DUMPSARENA

TelePresence Video Sales Engineer for Express

Cisco 650-293

Version Demo

Total Demo Questions: 6

Total Premium Questions: 60

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Cisco TelePresence Video Portfolio and Market	2
Topic 2, Cisco TelePresence Video Architecture	20
Topic 3, Cisco TelePresence Video Endpoints	11
Topic 4, Cisco TelePresence Video Infrastructure	15
Topic 5, Cisco TelePresence Video Management	9
Topic 6, Cisco TelePresence Video Services	2
Topic 7, Mix Questions	1
Total	60

QUESTION NO: 1

In a firewall traversal solution, where should the Cisco TelePresence VCS control be located?

A. within the network of a customer

B. internal to your network

C. within a DMZ

D. outside the firewall

ANSWER: B

Explanation:

internal to your network is correct. In Cisco's firewall-traversal architecture, the VCS Control, now generally referred to as Expressway-C, is the trusted internal call-control component. It is deployed on the organization's private network, where it can communicate with internal video endpoints and integrate with internal collaboration services such as Cisco Unified Communications Manager. This placement keeps internal signaling, endpoint registration, and directory-related communications inside the protected enterprise environment.

The paired VCS Expressway/Expressway-E is the component designed for the edge deployment and communicates across the firewall boundary with the internal control system. The control component and edge component establish a secure traversal relationship, allowing remote users and external systems to connect without exposing the internal call-control infrastructure directly to untrusted networks. Cisco deployment guidance describes Expressway-C as residing on the internal network and Expressway-E as the externally facing traversal peer. This separation is a core security and design principle for business-to-business and mobile remote-access video calling.

See Cisco's Expressway Basic Configuration Deployment Guide and Expressway installation and configuration guides.

QUESTION NO: 2

Which three network conditions can negatively affect the quality of a Cisco TelePresence video call? (Choose three.)

A. packet loss

B. delay

C. jitter

D. directory synchronization

E. DNS aliases

F. phone book replication

ANSWER: A B C

Explanation:

Packet loss, **delay**, and **jitter** can all impair real-time video communication. Packet loss can cause visible artifacts, frozen video, and degraded audio. Excessive one-way delay makes conversation unnatural because participants talk over one another. Jitter is variation in packet arrival time and can result in uneven playback when it exceeds the endpoint jitter buffer capability.

TelePresence traffic should therefore be assessed for available bandwidth, packet loss, latency, and jitter, and it should receive appropriate QoS treatment across constrained network links. RTP provides sequence numbers and timestamps that help endpoints process real-time media, but it cannot fully eliminate the effect of severe network impairment. See RFC 3550.

QUESTION NO: 3

Which three scenarios represent a multipoint Cisco TelePresence setup? (Choose three)

A. two video participants and an audio participant, all at different sites

B. three audio participants and three video participants

C. two participants who are communicating over the WAN

D. two participants who are conversing over an IP phone connection

E. two video participants

F. three audio participants, all at different sites

G. one participant who is sharing his desktop and other documents with a remote participant

ANSWER: A B F

Explanation:

A multipoint Cisco TelePresence conference involves three or more participating endpoints or participants in a single conference. The participants do not all need to use video: a Cisco conferencing bridge can join video-capable TelePresence endpoints and audio-only participants in the same multipoint call. Therefore, *two video participants and an audio participant, all at different sites* is a multipoint scenario because it contains three participants and combines supported media types. *three audio participants and three video participants* is also multipoint because six participants are joined in one conference, well beyond the minimum of three. Likewise, *three audio participants, all at different sites* represents multipoint conferencing because three distinct participants are connected in a common call, even though no video endpoint is specified. Cisco documents that its conferencing resources support multipoint calls and can accommodate both video and audio endpoints, while Cisco's TelePresence terminology distinguishes point-to-point calls from conferences involving multiple participants. See Cisco's TelePresence Server configuration documentation and the Cisco conferencing product overview.

QUESTION NO: 4

A customer needs a single dialable address that can ring the user's office TelePresence system and Cisco TelePresence Movi client at the same time. Which VCS feature should you recommend?

A. FindMe

B. Multiway

C. continuous presence

D. bandwidth management

ANSWER: A

Explanation:

FindMe is correct because it associates one user identity with multiple configured locations. A caller dials the user's FindMe address, and Cisco VCS routes the call to the selected locations according to the configured policy. The locations can be called simultaneously or in sequence.

This allows a user to remain reachable through more than one endpoint without requiring callers to know the individual URI of each device. FindMe is a VCS call-routing feature rather than a conference, recording, or bandwidth-management feature. See the Cisco VCS Configuration Guide.

QUESTION NO: 5

A Cisco Expressway-E is deployed behind a firewall using network address translation. Which NAT method is normally required to ensure that external systems can reliably reach the Expressway-E?

A. Static NAT

B. Dynamic NAT

C. Port address translation only

D. DNS forwarding

ANSWER: A

Explanation:

Static NAT is correct because an externally reachable Expressway-E requires a stable, consistent mapping between its private address and public address. The public address can then be configured in the Expressway-E and published in DNS for external callers.

Dynamic NAT can assign changing public addresses and is not appropriate for an externally advertised collaboration service. Port address translation is commonly used for outbound client traffic, but it does not provide the predictable one-to-one public addressing normally required for an Expressway-E deployment. Cisco deployment guidance describes the required NAT considerations for Expressway edge deployments. See the Cisco Expressway Basic Configuration Deployment Guide.

QUESTION NO: 6

Assume that you have a firewall that is configured on your network that allows data from inside to go out. Under which two circumstances will a packet from the outside get passed to a device on the inside? (Choose two.)

A. The data is encrypted.

B. The packet is a reply to a request that is sent by internal device to the external device.

C. The firewall is not configured to function across the LAN.

D. Your firewall traversal client is improperly configured.

E. A firewall rule specifies that packets on the destination port should be passed to the device.

F. The sending device has the correct password that can be verified by the receiving device.

ANSWER: B E

Explanation:

A packet from an external network can be passed to an internal device when it is a reply to a request that is sent by internal device to the external device. Stateful firewalls track outbound sessions in a connection table and permit the corresponding return traffic when it matches the state, protocol, addresses, and ports of an established session. This behavior lets internal endpoints initiate calls, registrations, HTTPS requests, and other outbound communications without requiring a broadly open inbound rule.

A packet can also reach an internal device when a firewall rule specifies that packets on the destination port should be passed to the device. This is an explicitly permitted inbound service, commonly implemented through an access-control rule together with static NAT or port forwarding when the internal device uses a private address. For video deployments, such rules may be used only for required signaling or media services, with the permitted protocols, destination addresses, and ports restricted to the documented design. Cisco describes the role of stateful inspection and connection state in its firewall overview, and its Expressway deployment guidance discusses firewall traversal and externally reachable services in the Cisco Expressway configuration guides.