PassQueen
a.k.a dumpsqueen.com

Cisco Routing and Switching Solutions Specialist

Cisco 644-066

Version Demo

Total Demo Questions: 12

Total Premium Questions: 124

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which Cisco advanced technology provides interconnected storage area networks so that you can reduce costs and improve reliability?

A. Cisco Unified Communications

B. Data Center

C. Mobility
Network Management

D. Security

ANSWER: B

Explanation:

Data Center is correct because Cisco data-center technologies encompass storage networking and SAN interconnection capabilities designed to consolidate, extend, and operate storage resources across the data center. Cisco SAN solutions use platforms such as the Cisco MDS family and Nexus data-center switches to provide high-availability Fibre Channel and IP-based storage connectivity. Interconnecting SANs enables organizations to centralize storage operations, use resources more efficiently, and support resilient designs across separate locations or fabrics. This can lower operational and infrastructure costs through consolidation and simplified management while improving reliability through redundant paths, resilient fabrics, nondisruptive operations, and replication-oriented architectures. Cisco describes its MDS portfolio as providing highly available storage networking for mission-critical applications, with capabilities intended to simplify SAN operations and protect availability. These functions are core data-center capabilities rather than endpoint collaboration or access-network functions. Cisco's data-center portfolio also explicitly includes networking infrastructure for connecting compute, storage, and applications, making Data Center the technology category that directly matches interconnected storage area networks. See Cisco's SAN switches overview and data center networking overview for further details.

QUESTION NO: 2

Which of the following statements correctly describes the platform module slot evolution from pre-ISR through ISR to ISR G2?

A. All three platforms support WIC, VWIC, and VIC.?

B. NM and NME can be used in the ISR G2 via an adapter. NME-X is not supported on ISR G2.?

C. All three platforms support AIM.

D. ISR and ISR G2 support PVDM2; no adapter is required in ISR G2.?

ANSWER: B

Explanation:

NM and NME can be used in the ISR G2 via an adapter. NME-X is not supported on ISR G2. This accurately reflects Cisco's investment-protection approach during the transition to second-generation Integrated Services Routers. ISR G2 platforms introduced Service Module slots and newer module families, but Cisco also provided the SM-NM-ADPTR network-module adapter to allow supported legacy Network Modules and Network Module Enhanced cards to be deployed in an ISR G2 chassis. This lets organizations preserve selected existing module investments while migrating router platforms and adopting newer ISR G2 capabilities.

The compatibility is not universal: it depends on both the adapter and the specific legacy module. Cisco's ISR G2 hardware documentation identifies the network-module adapter as the mechanism for installing supported NM and NME modules, while certain module types—including NME-X—are excluded from ISR G2 support. This distinction is important for hardware planning because physical slot form factor alone does not establish compatibility; platform power, architecture, software

support, and validated adapter support also apply. Cisco's ISR G2 data sheet describes the modular architecture and backward-investment considerations, and the hardware installation documentation details supported module installation through the adapter. See Cisco ISR G2 data sheet and Cisco 3900 Series hardware installation guide.

QUESTION NO: 3

Which three statements are true about Cisco distribution switches? (Choose three.)

A. The Cisco Catalyst 3750 Series Switches are suitable for small site aggregation.

B. The Cisco Catalyst 4500 Series Switches are suitable for collapsed access and distribution.

C. The Cisco Catalyst 4500 Series Switches are typically used at small branches.

D. The Cisco Catalyst 6500 Series Switches are suitable for collapsed core and distribution.

E. The Cisco Catalyst 4500 and 6500 Series Switches both support borderless service modules and the Virtual Switching System (VSS).

ANSWER: A B D

Explanation:

The Cisco Catalyst 3750 Series Switches are suitable for small site aggregation because their stackable design provides a practical distribution-layer solution where a separate, high-capacity chassis-based distribution pair is unnecessary. StackWise allows multiple switches to operate as one logical unit, simplifying management while providing aggregation and Layer 3 capabilities appropriate to smaller campus sites.

The Cisco Catalyst 4500 Series Switches are suitable for collapsed access and distribution because this modular platform was designed to combine access-layer connectivity with distribution-layer policy, resiliency, and routing functions in a single chassis. This model is especially useful where the scale and physical layout do not justify distinct access and distribution tiers.

The Cisco Catalyst 6500 Series Switches are suitable for collapsed core and distribution because the platform provides high chassis capacity, modular interfaces, and substantial Layer 3 and service capability. In a campus design, these characteristics allow it to aggregate distribution functions while also providing the highly available, high-performance forwarding expected of a collapsed core. These platform roles reflect the hierarchical campus design guidance and product positioning applicable to this legacy certification topic. See Cisco's Catalyst 3750 Series data sheet and Catalyst 6500 campus design documentation.

QUESTION NO: 4

You are designing a campus network and you want to provide a resilient default gateway to end services. Which campus network component should you use?

A. Layer 3 routing protocols

B. UniDirectional Link Detection

C. First Hop Redundancy Protocol

D. load balancing

ANSWER: C

Explanation:

First Hop Redundancy Protocol is correct because it provides hosts with a highly available default gateway. End devices normally use one configured default-gateway IP address and do not dynamically select a replacement gateway when that router fails. A first-hop redundancy protocol solves this issue by presenting a shared virtual IP address, and usually a shared virtual MAC address, to the LAN. One gateway device actively forwards traffic for the virtual gateway, while another device

monitors the active device and can take over forwarding if a failure occurs. This allows endpoints to continue using the same configured default gateway without requiring manual reconfiguration or waiting for a routing-protocol convergence event. Cisco platforms support first-hop redundancy through protocols such as Hot Standby Router Protocol, Virtual Router Redundancy Protocol, and Gateway Load Balancing Protocol. In a campus design, deploying one of these protocols on the multilayer switches or routers that provide the user VLAN gateway is a standard method of improving default-gateway resilience. Cisco describes HSRP as a mechanism that provides network redundancy for IP traffic from hosts on Ethernet networks, with a virtual router serving as the gateway. See Cisco IOS XE HSRP Configuration Guide and Cisco HSRP Overview.

QUESTION NO: 5

Given a Cisco Catalyst 4500 Series Switch with redundant supervisors, what feature allows phone calls to remain up in the event of a supervisor failure?

A. HSRP

B. SSO

C. CEF

D. NSF

E. NetFlow

ANSWER: B

Explanation:

SSO is correct because Stateful Switchover maintains synchronization of critical Layer 2 and Layer 3 control-plane information between the active and standby supervisor engines in a redundant Cisco Catalyst 4500 Series Switch. If the active supervisor fails, the standby supervisor takes over using the already synchronized state rather than initializing the system from scratch. This minimizes disruption to the forwarding plane and preserves established network connectivity.

For IP telephony, maintaining forwarding during supervisor failover is essential: phones need continuing access to call-control services and media paths so that established calls are not dropped. Cisco documents SSO as the redundancy mode that provides subsecond supervisor failover and supports nonstop forwarding capabilities when used with the appropriate hardware and software features. The standby supervisor is prepared to assume the active role immediately, substantially reducing the outage that would otherwise affect voice traffic. See Cisco's Catalyst 4500 Series release notes and the Catalyst 4500 software configuration guide for redundancy and SSO operation details.

QUESTION NO: 6

Which two of these protocols can be used to provide secure connectivity when connecting a branch office to the campus core? (Choose two.)

A. GRE

B. L2TP

C. IPsec

D. IP in IP

E. L2TP over IPsec

ANSWER: C E

Explanation:

IPsec is appropriate because it provides network-layer VPN protection for traffic exchanged between a branch office and a campus-core network across an untrusted IP transport network. IPsec uses security associations negotiated through IKE to

apply authentication, integrity protection, anti-replay services, and encryption through Encapsulating Security Payload (ESP). This makes it a standard foundation for site-to-site VPN connectivity, while allowing private routing between the connected locations.

L2TP over IPsec is also secure because L2TP supplies the tunneling mechanism and IPsec protects the L2TP packets in transit. The combined design is commonly used where Layer 2 tunneling is needed while IPsec delivers the confidentiality and integrity safeguards required over a public or otherwise untrusted network. In this arrangement, security is provided by the IPsec protection surrounding the L2TP tunnel, so it can securely carry branch-to-campus connectivity traffic. Cisco describes IPsec VPN operation and IKE negotiation at Cisco: IPsec and IKE. The L2TP-over-IPsec encapsulation and security model is specified in RFC 3193.

QUESTION NO: 7

During which PPDIOO phase is the existing network characterized to identify gaps between the current environment and the required capabilities?

A. Prepare

B. Plan

C. Design

D. Implement

E. Optimize

ANSWER: B

Explanation:

Plan is correct. The Plan phase assesses the existing network environment, documents its current capabilities, and identifies gaps relative to the business and technical requirements established during Prepare. Typical activities include site surveys, inventory collection, traffic characterization, risk analysis, and development of a project plan.

The resulting information provides the basis for the detailed solution work performed during the Design phase. Cisco lifecycle guidance describes Plan as the phase in which the current network is assessed and requirements are translated into a deployment plan. See the Cisco PPDIOO network lifecycle overview.

QUESTION NO: 8

In the Cisco Catalyst 6500-E Series chassis, what are three key chassis specifications? (Choose three.)

A. requires Cisco IOS 12.2(1) SXD and beyond

B. three-slot chassis supports CEF720 line cards

C. is backward-compatible with all existing software versions

D. six- and nine-slot chassis support only 6000-W power supplies

E. supports all existing supervisors, line cards, switch fabrics, and software releases

ANSWER: B C E

Explanation:

The Cisco Catalyst 6500-E chassis family was designed as an evolutionary platform upgrade that retained broad investment protection for deployed Catalyst 6500 hardware and software. The three-slot chassis supports CEF720 line cards because the 6503-E chassis provides the architecture and slot connectivity required for these higher-performance, fabric-enabled modules. This makes the compact E-Series chassis suitable where CEF720-capable line-card support is required without deploying a larger chassis.

The statements that it is backward-compatible with all existing software versions and that it supports all existing supervisors, line cards, switch fabrics, and software releases express the E-Series family's core compatibility objective. Cisco positioned the E-Series chassis to preserve use of established Catalyst 6500 components while adding capacity and environmental improvements. Consequently, existing supervisor engines, line cards, and switch-fabric components can be retained, and established software releases remain usable as applicable to the installed hardware. Cisco's Catalyst 6500 product documentation describes the E-Series chassis as maintaining compatibility with the Catalyst 6500 ecosystem; see the Cisco Catalyst 6500 Series product page and Cisco's Catalyst 6500 Series data sheet.

QUESTION NO: 9

Which two statements are true about CVD and SBA? (Choose two.)?

A. The SBA toolset includes Partner Enablement Assets and EcoPartner Guides.

B. SBA guides are available for enterprise deployments only.

C. CVDs are end-to-end designs which are well-tested and fully documented.

D. Gold partners have access to a demo lab for each validated design.

ANSWER: A C

Explanation:

The SBA toolset includes Partner Enablement Assets and EcoPartner Guides. Cisco Smart Business Architecture was created to help partners and customers deploy validated solutions using practical implementation materials, including design and deployment guides, partner-oriented enablement resources, and guidance for integrating complementary ecosystem products. These assets make the architecture more repeatable for common customer environments and help partners move from a high-level solution design to deployment activities.

CVDs are end-to-end designs which are well-tested and fully documented. Cisco Validated Designs provide prescriptive, documented architectures that Cisco develops and validates through testing. A CVD typically brings together technologies, design guidance, configuration recommendations, and operational considerations for an end-to-end solution. The validation and documentation are important because they provide an implementation baseline that customers and partners can use with greater confidence than an untested reference design. Cisco's validated-design portfolio and its associated documentation are available through the Cisco Design Zone. See Cisco Design Zone and Cisco Smart Business Architecture.

QUESTION NO: 10

Which two are switch security features that enable a secure borderless network? (Choose two.)

A. device profiling and profile-based selection of security policies

B. Cisco ASA Firewall

C. MACSec

D. Security Group Tagging

ANSWER: C D

Explanation:

MACSec and **Security Group Tagging** are switch-based capabilities that support Cisco's secure borderless-network approach. MACsec, defined by IEEE 802.1AE, provides Layer 2 confidentiality, integrity, and origin authentication for Ethernet frames on a protected link. On supported Cisco switches, it protects traffic traversing access, uplink, or inter-switch Ethernet connections, reducing the exposure of data to interception or modification within the wired network.

Security Group Tagging is a core Cisco TrustSec capability. A Security Group Tag is assigned according to identity and policy, then carried with traffic so that enforcement can be based on logical group membership rather than only IP

addresses, VLANs, or physical location. This enables consistent segmentation and policy enforcement as users and devices move across the network, which is fundamental to a borderless design. Together, MACsec secures the Ethernet transport while Security Group Tagging enables identity-based segmentation and access control. Cisco describes these TrustSec mechanisms in its TrustSec architecture overview and documents MACsec capabilities in its MACsec product information.

QUESTION NO: 11

Which three statements correctly describe the Cisco router portfolio? (Choose three.)

A. The Cisco 800 Series Integrated Services Router family is a 1-RU solution for small offices.

B. The Cisco 1900 Series Integrated Services Router family is a 1-RU solution for small offices.

C. The Cisco 1900 Series Integrated Services Router family provides a modular solution for small offices.

D. The Cisco 800 Series Integrated Services Router family includes 3G WAN options.

E. The Cisco 2900 Series Integrated Services Router family provides interactive media services and service virtualization or midrange deployments.

F. The Cisco 2900 Series Integrated Services Router family provides interactive media services, including TelePresence.

ANSWER: C D E

Explanation:

The Cisco 1900 Series Integrated Services Router family provides a modular solution for small offices because these Integrated Services Routers support field-installable interface and service modules, allowing a branch to add WAN connectivity and other services as its requirements grow. This modular design made the platform appropriate for small branch and small-office deployments that needed more flexibility than a fixed-configuration router. Cisco's ISR G2 portfolio documentation describes the modular architecture and branch-focused role of the 1900 platform: Cisco 1900 Series ISR data sheet.

The Cisco 800 Series Integrated Services Router family includes 3G WAN options. Selected 800-series models were designed for small-office, teleworker, and mobile deployments and supported integrated cellular WAN access, including 3G capabilities, to provide primary connectivity or WAN backup. The Cisco 2900 Series Integrated Services Router family provides interactive media services and service virtualization or midrange deployments because it was positioned as a higher-capacity modular branch platform. Its architecture supports integrated services, including collaboration and rich-media capabilities, while supplying the performance and expansion needed for midrange branch locations. Cisco documents these platform capabilities in its Cisco 2900 Series ISR data sheet.

QUESTION NO: 12

Which spanning-tree protection feature places a PortFast-enabled access port into an error-disabled state when it receives a BPDU?

A. BPDU guard

B. Root guard

C. Loop guard

D. UplinkFast

E. EtherChannel guard

ANSWER: A

Explanation:

BPDU guard is correct. BPDU guard is applied to edge-facing ports, commonly ports configured with PortFast. If the port receives a BPDU, the switch treats this as evidence that another switch or bridge has been connected where an endpoint was expected and places the port into the error-disabled state.

This protects the Layer 2 topology by preventing an unauthorized switch from participating in spanning tree through an access port. Root guard has a different purpose: it prevents a downstream device from becoming the root bridge. Cisco documents BPDU guard as a spanning-tree protection mechanism for PortFast-enabled ports. See Cisco spanning-tree guard configuration guidance.