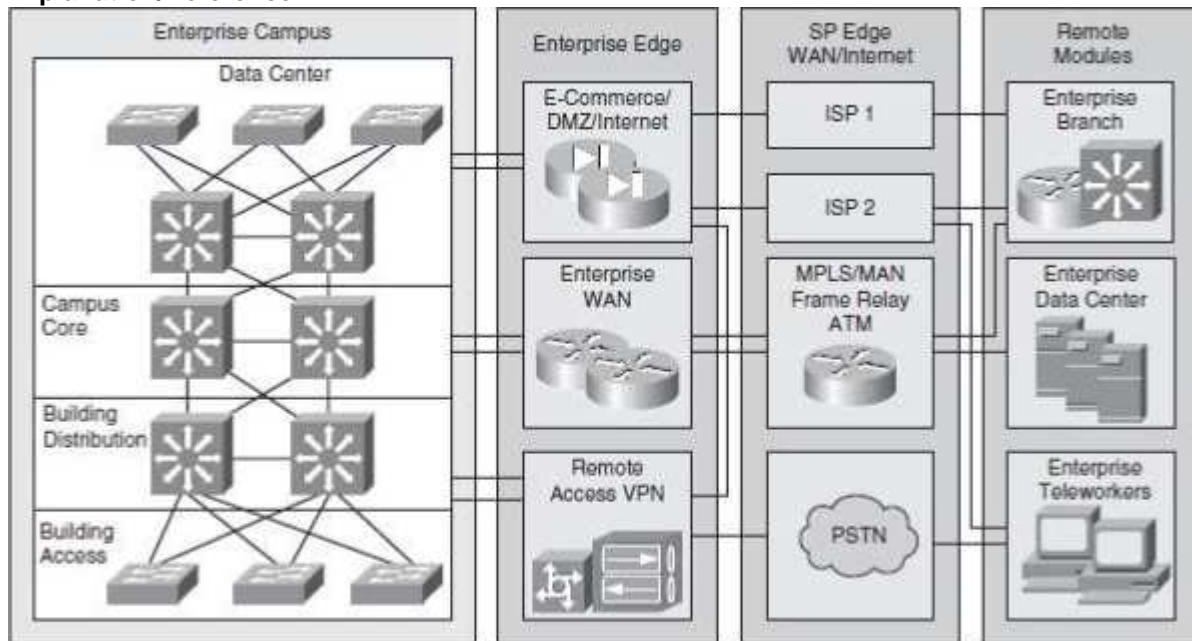
- A. network management servers
- B. DHCP servers
- C. Active Directory servers
- D. IP SLA servers
- E. web servers

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**Figure 2-5** Cisco Enterprise Architecture Model

The network management servers reside in the campus infrastructure but have tie-ins to all the components in the enterprise network for monitoring and management.

#### QUESTION 8

Which Gigabit Ethernet media type provides the longest reach without a repeater?

- A. 1000Base-CX
- B. 1000Base-LX
- C. 1000Base-SX
- D. 1000Base-T

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

1000BASE-LX 62.5µm MMF 550m 1310nm  
1000BASE-LX 50µm MMF 550m 1310nm  
1000BASE-LX/LH SMF 10km 1310nm

#### QUESTION 9

Which three options represents the components of the Teleworker Solution? (Choose three.)

- A. Cisco Unified IP Phone
- B. Cisco 880 Series Router
- C. Aironet Office Extend Access Point
- D. Catalyst 3560 Series Switch
- E. Cisco 2900 Series Router
- F. MPLS Layer 3 VPN
- G. Leased lines

**Correct Answer:** ABE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

I dot know why Cisco2900 is an answer.... But its like that :) This question is already there I think.

#### QUESTION 10

What is the maximum number of groups that is supported by GLBP?

- A. 64
- B. 256
- C. 512
- D. 1024

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 11

Which three service categories are supported by an ISR? (Choose three.)

- A. voice
- B. security
- C. data
- D. Internet
- E. storage
- F. satellite

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 12**

Which three protocols support VLSM? (Choose three.)

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

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 13**

Which statement describes a unique advantage of EIGRP?

- A. It enables unequal-cost load balancing.
- B. It enables equal-cost load balancing.
- C. It enables source-based load balancing
- D. It enables port-based load balancing.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 14**

ACME corporation is implementing dynamic routing on the LAN at its corporate headquarters. The interior gateway protocol that they select must support these requirements: multivendor environment, efficient subnetting, high scalability, and fast convergence.

Which interior gateway protocol should they implement?

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

**Correct Answer:** A

**Section:** (none)

## **Explanation**

### **Explanation/Reference:**

MultiVendor and Fast Convergence.

### **QUESTION 15**

Which routing protocol classification should you use when full topology information is needed?

- A. link-state
- B. distance vector
- C. stateful
- D. path vector

**Correct Answer:** A

**Section:** (none)

## **Explanation**

### **Explanation/Reference:**

Link-State Routing protocols are routing protocols whose algorithms calculate the best paths to networks differently than Distance Vector routing protocols. Whereas Distance Vector protocols know routes by measures of distance and vector(direction) as reported by neighboring routers, Link-State routing protocols calculate their network routes by building a complete topology of the entire network area and then calculating the best path from this topology or map of all the interconnected networks.

### Link-State Advantages

**Faster Convergence** - Unlike Distance Vector routing protocols which run algorithm calculations before sending updates, Link-State routing protocols send link-state updates to all routers in the network before running route calculations

**Triggered Updates** - Unlike Distance Vector routing protocols (except EIGRP) which send periodic updates at regular intervals, Link-State routing protocols send LSPs during router startup (flooding) and when a link changes states like going up or down. If there are no changes in the network the protocol only sends hello packets to maintain adjacencies.

**Scalability** - Link-State routing protocols support the ability to configure multiple routing "areas" which allows an administrator to segment a routing protocol processes to defined areas which supports the expansion and troubleshooting of much larger networks.

### Link-State Disadvantages

**Greater Processing Requirements** - Link-State routing protocols typically demand greater processing power and memory resources from the router.

**Greater Administrator Knowledge** - Link-State routing protocols can demand advanced administrator knowledge to configure and troubleshoot the network area

### **QUESTION 16**

When you are designing a large IPv6 multivendor network, which IGP does Cisco recommend that you use?

- A. OSPFv3
- B. EIGRP for IPv6
- C. BGP
- D. RIPng

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Multivendor for Large Networks..... OSPF

**QUESTION 17**

When designing the infrastructure protection portion for the enterprise edge, which solution 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:**

**QUESTION 18**

Which two design approaches provide management of enterprise network devices? (Choose two.)

- A. in-band
- B. out-of-line
- C. out-of-band
- D. in-line

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

In-Band

PROS

- Agnostic to switch/router platform and versions
- Appropriate for wired and wireless
- Full network access control
- Bandwidth management control

CONS

- Inline dependency
- No switch-port-level control

Out-of-Band

PROS:

- Inline-only for quarantined traffic



- Full access control in quarantine
- Smooth switch control via Simple Network Management Protocol (SNMP)
- Port- or role-based VLAN assignment

**CONS:**

- Switch platform and version dependencies
- Most appropriate for wired scenarios

(C) Aqeel

**QUESTION 19**

Refer to the list of requirements.

Which IP telephony design model should you implement to fulfill these requirements?

- Must be a single, large location with many remote sites
- Must have multisite WAN connectivity
- Requires SRST for call processing redundancy

- A. centralized
- B. distributed
- C. clustered
- D. decentralized

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 20**

What are the three modes of unicast reverse path forwarding? (Choose three.)

- A. strict
- B. loose
- C. VRF
- D. global
- E. PIM
- F. local

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Network administrators can use Unicast Reverse Path Forwarding (Unicast RPF) to help limit the malicious traffic on an enterprise network.

This security feature works by enabling a router to verify the reachability of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP

address is not valid, the packet is discarded. Unicast RPF works in one of three different modes: strict mode, loose mode, or VRF mode. Note that not all network devices support all three modes of operation. Unicast RPF in VRF mode will not be covered in this document.

When administrators use Unicast RPF in strict mode, the packet must be received on the interface that the router would use to forward the return packet. Unicast RPF configured in strict mode may drop legitimate traffic that is received on an interface that was not the router's choice for sending return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths are present in the network.

When administrators use Unicast RPF in loose mode, the source address must appear in the routing table. Administrators can change this behavior using the allow-default option, which allows the use of the default route in the source verification process. Additionally, a packet that contains a source address for which the return route points to the Null 0 interface will be dropped. An access list may also be specified that permits or denies certain source addresses in Unicast RPF loose mode.

Care must be taken to ensure that the appropriate Unicast RPF mode (loose or strict) is configured during the deployment of this feature because it can drop legitimate traffic. Although asymmetric traffic flows may be of concern when deploying this feature, Unicast RPF loose mode is a scalable option for networks that contain asymmetric routing paths.

#### **QUESTION 21**

Which network access control technology is recommended to use with Layer 2 access layer switches?

- A. 802.1q
- B. 802.1x
- C. 802.3af
- D. 802.3q
- E. 802.11n

**Correct Answer:** B

**Section:** (none)

**Explanation**

#### **Explanation/Reference:**

802.1X provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority. The actual algorithm that is used to determine whether a user is authentic is left open and multiple algorithms are possible.

(A.K).

Cisco Guide Reference:

Understanding 802.1X Port-Based Authentication

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange

- Ports in Authorized and Unauthorized States
- Supported Topologies

#### QUESTION 22

Which technology enables WLCs to peer with each other to enable roaming support?

- A. WAP profiles
- B. roaming profiles
- C. mobility groups
- D. peer groups

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

A Mobility Group is a group of Wireless LAN Controllers (WLCs) in a network with the same Mobility Group name. These WLCs can dynamically share context and state of client devices, WLC loading information, and can also forward data traffic among them, which enables inter-controller wireless LAN roaming and controller redundancy. Refer to the Configuring Mobility Groups section of Cisco Wireless LAN Controller Configuration Guide, Release 7.0 for more information.

. A Mobility Group is configured manually. The IP and MAC address of the Wireless LAN Controllers (WLCs) that belong to the same Mobility Group are configured on each of the WLCs individually. Mobility Groups can be configured either through the CLI or the GUI.



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