PassQueen
a.k.a dumpsqueen.com

Advanced Borderless Network Architecture Field Engineer

Cisco 700-302

Version Demo

Total Demo Questions: 7

Total Premium Questions: 70

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Identify customer business requirements	1
Topic 2, Identify Cisco Borderless Network architectures	19
Topic 3, Identify Cisco Borderless Network solutions	47
Topic 4, Design a Cisco Borderless Network solution	2
Topic 5, Implement a Cisco Borderless Network solution	1
Total	70

QUESTION NO: 1

Which building block of the BYOD solution consists of Cisco Identity Services Engine as its main technology?

A. Core infrastructure

B. Secure mobility

C. Policy management

D. Workspace management

ANSWER: C

Explanation:

Policy management is correct because Cisco Identity Services Engine is the central policy decision and enforcement-enablement platform in a Cisco BYOD architecture. It establishes identity- and context-based access policies by gathering information about users, endpoints, authentication methods, device posture, and network location. Using this information, it determines the appropriate authorization result, such as a downloadable access control list, VLAN assignment, security group tag, or restricted access level.

For BYOD specifically, Cisco Identity Services Engine provides the workflows needed to securely register and onboard personal devices, provision certificates, assess compliance posture where applicable, and apply consistent network-access policy across wired, wireless, and remote-access environments. It integrates with network access devices through standards such as RADIUS and supports integrations with identity stores and endpoint-management systems. This policy-centric role is why it is the principal technology within the policy-management building block rather than merely a transport, wireless, or endpoint workspace component. Cisco describes Identity Services Engine as a security policy management platform that enables context-aware access control: Cisco Identity Services Engine. Additional BYOD deployment and onboarding guidance is available in the Cisco Identity Services Engine support documentation.

QUESTION NO: 2

Which Cisco wireless architecture feature enables a lightweight access point to continue forwarding locally switched client traffic when its WAN connection to the wireless LAN controller is unavailable?

A. FlexConnect

B. Autonomous mode

C. Centralized local mode

D. Monitor mode

ANSWER: A

Explanation:

FlexConnect is correct because it allows access points at remote sites to operate with centralized controller management while locally switching selected WLAN client traffic at the branch. When the WAN connection to the controller is interrupted, a FlexConnect access point can continue to provide local switching for configured WLANs, subject to the authentication and survivability configuration in use.

This design is useful for branch offices because it avoids backhauling all client data traffic across the WAN during normal operation and can preserve essential local wireless connectivity during a controller reachability failure. Cisco documents FlexConnect as a wireless branch solution that supports local switching and operation during WAN outages. See the Cisco FlexConnect Deployment Guide.

QUESTION NO: 3

Which element of the Cisco Unified Wireless Network solution provides unified, built-in support of leading-edge applications that are integrated into products such as the Cisco Wireless Location Appliance, Cisco Wireless Control System, Cisco SDN, Cisco NAC Appliance, and Wi-Fi phones?

A. Network unification

B. Client devices

C. Access points

D. Mobility services

ANSWER: D

Explanation:

Mobility services is correct because it is the Cisco Unified Wireless Network architectural element intended to deliver integrated wireless applications and services beyond basic client connectivity. This layer enables capabilities such as location-aware services, centralized wireless management, network access control, and support for mobility-sensitive endpoints such as Wi-Fi phones. In the architecture, these services are designed to work with the wireless infrastructure as a unified system, so organizations can apply consistent policy, visibility, security, and operational control across the WLAN.

Cisco's wireless architecture documentation describes mobility services as the area that extends the WLAN with applications including location, security, management, and voice-related capabilities. These functions rely on shared wireless-network information and integration with controllers and access points, rather than operating as isolated client or infrastructure features. The Wireless Control System and location platforms named in the question are therefore representative examples of the management and contextual services delivered through mobility services. Cisco's overview of wireless solutions and mobility services is available at Cisco Wireless Solutions and in Cisco's Mobility Services Engine overview.

QUESTION NO: 4

What are two characteristics of Cisco Converged Access? (Choose two.)

A. Wireless access points can be terminated directly on the Cisco Catalyst Cisco Catalyst 3750 -X Series Switches.

B. Cisco Converged Access supports integrated wired and wireless functionalities.

C. Cisco Converged Access uses the Cisco Catalyst 3750 -X Series Switches as a single platform for supporting wired and wireless functionalities

D. Cisco Converged Access includes both LAN switching and wireless capabilities powered by the new Cisco Unified Access Data Plane ASIC.

E. In multicast optimization with Cisco Converged Access, the number of streams increases for the same traffic type in the network.

ANSWER: B D

Explanation:

Cisco Converged Access supports integrated wired and wireless functionalities because it unifies the wired switching and wireless access architectures at the access layer. Rather than treating wireless as a separate overlay with independently managed controllers and switches, this design applies common infrastructure, policy, visibility, and operational processes across both connection types. This integrated model helps provide a more consistent user experience and simplifies deployment and troubleshooting in enterprise campus networks.

Cisco Converged Access includes both LAN switching and wireless capabilities powered by the new Cisco Unified Access Data Plane ASIC because the converged-access Catalyst architecture was designed to perform wired switching and wireless control/data-plane functions on a common hardware platform. The Unified Access Data Plane ASIC provides the hardware foundation for forwarding and enforcing capabilities needed by the integrated access design. This architecture enabled policy and services to be applied closer to users and devices, regardless of whether they connect through an Ethernet port or Wi-Fi. Cisco describes the converged-access architecture and its unified wired/wireless operation in its Catalyst 3850 Converged Access white paper and product documentation for the Cisco Catalyst 3850 Series.

QUESTION NO: 5

Which two statements about Cisco Validated Designs are true? (Choose two.)

A. They consist of systems and solutions that are designed, tested, and documented to facilitate and improve customer deployments

B. They are prescriptive, scalable, flexible designs that are used to quickly deploy a full-service network.

C. They get the design working the first time by using validated configurations and topologies.

D. Their implementations are mainly partner-led.

E. They consist of three primary modular yet interdependent components.

ANSWER: A B

Explanation:

Cisco Validated Designs consist of integrated systems and solutions that Cisco has designed, tested, and documented. This validation provides customers with implementation guidance based on proven architectures, including tested hardware and software combinations, configurations, deployment procedures, and design guidance. The documentation is intended to make deployments more predictable and to help customers implement Cisco technologies according to established best practices.

Cisco Validated Designs are also prescriptive, scalable, and flexible designs for rapidly deploying a full-service network. “Prescriptive” means the design supplies specific, actionable implementation direction rather than only high-level architectural concepts. “Scalable” allows the design to support different deployment sizes and growth requirements, while “flexible” permits adaptation to customer requirements without abandoning the validated architectural approach. Together, these characteristics allow an organization to use a repeatable, tested foundation while selecting the modules, capacity, and features appropriate to its environment. Cisco describes its validated design portfolio and associated implementation guidance at Cisco Design Zone and in its Enterprise Validated Designs resources.

QUESTION NO: 6

Which power level is the default value for Cisco EnergyWise level for platforms such as Cisco Catalyst switches, switch stacks, and Cisco Integrated Services Routers Generation 2 routers?

A. Level 1

B. Level 10

C. Level 5

D. Level 0

ANSWER: B

Explanation:

Level 10 is the default Cisco EnergyWise power level for supported Cisco Catalyst switches, switch stacks, and Cisco Integrated Services Routers Generation 2. EnergyWise represents device and endpoint operating states with a scale from level 0 through level 10. Level 10 denotes the fully operational, highest-power state, so it is the appropriate default for network infrastructure that must be available to forward traffic and provide normal services immediately after startup. A device at this level is not being placed into an energy-saving reduced-function or shutdown state by the EnergyWise policy.

This default also provides a predictable baseline for administrators: power-management policies can subsequently lower an endpoint or device power level according to operational schedules, organizational energy objectives, and hardware capabilities, while level 10 remains the normal full-service state. Cisco’s EnergyWise documentation describes the power-level model and identifies level 10 as the default level used by EnergyWise-enabled devices. See the Cisco IOS EnergyWise Overview and Cisco’s EnergyWise technology overview for the operating-state and energy-management concepts.

QUESTION NO: 7

Which two statements about Cisco Cloud Web Security are true? (Choose two.)

A. It is powered by Cisco Security Intelligence Operations, a cloud-based service.

B. It extends web security to users on the go with the Cisco AnyConnect Secure Mobility Client.

C. It provides unmatched cloud-based web security and control only to very small-sized organizations.

D. It can only be integrated with Cisco switches.

ANSWER: A B

Explanation:

Cisco Cloud Web Security was a cloud-delivered web-security service that used Cisco Security Intelligence Operations (SIO) as its threat-intelligence foundation. SIO provided globally collected security telemetry and intelligence to help identify web-based threats, including malware and malicious destinations, so policy enforcement could be informed by current threat data rather than relying solely on static local controls. Cisco described this intelligence capability as a key component of its cloud web-security architecture.

It also extended web-security protection to roaming users through the Cisco AnyConnect Secure Mobility Client. When a user was away from the corporate network, AnyConnect could direct applicable web traffic to the Cloud Web Security service, allowing the organization's web-use and security policies to continue being enforced without requiring the user to be connected through an on-premises web-security appliance. This capability supported consistent protection for mobile users while retaining centralized visibility and policy control. Cisco's Cloud Web Security documentation describes the AnyConnect integration and the cloud service's use of Cisco security intelligence.

References: Cisco Cloud Web Security product information and Cisco AnyConnect Secure Mobility Client.