Implementing Cisco Video Network Devices v1.0

Cisco 210-065 Dumps Available Here at:

https://www.certification-questions.com/cisco-exam/210-065-dumps.html

Enrolling now you will get access to 172 questions in a unique set of 210-065 dumps

Question 1

Which of the following commands or command sets should you issue to configure a Cisco TelePresence System 1000 with IP address 192.168.1.43, subnet mask 255.255.255.0, and default gateway 192.168.1.1?

Options:

A. static 192.168.1.43 255.255.255.0 192.168.1.1

B. ip address 192.168.1.43 255.255.255.0 192.168.1.1

C. set network ip static 192.168.1.43 255.255.255.0 192.168.1.1

D. xConfiguration Network 1 IPv4 Address: "192.168.1.43"

xConfiguration Network 1 IPv4 SubnetMask: "255.255.255.0"
xConfiguration Network 1 IPv4 Gateway: "192.168.1.1"

E. ip address 192.168.1.43 255.255.255.0

ip defaultgateway 192.168.1.1

Answer: C

Explanation:
Section: Troubleshooting and Support Explanation
You should issue the set network ip static 192.168.1.43 255.255.255.0 192.168.1.1 command. The syntax of the set network ip static command is set network ip static ip-address subnet-mask default-gateway [dnsaddress1] [dnsaddress2] [domain]. After you configure the static IP address, the Cisco TelePresence System (CTS) 1000 will automatically restart.
You can also configure a static IP address on a CTS 1000 by using the web interface. To configure a static IP address by using the web interface, navigate to Configuration > IP Settings, change DHCP Enabled to No, and configure the IP address, subnet mask, and default gateway fields.
You should not issue the static 192.168.1.43 255.255.255.0 192.168.1.1 command. The static command configures a static IP address for a port on the Cisco TelePresence multipoint control unit (MCU) 5300.

The syntax of the static command is static port ip-address subnet-mask [default-gateway], where port is A for Port A or B for Port B.
You should not issue the ip address 192.168.1.43 255.255.255.0 192.168.1.1command. The ip address command is not valid on a CTS 1000.
You should not issue the following command set:
xConfiguration Network 1 IPv4 Address: "192.168.1.43"
xConfiguration Network 1 IPv4 SubnetMask: "255.255.255.0"
xConfiguration Network 1 IPv4 Gateway: "192.168.1.1"
You would issue these commands to configure a static IP address on a CTS Codec, such as the C40 or C60.
You should not issue the following command set:
ip address 192.168.1.43 255.255.255.0
ip defaultgateway 192.168.1.1
This command set is similar to the IP address configuration of a Cisco router or switch. However, these commands are not valid on a CTS 1000.
Reference:
Cisco: Configuring the Cisco TelePresence System: Configuring a Static IP Address for Networks That Do Not Use DHCP

Question 2

Which of the following will not be affected when you issue the xCommand SystemUnit FactoryReset Confirm: Yes command on a Cisco TelePresence EX, MX, SX, or C-series system? (Choose two.)

Options:

A. call logs

B. certificates

C. custom backgrounds

D. local phonebook

E. option keys

F. release keys

G. ring tones

H. system parameters

Answer: E, F

Explanation:
Section: Troubleshooting and Support Explanation
Release keys and option keys will not be affected when you issue the xCommand SystemUnit

FactoryReset Confirm: Yes command on a Cisco TelePresence EX, MX, SX, or C-series system. The xCommand SystemUnit FactoryReset Confirm: Yes command is used to perform a factory reset on a system. You might want to perform a factory reset if there is a severe problem with the video system. If possible, you should back up log files and the current configuration before proceeding with a factory reset. The following items are deleted when you perform a factory reset:
- Call logs
- Custom backgrounds
- Ring tones
- Certificates
- Local phonebook
- In addition, all system parameters are set to their default values.

Reference:
Cisco: Troubleshooting Guide TC6.0: Factory reset using SSH, Telnet and serial connection(PDF)
Cisco: Cisco TelePresence System Codec C40/C60 and Profiles using C40/C60, Administrator guide: Factory resetting the codec (PDF)

Question 3

During a call, you discover that you are unable to control the remote camera from your Cisco TelePresence SX20 Quick Set endpoint.
Which of the following reasons might cause this behavior to occur? (Choose two.)

Options:

A. The call is encrypted.

B. The remote camera does not have PTZ functionality.

C. The Conference FarEndControl Mode setting on your system is set to Off.

D. The Conference FarEndControl Mode setting on the remote system is set to Off.

E. Remote cameras cannot be controlled from an SX20 endpoint.

Answer: B, D

Explanation:
Section: Endpoint Configuration Explanation
You will be unable to control the remote camera from your Cisco TelePresence SX20 Quick Set endpoint if the Conference FarEndControl Mode setting on the remote system is set to Off or if the remote camera does not have pan-tilt-zoom (PTZ) functionality. If the Conference FarEndControl Mode setting on your system is set to Off, remote participants will be unable to control your camera.
Encryption does not prevent control of remote cameras. However, encryption does affect the remote snapshot feature? snapshots are disabled on encrypted calls.
You can also change the local or remote layout from a Cisco SX20. The following video layout options are available:

- Auto
- Equal
- Overlay
- Prominent
- Single

The Auto layout option uses the default layout family. The Equal layout option displays all participants in pictures of the same size as long as there is enough space on the screen to display them. The Overlay layout option displays the active speaker or presentation in a full screen and displays the other participants in small pictures-in-picture (PiP). The Prominent layout option displays the active speaker or presentation in a large picture and displays the other participants in small pictures. The Single layout option displays only the active speaker or presentation? the other participants are not displayed.

Reference:

Cisco: Administrator guide for Cisco TelePresence SX20 Quick Set: Controlling the far end camera (PDF)

Question 4

You issue the xStatus Camera command on a Cisco SX20 and receive the following output:

```
xStatus Camera
*s Camera 1 Connected: True
*s Camera 1 HardwareID: "53000000"
*s Camera 1 Manufacturer: "Cisco"
*s Camera 1 Model: "PrecisionHD 1080p 4X S2"
*s Camera 1 SoftwareID: "S01777-2.0 FINAL [ID:20010] 2012-12-07"
*s Camera 1 SerialNumber: "MDA8675309J"
*s Camera 1 IpAddress: ""
*s Camera 1 MacAddress: ""
*s Camera 1 Position Pan: 334
*s Camera 1 Position Tilt: 729
*s Camera 1 Position Zoom: 201
*s Camera 1 Position Focus: 135
*s Camera 1 Capabilities Options: "ptzf"
*s Camera 1 Flip: "On"
*s Camera 1 UpgradeStatus: None
*s Camera 1 DownloadProgress: 0
```

Which of the following statements is true?

Options:

A. The SX20 has the best possible camera installed.

B. The camera is pointed up.

C. The camera is pointed to the left.

D. The image can be flipped horizontally.

E. The camera is configured to auto focus.

Answer: B

Explanation:
Section: Troubleshooting and Support Explanation
The camera is pointed upward. The Position Tilt value indicates whether the camera is pointed upward or downward. If the value is negative, the camera is tilted downward; if the value is positive, the camera is tilted upward.
The xStatus Camera command can be used to display status information about a camera. The same information can be obtained from the web interface by navigating to Configuration > System Status > Camera.
The Position Pan value indicates whether the camera is pointed to the left or to the right. If the value is negative, the camera is pointed to the left; if the value is positive, the camera is pointed to the right. In this scenario, the value is 334, so the camera is pointed to the right.
The Flip value indicates whether the camera can be flipped vertically, not horizontally. You can configure the Flip value to a value of Auto, On, or Off. If the value is set to Auto, the camera image will flip vertically if the camera is upside down.
The xStatus Camera output does not indicate whether a camera is configured to auto focus. However, you can configure a camera to auto focus by issuing the xConfiguration Cameras Camera 1 Focus Mode: Auto command.
The SX20 in this scenario does not have the best possible camera installed. The SX20 can be configured with a 2.5x, 4x, or 12x camera. The model number indicates what kind of camera is installed. In this scenario, the SX20 is configured with a 4x zoom camera.
Reference:
Cisco: Application Programmer Interface (API) Reference Guide, Cisco TelePresence SX20 Codec: Camera status (PDF)
Cisco: Cisco TelePresence SX20 Quick Set Data Sheet

Question 5

Which of the following endpoints can communicate by using Cisco TelePresence VCS?

Options:

A. only SIP endpoints

B. only H.323 endpoints

C. both SIP and H.323 endpoints

D. neither SIP nor H.323 endpoints

Answer: C

Explanation:
Section: Video Concepts Explanation
Both Session Initiation Protocol (SIP) and H.323 endpoints can communicate by using Cisco TelePresence Video Communication Server (VCS). Third-party standards-based SIP and H.323 systems can also be integrated into the TelePresence environment.
In order to configure Cisco TelePresence VCS so that it can perform call control between SIP and H.323 endpoints, you must first create a transform that checks whether the called address contains the @ sign. If it does not, an @ and the SIP domain name are appended to the called address, thereby standardizing SIP and H.323 addresses.
After you create a transform to route calls, you must create two search rules. The first search rule removes the SIP domain portion of the address and searches for a corresponding H.323registered device. The second rule, which is used if no H.323 device is located, uses the full address to search for a corresponding SIP-registered device.
Reference:
Cisco: H.323 Video Internetworking Using VCS Technology Design Guide (PDF)

Question 6

For which of the following reasons is a red oval most likely to appear next to a contact in Cisco Jabber? (Choose two.)

Options:

A. The user is on a call.

B. The user has missed a call.

C. The user is sharing content.

D. The user has been idle for a while.

E. The user does not want to be disturbed.

F. The user is attending a WebEx meeting.

G. The user is in a scheduled Outlook meeting.

H. The user is experiencing registration problems.

Answer: C, E

Explanation:
Section: Conferencing Concepts Explanation
A red oval is most likely to appear next to a contact in Cisco Jabber if the user is sharing content or does not want to be disturbed. If grayscale is used, the icon will appear as a gray oval with a diagonal slash.
The oval next to a contact indicates the contact's presence status. The presence status is used to indicate to other users whether someone is available.

A yellow oval next to a contact in Cisco Jabber indicates a user who has been idle for an extended period of time, on a call, in a WebEx meeting, or in a scheduled Outlook meeting. If grayscale is used, the icon will appear as a gray oval with a horizontal line.
A green oval next to a contact in Cisco Jabber indicates a user who is available. If grayscale is used, the icon will appear as a gray oval with a check mark.
A gray oval next to a contact in Cisco Jabber indicates a user who is offline. If grayscale is used, the icon will still appear as a solid gray oval.
A user who is experiencing registration problems might appear on other users' screens next to a gray oval. The user who is experiencing registration problems might have a red X on that user's phone controls icon in Cisco Jabber. This often occurs because the user is not signed in, the user name or password is incorrect, or the directory number (DN) is not properly associated with the user's account in Cisco Unified Client Services Framework.
A user who has missed calls will not cause the user's presence status to change. That user will likely see a red circle next to a phone on Cisco Jabber. The number that appears within the red circle indicates the number of missed calls. A red circle with a number might also appear next to an envelope, which indicates the number of new voice mail messages.
Reference:
Cisco: Frequently Asked Questions: Cisco Jabber for Mac Release 9.2(1) (WebEx Connect): Presence Status
Cisco: Cisco Jabber for Windows 10.6 User Guide: Grayscale Status Icons

Question 7

Which of the following statements is correct regarding H.323 registrations on a Cisco VCS that is configured with the default settings?

Options:

A. H.323 endpoints cannot register to a Cisco VCS by default.

B. H.323 endpoints must register manually by connecting to the IPv4 address of the Cisco VCS.

C. H.323 endpoints must register automatically by sending out a Gatekeeper Discovery Request.

D. H.323 endpoints can register manually by connecting to the IPv4 address of the Cisco VCS or automatically by sending out a Gatekeeper Discovery Request.

Answer: D

Explanation:
Section: Troubleshooting and Support Explanation
By default, H.323 endpoints can register manually by connecting to the IPv4 address of the Cisco TelePresence Video Communication Server (VCS) or automatically by sending out a Gatekeeper Discovery Request. Cisco VCS is configured by default to be an H.323 gatekeeper. In order for a Cisco VCS to be an H.323 gatekeeper, the H.323 mode must be enabled. To enable H.323 mode, navigate to Configuration > Protocols > H.323 and set the H.323 mode option to On.

Manual registrations require that the H.323 endpoint be configured with the IPv4 address of the Cisco VCS and be configured with an IPv4 address, subnet mask, and default gateway that will allow the endpoint to communicate with the Cisco VCS. H.323 endpoints can register manually as long as the VCS is configured to be an H.323 gatekeeper.
Automatic registrations require that the VCS be configured to allow automatic discovery. To enable automatic discovery, navigate to Configuration > Protocols > H.323 and set the Auto discovery option to On. Automatic discovery is enabled on Cisco VCS by default.
When an H.323 endpoint registers with Cisco VCS, the endpoint sends one or more of the following aliases to the VCS:
- One or more H.323 IDs
- One or more E.164 aliases
- One or more Uniform Resource Identifiers (URIs)
If an endpoint attempts to register an alias that has previously been registered from another IP address, the VCS will reject the registration by default. You can configure Cisco VCS to overwrite the original registration by navigating to Configuration > Protocols > H.323 and setting the Registration conflict mode option to Overwrite.
Reference:
Cisco: Cisco TelePresence Video Communication Server, Administrator Guide, Software version: X8.1: Registering aliases (PDF)
Cisco: Cisco TelePresence Video Communication Server, Administrator Guide, Software version: X8.1: About H.323 (PDF)
Cisco: Cisco TelePresence Video Communication Server, Administrator Guide, Software version: X8.1: Configuring H.323 (PDF)

Question 8

Which of the following devices are used for call control? (Choose two.)

Options:

A. CTRS

B. Cisco TMS

C. Cisco Unified CM

D. Cisco TelePresence VCS

E. Cisco TelePresence Server

F. Cisco TelePresence Manager

G. Cisco TelePresence Content Server

Answer: C, D

Explanation:

Section: Video Concepts Explanation
Cisco Unified Communications Manager (CM) and Cisco TelePresence Video Communication Server (VCS) are used for call control. Call control devices perform endpoint registration, call routing, call maintenance, and call monitoring. Cisco Unified CM supports Session Initiation Protocol (SIP), whereas Cisco VCS supports H.323 and SIP.
Cisco TelePresence Content Server (TCS) and Cisco TelePresence Recording Server (CTRS) are not used for call control. Cisco TCS is an appliance or blade that provides live recording, streaming, and playback of video content for any TelePresence or Unified CM endpoint. CTRS is a server that provides recording and playback of video content for certain endpoints.
Cisco TelePresence Server is not used for call control; it is used as a conferencing device. Cisco conferencing devices support either switching or transcoding. Switching simply forwards the audio and video to endpoints, whereas transcoding encodes and decodes the media streams. Cisco TelePresence Multipoint Switch supports switching; Cisco TelePresence Server, Cisco TelePresence multipoint control unit (MCU) 4000, Cisco TelePresence MSE 8000, and Cisco Integrated Services Router (ISR) G2 support transcoding.
Cisco TelePresence Manager is not used for call control; it is used as a management device. Management devices are typically responsible for scheduling, monitoring, and provisioning. Cisco TelePresence Manager is a server-based platform, whereas Cisco TelePresence Management Suite (TMS) can be delivered as a server-based software application or as an appliance. Both Cisco TMS and Cisco TelePresence Manager can interface with Microsoft Exchange. However, Cisco TMS also has a built-in web-scheduling interface; Cisco TelePresence Manager does not.
Reference:
Cisco: Video Infrastructure Components

Question 9

Which of the following MCU logs cannot be downloaded to an XML file by using the web interface on a Cisco TelePresence MCU?

Options:

A. the audit log

B. the event log

C. the call detail records

D. the H.323/SIP log

Answer: B

Explanation:
Section: Troubleshooting and Support Explanation
The event log cannot be downloaded to an Extended Markup Language (XML) file by using the web interface on a Cisco TelePresence multipoint control unit (MCU). However, the event log can be downloaded as text or can be sent to syslog servers. Errors, warnings, and other informational messages

are found in the event log. The last 2,000 event log messages can be displayed by navigating to Logs > Event log.
The audit log can be downloaded to an XML file by using the web interface on a Cisco TelePresence MCU. Configuration changes are found in the audit log. A Cisco TelePresence MCU stores the last 100,000 audit messages internally or on compact flash if it is available. However, only 2,000 messages are displayed by using the web interface.
The call detail records can be downloaded to an XML file by using the web interface on a Cisco TelePresence MCU. Call detail records can be used for billing and reporting purposes.
The H.323/SIP log can be downloaded to an XML file by using the web interface on a Cisco TelePresence MCU. H.323 messages and Session Initiation Protocol (SIP) messages are found in the H.323/SIP log. Only 10 pages of logged messages can be stored in the H.323/SIP log. By default, the H.323/SIP log is disabled.
Reference:
Cisco: Cisco TelePresence MCU Series, Administrator Guide: Advanced topics (PDF)

Question 10

A Cisco TelePresence Multipoint Switch is configured for room switching.
Which of the following will most likely happen when someone who is in another room and who is not currently displayed onscreen becomes the active speaker during a multipoint meeting?

Options:

A. All of the screens will change to display the active speaker.

B. All of the screens will change to display the active speaker's room.

C. The active speaker will be displayed on the center screen.

D. The active speaker will be displayed on the screen that corresponds to the speaker's room.

E. The screens will not change.

Answer: B

Explanation:
Section: Conferencing Concepts Explanation
All of the screens will change to display the active speaker's room. The Cisco TelePresence Multipoint Switch can be configured for one of two switching modes: room switching or speaker switching. The switching mode indicates what should be displayed on participants' screens when the active speaker changes. The active speaker is the person who is the loudest speaker for two seconds.
With room switching, the active speaker's room is displayed on all three screens in all other rooms. When the active speaker changes to someone in a different room, all of the screens in other rooms will display the new active speaker's room.
With speaker switching, each screen in a room can change independently of the other screens. The screens can display different table segments in the same room or in different rooms. When the active

speaker changes, the active speaker's table segment will be displayed on one of the screens in all rooms. The active speaker might not be displayed on the center screen. The active speaker will be displayed on the center screen only if the speaker is sitting in front of the center camera. If someone who is in another room and is not displayed onscreen becomes the active speaker, the screens will change to show that person or the room that the active speaker is in. With room switching, all screens will change; with speaker switching, only one screen will change. All of the screens will not change to display the active speaker. The other screens will display other participants in the same room. With speaker switching, the other screens will display two other active table segments.
Reference:
Cisco: Multipoint Solution for Cisco TelePresence Systems
Cisco: Managing CTMS Meetings

Question 11

Which of the following features are supported by TelePresence Server operating in locally managed mode? (Choose two.)

Options:

A. Active Control

B. Conductor

C. clustering

D. ad hoc conferencing

E. Multiway conferencing

F. rendezvous conferencing

G. scheduled conferencing

Answer: C, G

Explanation:
Section: Conferencing Concepts Explanation
Clustering and scheduled conferencing, including WebEx conferencing, are supported by TelePresence Server operating in locally managed mode. In locally managed mode, the TelePresence Server manages all conference functions. In remotely managed mode, a device external to the TelePresence Server, such as Cisco TelePresence Conductor, manages conference functions.
TelePresence Server 7010 and MSE 8710 devices can operate in either locally managed mode or remotely managed mode. Cisco TelePresence Server on Multiparty Media 310 and 320 and Cisco TelePresence Server on Virtual Machine support only remotely managed mode.
TelePresence Server operating in locally managed mode does not support Conductor, Active Control, ad hoc conferencing, Multiway conferencing, or rendezvous conferencing. These features are supported by TelePresence Server operating in remotely managed mode. Active Control provides conference control

functions and participant information to endpoints. Remotely managed mode also supports ClearPath, which optimizes video quality by using advanced error-correction techniques.
Up to four blades can be configured in a cluster. A cluster of blades appears as if the blades are a single TelePresence Server. All blades in a cluster must be of the same type and run the same version of software. However, several different clusters can exist within an MSE chassis. Clustering is supported in both locally managed mode and remotely managed mode.
Reference:
Cisco: Optimized Conferencing for Cisco Unified CM and Cisco VCS (PDF)
Cisco: Cisco Rich Media Conferencing

Question 12

Which of the following is a Cisco DMM module that is used to provide an on-screen program guide for IPTV?

Options:

A. Cisco Cast

B. Cisco Digital Signs

C. Cisco Live Event

D. Cisco Show and Share

E. Cisco Media Experience Engine

Answer: A

Explanation:
Section: Endpoint Configuration Explanation
Cisco Cast is a Cisco Digital Media Management (DMM) module that is used to provide an onscreen program guide for IP television (IPTV) and Video on Demand (VoD) content on Cisco Digital Media Players (DMPs). Cisco DMM is an application that can manage, schedule, and publish digital media to displays.
Cisco DMM consists of the following modules:
- Cisco Digital Signs
- Cisco Show and Share
- Cisco Live Event - Cisco Cast
Cisco Digital Signs is used to categorize and manage Cisco DMPs. Each display can be controlled remotely and programmed to display whatever content is desired. Managers can create screen layouts that divide the screen into regions in which programmable content can be displayed.
Cisco Show and Share is an application that provides a secure community for video sharing and collaboration. User management and authentication are provided by Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), or an embedded DMM database. Each publisher can define which users can watch their video content. Searchable text transcripts can be added to each video so that media can be easily located. Related videos can be associated so that viewers can view additional relevant

material. Publishers can also allow viewers to comment, rate, and tag their videos.
Cisco Live Event enables Show and Share publishers to add synchronized graphics to their audio and video streams. Producers of live streaming events can publish poll questions to webcast viewers and allow those viewers to submit text-based questions to the presenters. Streamed events can be saved as a VoD session for subsequent viewing.
Cisco Media Experience Engine (MXE) is not a module of Cisco DMM. Cisco MXE is an appliance that can convert and adapt media formats as well as perform media postproduction. Media can be converted from and to many different formats for consumption on a wide variety of devices. Various formats are supported, from standard definition (SD) to high definition (HD). Media postproduction involves adding professional-looking features to media files, including bumpers, trailers, fades, transitions, animations, subtitles, captions, and other overlay graphics. Cisco Pulse Video Analytics, which is a component of MXE, can also automatically tag and index media files so that you can search videos that include a particular spoken phrase or word. MXE integrates with Cisco TelePresence Content Server (TCS) and Cisco Show and Share.
Reference:
Cisco: Cisco Digital Media Manager
Cisco: Cisco Media Experience Engine (MXE) 3500

Question 13

Which content sharing protocol is negotiated for point-to-point meetings in a Cisco TelePresence environment with H.323?

Options:

A. BFCP

B. H.239

C. Auto-Collaborate

D. Switched Presentation

Answer: B

Explanation:
Section: Conferencing Concepts Explanation
239 is negotiated for point-to-point meetings in a Cisco TelePresence environment with H.323. Content sharing protocols use a separate content channel to enable endpoints to display presentation materials and participants simultaneously.
Binary Floor Control Protocol (BFCP) is negotiated for point-to-point meetings in a Cisco TelePresence environment with Session Initiation Protocol (SIP). Auto-Collaborate is negotiated for point-to-point and multipoint meetings in a Cisco TelePresence environment with TelePresence Interoperability Protocol (TIP). If a content-sharing protocol cannot be negotiated, Switched Presentation can be used. However, when a participant is displaying presentation materials, only the presentation materials will be displayed; the participant will not be displayed.

Reference:
Cisco: Presentation Sharing in Cisco TelePresence Meetings (PDF)

Question 14

Which of the following statements is not correct regarding the Cisco TelePresence MCU?

Options:

A. Cisco TelePresence MCU is a software conference bridge.

B. Cisco TelePresence MCU supports SIP as the signaling protocol.

C. Cisco TelePresence MCU delivers up to 1080p at 30 frames per second.

D. Cisco TelePresence MCU supports ad-hoc and meet-me conferences.

E. Cisco TelePresence MCU can support multiple simultaneous conferences.

Answer: A

Explanation:
Section: Video Concepts Explanation
Cisco TelePresence multipoint control unit (MCU) is not a software conference bridge; it is a hardware conference bridge. By contrast, Cisco TelePresence Multipoint Switch (CTMS) is a software conference bridge.
Cisco TelePresence MCU is a multipoint video conferencing bridge that delivers up to 1080p at 30 frames per second. It supports ad-hoc and meet-me conferences, and multiple conferences can be hosted simultaneously on an MCU. Session Initiation Protocol (SIP) is used by Cisco TelePresence MCU as the signaling protocol.
Reference:
Cisco: Conference Bridge Configuration: Cisco TelePresence MCU Configuration Settings

Question 15

Which of the following network diagnostic commands can be issued on a Cisco TelePresence System Codec C60? (Choose two.)

Options:

A. systemtools network ping

B. systemtools network traceroute

C. utils network ping

D. utils network tracert

E. utils network traceroute

Answer: A, B

Explanation:
Section: Troubleshooting and Support Explanation
The systemtools network ping command and the systemtools network traceroute command can be issued on a Cisco TelePresence System Codec C60. The syntax of the systemtools network ping command is systemtools network ping destination, where destination is the IP address or Uniform Resource Locator (URL) of the destination target. The syntax of the systemtools network traceroute command is systemtools network traceroute destination, where destination is the IP address or URL of the destination target.
You cannot issue the utils network ping command on a Cisco C60, but you can issue it on a Cisco TelePresence Multipoint Switch (CTMS), Cisco TelePresence Manager, and Cisco Unified Communications Manager (CM). The syntax of the utils network ping command is utils network ping destination [count] [size], where destination is the IP address or host name of the destination. The optional count variable specifies the number of times to ping; if the count variable is not specified, the default value of 4 is used. The optional size variable specifies the size of the ping packets in bytes; if the size variable is not specified, the default value of 56 is used.
You cannot issue the utils network tracert command on a Cisco C60, but you can issue it on Cisco TelePresence Manager. The syntax of the utils network tracert command is utils network tracert destination, where destination is the IP address or host name of the destination.
You cannot issue the utils network traceroute command on a Cisco C60, but you can issue it on a CTMS and Cisco Unified CM. The syntax of the utils network traceroute command is utils network traceroute destination, where destination is the IP address or host name of the destination.
Reference:
Cisco: Cisco TelePresence System Codec C40/C60, API Reference Guide: The SystemTools commands (PDF)

Question 16

Which of the following statements is true regarding ad-hoc conferences for endpoints without Cisco VCS?

Options:

A. H.323 endpoints can neither initiate nor be added to an ad-hoc conference.

B. H.323 endpoints cannot initiate an ad-hoc conference but can be added to an ad hoc conference.

C. H.323 endpoints can initiate an ad-hoc conference but cannot be added to an ad hoc conference.

D. H.323 endpoints can initiate an ad-hoc conference and can be added to an ad-hoc conference.

Answer: B

Explanation:

Section: Conferencing Concepts Explanation
323 endpoints without Cisco TelePresence Video Communication Server (VCS) cannot initiate an ad-hoc conference but can be added to an ad-hoc conference by a Session Initiation Protocol (SIP) endpoint. Alternatively, H.323 endpoints can initiate an ad-hoc conference by using Multiway with Cisco VCS.
Ad-hoc conferences are also known as unscheduled or on-demand conferences. To participate in an ad-hoc conference, simply press the Conf, Join, cBarge, or Add keys on the endpoint.
SIP endpoints can initiate an ad-hoc conference and can be added to an ad-hoc conference. A SIP endpoint is required to add an H.323 endpoint to an ad-hoc conference without Cisco VCS.
Either MultiSite or Multiway can be used for ad-hoc conferences, which are also called on-demand conferences. MultiSite uses a phone's native multipoint control unit (MCU) functionality and allows up to four participants in a conference. However, MultiSite requires that an option key be installed on each endpoint. Multiway allows many more participants but requires a Cisco VCS and a Cisco TelePresence MCU to handle the conference. In addition, an option key is not required for Multiway. MultiSite and Multiway are mutually exclusive; if Multiway is used on your network, you should disable MultiSite on the endpoints.
Reference:
Cisco: Cisco Rich Media Conferencing: Ad-hoc Audio Conference