PassQueen
a.k.a dumpsqueen.com

Advanced Routing and Switching for Field Engineers – ARSFE

Cisco 644-068

Version Demo

Total Demo Questions: 7

Total Premium Questions: 79

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, LAN Switching	18
Topic 2, IP Routing	7
Topic 3, MPLS	1
Topic 4, IP Multicast	1
Topic 5, Network Services	27
Topic 6, Network Security	6
Topic 7, Mix Questions	19
Total	79

QUESTION NO: 1

Which of the following spanning-tree features provides rapid transition to the forwarding state for a port connected to a single end station?

A. PortFast

B. Root Guard

C. Loop Guard

D. UDLD aggressive mode

ANSWER: A

Explanation:

PortFast is correct because it causes an access port to bypass the normal listening and learning delay when the port comes up. This allows an attached endpoint, such as a workstation, IP phone, or server, to begin communicating quickly. PortFast should be enabled only on ports that do not connect to another switch, bridge, or shared Layer 2 segment. BPDU Guard is commonly deployed with PortFast to protect against an unexpected bridge connection.

See the Cisco PortFast Configuration Guide.

QUESTION NO: 2

Which three of the following statements correctly describe GET VPN? (Choose three.)

A. GET VPN uses a key server to distribute security policies and encryption keys to group members.

B. GET VPN preserves the original IP header of the customer packet.

C. GET VPN supports any-to-any encrypted communication between group members.

D. GET VPN requires a separate GRE tunnel to be configured between every pair of group members.

E. GET VPN replaces the routing protocol used between enterprise sites.

ANSWER: A B C

Explanation:

GET VPN uses a key server to distribute security policies and encryption keys to group members. The key server centrally manages the group security association and supplies the policy information required by participating routers.

GET VPN preserves the original IP header of the customer packet. Unlike tunnel-based VPN technologies that add a new outer IP header, GET VPN encrypts the payload while retaining the original source and destination addresses. This characteristic allows the service-provider MPLS network to continue using the original IP header for routing and QoS treatment.

GET VPN supports any-to-any encrypted communication between group members. Group members use the common group security association, so tunnels do not need to be built individually between every pair of sites. Cisco describes this group-encryption model in the Cisco GET VPN overview.

QUESTION NO: 3

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 VI

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; noadapter 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 describes the backward-compatibility approach used by Cisco ISR G2 platforms. The ISR G2 modular architecture introduced Service Module (SM) slots rather than providing native Network Module (NM) or Network Module Enhanced (NME) slots. Cisco provided the SM-NM-ADPTR service-module adapter so that supported legacy NM and NME modules could continue to be deployed in an ISR G2 router. This lets customers preserve appropriate existing module investments while moving to the newer router platform and its service-module architecture.

The adapter is an important qualification: legacy modules are not inserted directly into an ISR G2 service-module slot. Compatibility is mediated through the adapter and is subject to Cisco's supported-module list. Cisco specifically excludes NME-X enhanced network modules from support in this ISR G2 adapter arrangement. Thus, the statement correctly captures both the migration mechanism for supported NM/NME hardware and the NME-X limitation. Cisco's ISR G2 platform documentation describes its service-module expansion design, while the SM-NM adapter documentation defines the supported legacy-module compatibility model. See the Cisco 3900 Series ISR G2 data sheet and the Cisco SM-NM-ADPTR installation documentation.

QUESTION NO: 4

Which of the following statements regarding the WAAS vendor landscape is not true??

A. Riverbed is the market leader.

B. Blue Coat is number two in the WAAS market.

C. Riverbed lacks routing functionality.

D. The benefits of Cisco WAAS include scalability, the comprehensive product portfolio, and VDI vendor-validated optimization.

ANSWER: B

Explanation:

Blue Coat is number two in the WAAS market. is the untrue statement. In the WAN-optimization market context used by this Cisco training material, Riverbed was generally positioned as the market leader and Cisco WAAS was positioned as the principal number-two competitor. Cisco's WAAS offering combined WAN optimization with network-aware deployment and integration with Cisco routing and branch-office infrastructure, which was an important differentiator in Cisco's market positioning. Blue Coat was a recognized vendor in adjacent technologies, especially secure web gateways and proxy services, and also offered WAN-optimization capabilities, but it was not the vendor described as holding the number-two WAAS market position in this landscape. Cisco WAAS provided application acceleration, data reduction, and optimization for centralized applications and virtual-desktop workloads across WAN links. Its integration with the broader Cisco branch architecture supported scalable deployments and operational consistency. Cisco's WAN optimization product information is available at Cisco WAN Optimization. Historical industry coverage of WAN optimization and Riverbed's market leadership is also available from Riverbed's Gartner Magic Quadrant announcement.

QUESTION NO: 5

Which two of the following statements are true regarding placement of WAAS? (Choose two.)?

A. All WAE appliance models support inline deployment. Fail-to-wire capabilities ensure that traffic continues to flow through the system in case of ahardware or software failure.

B. Off-path interception of traffic can be achieved by policy-based routing or WCCP v2 interception.

C. Cisco WAAS Express supports off-path interceptiononly via WCCP v2 interception.

D. WAE appliances do not support 802.1Q.

ANSWER: B C

Explanation:

Off-path WAAS placement redirects selected traffic from a router or switch to a Wide Area Application Engine for optimization, rather than physically placing the appliance in the forwarding path. Cisco WAAS supports two established mechanisms for this redirection: policy-based routing, which forwards traffic matching configured policies to the WAE, and Web Cache Communication Protocol version 2, which enables network devices to redirect eligible flows to a cache engine. This flexibility allows deployment designs to select an interception method appropriate to the branch or data-center topology.

Cisco WAAS Express is the router-integrated WAAS capability and has a more limited off-path interception model. For WAAS Express, off-path traffic redirection is performed through WCCP version 2. WCCP provides the router with a standardized mechanism to identify and redirect applicable TCP flows to the WAAS Express service while retaining normal routing behavior for traffic that is not selected for optimization. Consequently, the statements identifying PBR or WCCP v2 for general off-path WAE interception, and WCCP v2 as the WAAS Express off-path method, are the accurate placement statements. Cisco's WAAS deployment information is available in the Cisco WAAS Deployment Guide and Cisco's WAAS product documentation portal.

QUESTION NO: 6

Which two of the following statements correctly describe Cisco Prime features that help improve operational efficiency? (Choose two.)

A. The Cisco Prime user interface is optimized for touchscreens.

B. All components of the Cisco Prime for Enterprise product portfolio provide a common look and feel, which simplifies usability.

C. Integrated workflows and best practices enable quick and error-free deployment.

D. TrustSec, MediaNet, and EnergyWise services are only configured outside Work Centers in Cisco Prime LMS.

ANSWER: B C

Explanation:

Cisco Prime was designed to centralize network lifecycle management and present management functions through a consistent operational experience. "All components of the Cisco Prime for Enterprise product portfolio provide a common look and feel, which simplifies usability." correctly identifies this common user experience as an efficiency feature: administrators can move among related management tasks without having to learn unrelated interfaces and interaction models for each product area. This consistency helps reduce operational overhead and speeds adoption of the platform's monitoring, configuration, and assurance capabilities.

"Integrated workflows and best practices enable quick and error-free deployment." is also correct because Cisco Prime provides guided workflows that connect common lifecycle activities, such as device onboarding, inventory, configuration deployment, and monitoring. By incorporating validated procedures, templates, and automation into these workflows, Prime helps teams perform repeatable changes more quickly and with fewer manual-entry mistakes. This is directly aligned with the platform's objective of simplifying network operations and improving administrator productivity. Cisco's Prime Infrastructure documentation describes its unified management approach and workflow-oriented capabilities; see the Cisco Prime Infrastructure product page and the Cisco Prime Infrastructure User Guide.

QUESTION NO: 7

Which of the following features protects against ARP spoofing by validating ARP packets against the DHCP snooping binding database?

A. Port security

B. Dynamic ARP Inspection

C. IP Source Guard

D. BPDU Guard

ANSWER: B

Explanation:

Dynamic ARP Inspection is correct. Dynamic ARP Inspection, commonly abbreviated DAI, intercepts ARP packets on untrusted switch ports and verifies the sender information against trusted IP-to-MAC bindings learned by DHCP snooping. An ARP packet with an invalid association can be dropped, helping protect hosts from forged ARP replies that attempt to redirect local traffic.

DHCP snooping itself builds the trusted binding database and blocks untrusted DHCP server messages. IP Source Guard uses DHCP snooping bindings to restrict IP and MAC address use on an interface. Port security limits MAC addresses learned on a port. Cisco documents DAI operation and its dependency on DHCP snooping information in the Dynamic ARP Inspection configuration guide.