

Cisco Express Foundation for Account Managers (CXFA) Exam

Cisco 646-365

Version Demo

Total Demo Questions: 10

Total Premium Questions: 105

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

QUESTION NO: 1

Which two Cisco products can demonstrate the "one policy" approach in the Cisco Unified Access solution? (Choose two.)

- A. Cisco Mobility Services Engine
- B. Catalyst 6500 Series Switch
- C. Cisco ISE
- D. Cisco WLC
- E. Cisco AnyConnect

ANSWER: C E

Explanation:

Cisco ISE and Cisco AnyConnect demonstrate the "one policy" approach by extending identity-based access control beyond a single access method. Cisco ISE is the central policy decision and administration platform: it uses user and device identity, device posture, location, and other contextual information to define and apply access policy consistently. In a Unified Access design, this lets the organization establish policy centrally rather than create disconnected policy sets for separate connection types.

Cisco AnyConnect complements ISE by connecting endpoint authentication, posture assessment, and secure remote access to those centrally administered policies. The client can provide endpoint context and support posture validation through Cisco ISE, allowing the same identity- and context-aware policy model to follow users whether they connect through enterprise access services or remotely. Together, these products illustrate how access decisions can be based on a common policy framework while adapting enforcement to the user, device, and connection context. Cisco describes ISE as a platform for secure network access and policy enforcement in its [Identity Services Engine overview](#). Cisco documents the endpoint and secure-access capabilities of the client in its [Cisco Secure Client \(formerly AnyConnect\) overview](#).

QUESTION NO: 2

Which three of these vendors are the strongest competitors to Cisco in the switching market? (Choose three.)

- A. Extreme Networks
- B. IBM
- C. Juniper
- D. Riverbed Technology
- E. HP
- F. Brocade

ANSWER: C E F

Explanation:

In the historical market context of this Cisco Express Foundation for Account Managers question, **Juniper**, **HP**, and **Brocade** were major competitive suppliers in enterprise and data-center switching. Juniper competed with Cisco through its Ethernet switching portfolio and the broader Junos-based networking platform, particularly in campus, data-center, and high-performance network environments. HP was a substantial enterprise switching competitor, with a broad installed base and a portfolio aimed at campus access, aggregation, and core switching deployments. Brocade was also a significant switching vendor, especially in data-center networking and storage-related environments, where its Ethernet and Fibre Channel

capabilities created competitive overlap with Cisco offerings. These companies had the product portfolios, channel presence, and customer reach necessary to be considered prominent competitive alternatives in the switching market during the period reflected by the exam. Cisco's investor disclosures describe networking as a highly competitive market, while its annual-report archive provides the relevant historical business context: [Cisco annual reports and proxy information](#). Juniper's switching portfolio and positioning are also documented at [Juniper Networks switches](#).

QUESTION NO: 3

Which statement is true about Cisco Meraki cloud management?

- A. It centrally manages supported Meraki devices through a cloud-based dashboard.
- B. It requires a separate on-premises controller at every branch site.
- C. It supports only wireless access points and no other network devices.
- D. It removes the need to define network security policies.

ANSWER: A

Explanation:

Cisco Meraki cloud management provides centralized visibility and configuration management for supported Meraki networking devices through a web-based dashboard. This approach can simplify deployment and day-to-day operations for organizations that manage distributed sites, wireless networks, switches, security appliances, and other supported infrastructure.

Cloud management does not eliminate the need for local network design, security policy, or reliable connectivity planning. Instead, it provides a centralized operational model for applying configuration, monitoring network health, and troubleshooting across sites. Cisco describes the management model and portfolio capabilities at [Cisco Meraki Dashboard](#).

QUESTION NO: 4

Which two are advantages of Cisco Prime LAN Management Solutions? (Choose two.)

- A. It is bundled with any Cisco ISR G2 or Cisco ASR purchase.
- B. It includes Cisco Borderless Networks service work centers.
- C. It includes Cisco WAAS licenses.
- D. It includes WAN optimization features.
- E. It provides complete life-cycle management.

ANSWER: B E

Explanation:

Cisco Prime LAN Management Solutions provides centralized, end-to-end life-cycle management for campus LAN infrastructure. Its life-cycle capabilities cover the operational stages needed to manage network devices effectively, including discovery, inventory, configuration management, software-image management, fault monitoring, reporting, and compliance-oriented operational tasks. This centralized approach helps IT teams standardize administration and reduce the effort required to maintain a reliable campus network.

The solution also includes service work centers aligned to Cisco Borderless Networks use cases. These work centers organize management workflows around common operational services, giving administrators targeted visibility and tools for areas such as wireless, access control, energy management, and troubleshooting. Rather than requiring separate point-management tools for each task, Prime LAN Management Solutions brings relevant campus-management functions into an integrated platform.

Together, Cisco Borderless Networks service work centers and complete life-cycle management describe the product's core value: simplifying the deployment, operation, monitoring, and optimization of Cisco campus LAN environments. Cisco's product information describes Prime LAN Management Solutions as a campus-management offering with lifecycle and service-oriented capabilities. See the [Cisco Prime LAN Management Solution overview](#) and the [Cisco Prime LMS data sheet](#).

QUESTION NO: 5

Which statement correctly describes the purpose of network segmentation?

- A. It increases the number of broadcast domains without applying access policy.
- B. It separates resources into controlled groups and restricts access according to policy.
- C. It encrypts all application traffic automatically, regardless of protocol.
- D. It removes the need for endpoint-security controls.

ANSWER: B

Explanation:

Network segmentation separates users, devices, and workloads into controlled groups so that access can be limited according to business and security policy. It reduces unnecessary connectivity between resources and helps contain the impact of a compromised endpoint or application.

Segmentation is particularly important when an organization supports employee devices, guest access, operational technology, and business-critical applications on shared infrastructure. Cisco TrustSec can support segmentation by using Security Group Tags and policy-based controls that are associated with identity and role rather than only with IP address or physical location. Cisco provides an overview of this approach at [Cisco TrustSec](#).

QUESTION NO: 6

Which statement best describes the value of Cisco SMARTnet Service to a customer?

- A. It provides a permanent license for all Cisco software applications.
- B. It provides technical support, software maintenance, and hardware replacement options.
- C. It replaces the need for a customer network operations team.
- D. It provides managed WAN connectivity from a Cisco service provider.

ANSWER: B

Explanation:

Cisco SMARTnet Service provides customers with access to Cisco technical support, software updates, and hardware replacement options for eligible products. This helps customers maintain network availability and reduce operational risk throughout the lifecycle of the installed infrastructure.

For an account manager, SMARTnet should be positioned as more than a warranty extension. It gives IT staff access to Cisco Technical Assistance Center expertise and software maintenance, which can help resolve issues more quickly and keep the environment current. The appropriate service level depends on the customer's availability requirements, installed base, locations, and internal support capabilities. Cisco describes the available support capabilities in its [Cisco Smart Net Total Care service overview](#).

QUESTION NO: 7

Which three services can be provided by Cisco ISR G2 access routers? (Choose three.)?

- A. IP telephony
- B. integrated video services
- C. firewalling
- D. NX-OS-based services
- E. video control unit services
- F. Cisco WAAS engine

ANSWER: A B C

Explanation:

Cisco Integrated Services Routers Generation 2 were designed as branch-office platforms that consolidate routing with collaboration, video, and security capabilities. **IP telephony** is a core ISR G2 service: the routers can provide integrated voice-gateway functions and support Cisco Unified Communications deployments, allowing branch sites to connect IP phones and voice services through a single platform. **Integrated video services** are also supported through the ISR G2 services architecture, which was built to enable rich-media collaboration and video delivery at branch locations alongside WAN connectivity. **Firewalling** is a key integrated-security capability. ISR G2 routers can apply Cisco IOS security features, including stateful firewall services and policy enforcement, to protect traffic at the WAN and branch edge. These capabilities illustrate the ISR G2 value proposition of delivering multiple essential branch services from one modular router rather than requiring separate dedicated appliances. Cisco's ISR G2 data sheet describes the platform's integrated voice, video, application, and security services, while Cisco's branch-router materials further describe its role in converged branch deployments. See the [Cisco ISR G2 data sheet](#) and [Cisco Integrated Services Routers overview](#).

QUESTION NO: 8

Which two statements best describe the challenges that customers have to face when providing services in a borderless world? (Choose two.)

- A. How do you control energy consumption of devices that are owned by employees?
- B. How can you support video in the whole network?
- C. How can you integrate cloud services seamlessly in your network?
- D. Which type of firewall should you deploy?

ANSWER: B C

Explanation:

"How can you support video in the whole network?" is correct because a borderless organization must deliver consistent, high-quality access to rich collaboration applications for users regardless of location, device, or access method. Video places substantial demands on bandwidth, latency, jitter, wireless capacity, and quality-of-service policy. Supporting it throughout the network therefore requires an end-to-end architecture rather than isolated upgrades in one part of the infrastructure. Cisco identifies collaboration and video as key network services whose user experience depends on the network being able to intelligently prioritize and transport application traffic.

"How can you integrate cloud services seamlessly in your network?" is also correct because borderless networks extend connectivity beyond the traditional campus to hosted applications, public and private cloud resources, remote users, and distributed endpoints. Customers need secure, reliable, policy-consistent access to those services while maintaining visibility and an acceptable application experience. This integration is a core architectural challenge as workloads and services become distributed across on-premises and cloud environments. Cisco's borderless-network approach emphasizes secure access to applications and services from anywhere, while its cloud networking guidance addresses connecting users and sites to distributed cloud resources. See [Cisco Borderless Networks](#) and [Cisco Cloud Networking](#).

QUESTION NO: 9

Which statement best describes the value of a Cisco architectural approach for a customer?

- A. It requires customers to replace all network equipment at the same time.
- B. It combines technologies and services to address a customer business objective.
- C. It is limited to selecting the lowest-cost network devices.
- D. It eliminates the need for network design and operational planning.

ANSWER: B

Explanation:

A Cisco architectural approach connects individual products, services, and policies into an integrated solution that supports a customer business objective. Rather than evaluating routing, switching, security, collaboration, and management as unrelated purchases, the customer can consider how these capabilities work together to provide a consistent user experience, improve operational efficiency, and reduce risk.

This approach helps account managers relate technology investments to customer outcomes and lifecycle requirements. Cisco describes its architecture-based networking approach in its [Enterprise Networks](#) resources.

QUESTION NO: 10

What is the primary security requirement related to social media and collaboration?

- A. protection of network edges
- B. securing cloud transition
- C. enabling BYOD transformation
- D. authorizing content use

ANSWER: D

Explanation:

Authorizing content use is the primary security requirement for social media and collaboration because these tools are fundamentally designed to create, share, repost, store, and discuss information across users, teams, customers, and external communities. The security control must therefore determine who is permitted to access particular content, what they may do with it, and under which circumstances. Effective authorization applies identity- and role-based permissions to actions such as viewing, uploading, editing, sharing, downloading, and publishing content. It can also support policy enforcement for sensitive information, helping organizations preserve confidentiality while allowing the collaboration that business users need. Cisco describes secure collaboration as protecting users, data, applications, and devices, with identity and access controls providing an essential basis for secure use. In a social-media context, content authorization similarly limits unintended disclosure and establishes accountable, policy-governed sharing rather than merely controlling network connectivity. Cisco's collaboration-security resources provide further context at [Cisco Collaboration Security](#), and Cisco's guidance on identity-based access protection is available at [Cisco Zero Trust](#).