

300-835

Number: 300-835
Passing Score: 800
Time Limit: 120 min
File Version: 1

300-835



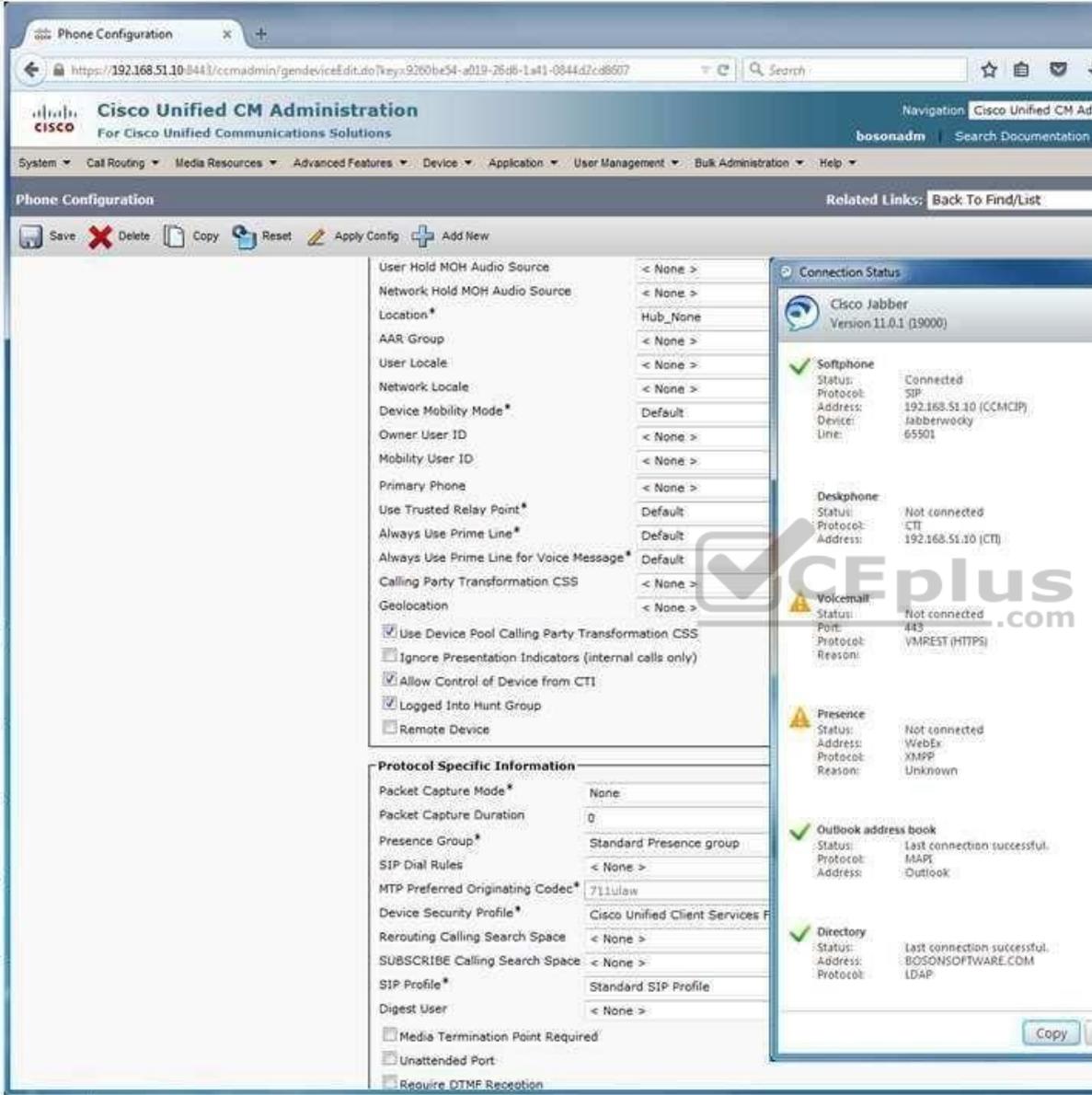
Website: <https://vceplus.com> - <https://vceplus.co>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

<https://vceplus.com/>

Exam A

QUESTION 1





The user named Joe Cambers is not able to use Cisco Jabber's IM or Presence functionality. Which of the following is most likely the reason?

- A. The softphone has no SIP profile.

- B. The softphone's profile does not allow CTI control.
- C. The SIP trunk to the CUPS server is down.
- D. The Cisco Unity Connection server either is down or is not installed.
- E. The Cisco Jabber client is configured to require a nonexistent desk phone.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most likely, the reason the user named Joe Cambers is not able to use Cisco Jabber's IM and Presence functionality is because the Session Initiation Protocol (SIP) trunk from Cisco Unified Communications Manager (UCM) to the Cisco Unified Presence (CUPS) server either is down or is not installed. Cisco Jabber relies on CUPS and the Extensible Messaging and Presence Protocol (XMPP) for instant messaging (IM) and Presence functionality. You can display and verify the backend systems to which the Cisco Jabber client is connected by clicking the gear icon and Show Connection Status in the Cisco Jabber home window. Clicking Show Connection Status displays the Connection Status window, which provides the connectivity status of every service to which Jabber is connected or is configured to connect. Services that are preceded by a green check mark have connected successfully. Services that display Not Connected or a caution icon have not connected successfully.

The Cisco Unity Connection server either is down or is not installed; however, this is not the reason that the user is not able to use Cisco Jabber's IM functionality. Cisco Unity Connection is a voice mail platform, not an IM platform.

The softphone has a SIP profile. Based on the value displayed in the SIP Profile field of the UCM Administration page in this scenario, you can determine that the softphone is configured to use the Standard SIP Profile, which is the default UCM SIP profile.

The softphone's profile does allow Computer Telephony Integration (CTI) control. Based on the value displayed in the Allow Control of Device from CTI field, you can determine that CTI control has been enabled for the softphone. However, disabling this option would not disable Jabber's IM functionality. CTI enables the Cisco Jabber client to control aspects of a connected hardware phone, or desk phone. However, the Cisco Jabber client does not require a desk phone. Both Jabber and Cisco Unified Personal Communicator communicate with a desk phone by using the CTI Quick Buffer Encoding (CTIQBE) protocol.

Reference:

Cisco: Troubleshooting the Cisco Unified Presence Server (CUPS) and Cisco Unified Personal Communication (CUPC): No Presence Information After Login

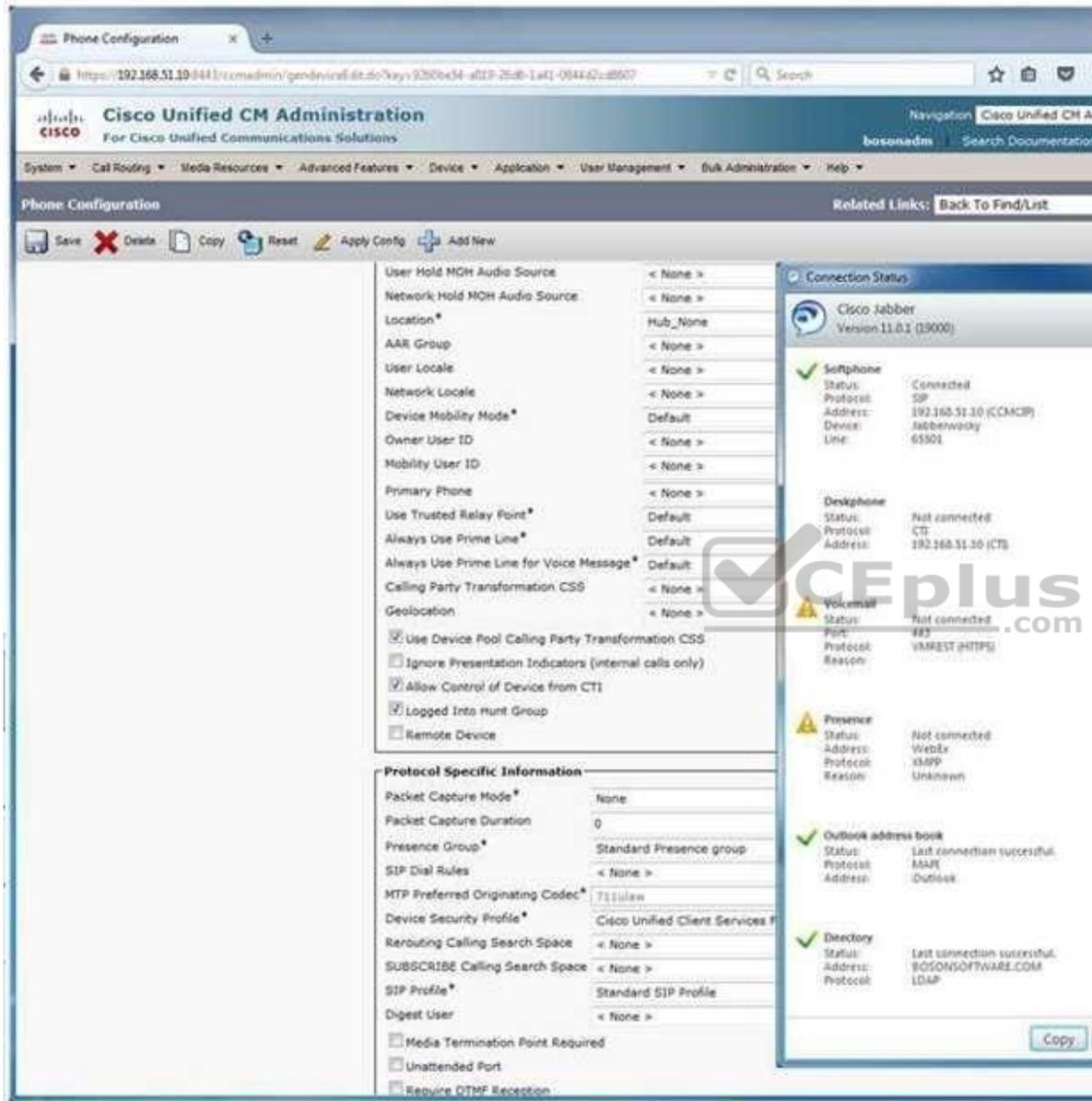
QUESTION 2

You are the administrator for your company's UCM network. Examine the exhibit below, and answer the question:



<https://vceplus.com/>





The screenshot shows the Cisco Unified CM Administration interface for configuring a Cisco Jabber client. The main configuration area includes fields for User Hold MOH Audio Source, Network Hold MOH Audio Source, Location, AAR Group, User Locale, Network Locale, Device Mobility Mode, Owner User ID, Mobility User ID, Primary Phone, Use Trusted Relay Point, Always Use Prime Line, Always Use Prime Line for Voice Message, Calling Party Transformation CSS, Geolocation, and checkboxes for Use Device Pool Calling Party Transformation CSS, Ignore Presentation Indicators, Allow Control of Device from CTI, Logged Into Hunt Group, and Remote Device. The 'Protocol Specific Information' section includes Packet Capture Mode, Packet Capture Duration, Presence Group, SIP Dial Rules, MTP Preferred Originating Codec, Device Security Profile, Rerouting Calling Search Space, SUBSCRIBE Calling Search Space, SIP Profile, Digest User, and checkboxes for Media Termination Point Required, Unattended Port, and Require DTMF Reception.

The 'Connection Status' window on the right shows the following information:

Device	Status	Protocol	Address	Line
Selfphone	Connected	SIP	192.168.51.10 (CCMCRP)	65501
Deskphone	Not connected	CTI	192.168.51.10 (CTI)	
VoiceMail	Not connected	483	VMREST (HTTPS)	
Presence	Not connected	WebEx	WebEx	Unknown
Outlook address book	Last connection successful	LDAP	Outlook	
Directory	Last connection successful	LDAP	BOSONSOFTWARE.COM	

Which of the following fields should you configure to enable calls from this Cisco Jabber client to be rerouted through the PSTN if bandwidth is lacking?

- A. AAR Group
- B. Location
- C. Rerouting Calling Search Space

- D. SUBSCRIBE Calling Search Space
- E. Use Trusted Relay Point

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You should configure the AAR Group field to enable calls from this Cisco Jabber client to be rerouted through the public switched telephone network (PSTN) if bandwidth is lacking. Automated Alternate Routing (AAR) Group configurations enable calls to be rerouted to specified destinations when Cisco Unified Communications Manager (UCM) blocks a call because bandwidth is lacking. AAR Group profiles are configured by navigating to Call Routing > AAR Group in UCM Administration. After you have configured a profile, you can assign it to an endpoint by selecting the profile from the AAR Group dropdown field on the Device > Phone configuration page for the given endpoint.

You should not configure the Location field. The Location field is used to configure call admission control (CAC). CAC is used to limit bandwidth available for audio and video calls between locations, thereby regulating the quality of those calls. The location of Hub_None, which is used in this scenario, indicates that UCM is not monitoring the bandwidth that this particular endpoint is using. Locations can be configured by navigating to System > Location in UCM Administration. After locations have been configured, you can apply the configuration to an endpoint by selecting it from the Location dropdown field on the Device > Phone configuration page for the given endpoint.

You should configure neither the Rerouting Calling Search Space field nor the SUBSCRIBE Calling Search Space field. A search space is an ordered list of partitions that a device is allowed to search for patterns that match a given string, such as a dialed number. The Rerouting Calling Search Space field determines the route to a refer to target. The target is specified in a Session Initiation Protocol (SIP) Refer message. The SUBSCRIBE Calling Search Space field, on the other hand, is used to route Presence subscribe requests from an endpoint.

You should not configure the Use Trusted Relay Point field. A Trusted Relay Point (TRP) is a transcoder or media termination point (MTP) device that UCM considers to be the closest to a given endpoint if multiple resources are required for the endpoint. When this option is configured to the Default setting, the endpoint uses a common device configuration to determine the TRP setting. If this option is configured to Off, UCM will not attempt to use a TRP for the endpoint regardless of the common device configuration. If this option is configured to On, UCM will attempt to use a TRP for the endpoint regardless of the common device configuration.

Reference:

[Cisco: Automated Alternate Routing Group Configuration](#)

QUESTION 3

You want to configure an alerting name that will be displayed on a caller's IP phone when the recipient's IP phone is ringing. Which of the following fields in UCM Administration should you edit?

- A. the Alerting Name field on the dn configuration page
- B. the Alerting Name field on the phone configuration page
- C. the Alerting Name field on the end user configuration page

D. the Alerting Name field on the server configuration page

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You should edit the Alerting Name field on the directory number (dn) configuration page in Cisco Unified Communications Manager (UCM) Administration if you want to configure an alerting name that will be displayed on a caller's IP phone when the recipient's IP phone is ringing. For example, if you want the name JOE to be displayed when a user calls Joe's extension, you would configure an alerting name of JOE on the dn configuration page for Joe's extension. The dn configuration page also contains a variety of other configuration options, such as the route partition to which the dn belongs and the maximum number of calls.

You should not edit the Alerting Name field on the phone configuration page, because that field does not exist on that page. The UCM Administration phone configuration page enables you to configure settings specific to a given IP phone. To identify the IP phone that you are configuring, you should enter the Media Access Control (MAC) address of the IP phone in the MAC Address field on the phone configuration page. You can also configure softkey templates and the common device configuration that you want to apply to the IP phone on this page.

You should not edit the Alerting Name field on the end user configuration page, because that field does not exist on that page. The UCM Administration end user configuration page enables you to configure settings specific to a given user. For example, you can configure a user ID, password, and personal identification number (PIN) on the end user configuration page.

You should not edit the Alerting Name field on the server configuration page, because that field does not exist on that page. The UCM Administration server configuration page enables you to configure settings such as the host name or IP address of the server, the IP version 6 (IPv6) name of the server, and a description of the server.

Reference:

Cisco: Directory Number Configuration: Directory Number Configuration Settings

QUESTION 4

You are editing the user account named jpublic in the Cisco Unity Connection administrative GUI. Which of the following cannot be modified from the Message Settings page?

- A. the maximum voice mail message length
- B. the voice mail message greeting
- C. voice mail message editing
- D. the voice mail message language
- E. the voice mail message urgency

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

You cannot modify a user's voice mail message greeting from the Message Settings page when editing a user account in the Cisco Unity Connection administrative graphical user interface (GUI). There are three typical ways to create users in Unity Connection: local manual creation, import from Cisco Unified Communications Manager (UCM), or synchronization by using Lightweight Directory Access Protocol (LDAP). When manually editing users in the GUI, you can modify settings that are related to a user's voice mail greeting by modifying the options on the Greeting page. For example, you can use the Callers Hear field on the Greeting page to determine whether callers who reach the user's voice mail hear the system default greeting, the user's personal greeting, or nothing. If you want to modify the Callers Hear field value for a single user, you should edit the field on the Greeting page of the user's account. You can also modify the setting for a number of users at once by editing the Callers Hear field in Bulk Edit Mode. In addition, you can configure the Callers Hear field on the Greeting page of a voice mail user template.

You can modify the maximum voice mail message length that can be recorded by an outside caller in a user's voice mailbox from the Message Settings page. By default, the Maximum Message Length field is configured to 300 seconds. If you want to modify the Maximum Message Length field value for a single user, you should edit the field on the Message Settings page of the user's account. You can also modify the setting for a number of users at once by editing the Maximum Message Length field in Bulk Edit Mode. In addition, you can configure the Maximum Message Length field on the Message Settings page of a voice mail user template to apply a nondefault maximum message length to any new user accounts that are based on the template.

You can modify whether a caller can edit voice mail messages from the Message Settings page. By default, the Callers Can Edit Messages check box is configured to allow callers to listen to, append to, rerecord, or delete their messages in a user's voice mailbox. If you want to modify the Callers Can Edit Messages check box for a single user, you should edit the check box on the Message Settings page of the user's account. You can also modify the setting for a number of users at once by editing the Callers Can Edit Messages check box in Bulk Edit Mode. In addition, you can configure the Callers Can Edit Messages check box on the Message Settings page of a voice mail user template to apply a nondefault setting to any new user accounts that are based on the template.

You can modify the language that callers hear from the Message Settings page. By default, the Language That Callers Hear field is configured to use the system default language. Modifying this field changes only the language of system prompts, not the language of user-recorded greetings. If you want to modify the Language That Callers Hear field for a single user, you should edit the field on the Message Settings page of the user's account. You can also modify the setting for a number of users at once by editing the Language That Callers Hear field in Bulk Edit Mode. In addition, you can configure the Language That Callers Hear field on the Message Settings page of a voice mail user template to apply a nondefault setting to any new user accounts that are based on the template.

You can modify the default urgency level of voice mail messages from the Message Settings page. The Message Urgency field can be configured to mark all voice mails as urgent, to mark all voice mails as normal, or to prompt callers to mark a message as urgent. If you want to modify the Message Urgency field for a single user, you should edit the field on the Message Settings page of the user's account. You can also modify the setting for a number of users at once by editing the Message Urgency field in Bulk Edit Mode. In addition, you can configure the Message Urgency field on the Message Settings page of a voice mail user template to apply a nondefault setting to any new user accounts that are based on the template.

Reference:

[Cisco: Cisco Unity Connection 8.x User Settings: Edit Greeting](#)

[Cisco: Cisco Unity Connection 8.x User Settings: Edit Message Settings](#)

QUESTION 5

You want to verify that an IP phone has downloaded a configuration file from a TFTP server.

Which of the following would you most likely do on the IP phone?

- A. Press settings > Network Configuration, and verify the TFTP server's IP address.
- B. Press settings > Network Configuration, and verify the DHCP server's IP address.
- C. Press settings > Network Configuration, and verify that DHCP is enabled.
- D. Press settings > Network Configuration, and verify the VLAN ID.
- E. Press settings > Status > Status Messages.
- F. Press settings > Status > Network Statistics.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You would most likely press settings > Status > Status Messages on the IP phone to verify that an IP phone has downloaded a configuration file from a Trivial File Transfer Protocol (TFTP) server. A TFTP server is required so that IP phones can download their startup configuration files. If an IP phone has successfully downloaded a configuration file from a TFTP server, you will see output in Status Messages indicating the time of the download and the name of the configuration file. A Session Initiation Protocol (SIP)-enabled phone configuration file typically consists of the letters SEP and the Media Access Control (MAC) address of the IP phone. Therefore, an IP phone with the MAC address 0012:3456:789A will attempt to download a configuration file named SEP00123456789A.cnf.xml from the TFTP server. If the IP phone does not successfully download the file, you might see one of the following messages in the Status Messages output:

- CFG file not found, which indicates that the TFTP server is reachable but that the configuration file was not found on the TFTP server
- CFG TFTP Size Error, which indicates that the TFTP server is reachable and the configuration file is available but that the configuration file is too large for the IP phone
- TFTP access error, which indicates that the IP phone can connect to the TFTP server but that the configuration file directory does not exist -
- TFTP Error, which indicates that the TFTP server generated an unknown error
- TFTP timeout, which indicates that the TFTP server did not respond to the download request

You would not press settings > Network Configuration on the IP phone and verify the virtual LAN (VLAN) ID. Although you could verify that the IP phone is able to contact a Dynamic Host Configuration Protocol (DHCP) server by ensuring that the DHCP server and the IP phone are operating on the same VLAN, the ability to communicate with a DHCP server alone is not an indicator that the IP phone has successfully downloaded a configuration file from the TFTP server.

You would not press settings > Network Configuration on the IP phone and verify the TFTP server's IP address to verify that an IP phone has downloaded a configuration file from a TFTP server. Although you could verify that the TFTP server's IP address is correct by viewing the information in the settings > Network Configuration > TFTP Server 1 field, a valid TFTP server IP address alone is not an indicator that the IP phone has successfully downloaded a configuration file from the TFTP server.

You would not press settings > Network Configuration on the IP phone and verify that DHCP is enabled to verify that an IP phone has downloaded a configuration file from a TFTP server. Although the IP phone can receive a TFTP server IP address from a DHCP server, the configuration of a TFTP server IP address alone is not an indicator that the IP phone has successfully downloaded a configuration file from the TFTP server.

You would not press settings > Network Configuration on the IP phone and verify the DHCP server's IP address to verify that an IP phone has downloaded a configuration file from a TFTP server. Although the IP phone can receive a TFTP server IP address from a DHCP server, and the IP phone must be able to communicate with the DHCP server so that the IP phone can receive network information from the DHCP server, verifying the DHCP server IP address alone is not an indicator that the IP phone has successfully downloaded a configuration file from the TFTP server.

You would not press settings > Status > Network Statistics on the IP phone to verify that an IP phone has downloaded a configuration file from a TFTP server. The settings > Status > Network Statistics display provides statistics about packets that have been transmitted to and from the IP phone. In addition, you can see whether the IP phone is bound to a DHCP server. However, none of the information in the Network Statistics output indicates that the IP phone has successfully downloaded a configuration file from the TFTP server.

Reference:

[Cisco: Viewing Status, Statistics, and Firmware Information on the Cisco Unified IP Phone: Status Messages Screen](#)

[Cisco: Viewing Model Information, Status, and Statistics on the Cisco Unified IP Phone: Call Statistics Screen](#)

[Cisco: Configuring Settings on the Cisco Unified IP Phone: Network Configuration Menu](#)

QUESTION 6

Another administrator modifies the UCM cluster security password by using the CLI.

Which of the following is most likely to be affected by this change?

- A. encryption of DRS backups that were made prior to the change
- B. encrypted communication between DRS Master Agents and Local Agents
- C. the addition of new backup devices to a DRS schedule
- D. the deletion of old backup devices from a DRS schedule
- E. access to network storage location configuration



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, encryption of Cisco Unified Communications Manager (UCM) Disaster Recovery System (DRS) backups that were made prior to the password change will most likely be affected if another administrator modifies the cluster security password by using the command-line interface (CLI). DRS, which is a cluster-level backup system for UCM, uses the existing cluster security password when performing encryption on a backup. If the cluster security password is modified by using the CLI or by a fresh UCM installation, you might not be able to decrypt and restore that backup. Workarounds to this issue include remembering the old cluster security password that was used to encrypt the data or immediately performing a fresh backup when the cluster security password changes.

Encrypted communications between DRS Master Agents and Local Agents are not likely to be affected by this change. Master Agents store component registrations, maintain scheduled tasks, and store backup data on a locally attached device. Local Agents, which are installed and activated by default on each cluster node, are responsible for running backup and restore scripts on the local server. DRS uses Secure Sockets Layer (SSL) to both authenticate and encrypt data between a Master Agent and a Local Agent. In addition, DRS uses IP Security (IPSec) for public key infrastructure (PKI) encryption.

The addition or deletion of backup devices to a DRS schedule will not be affected by the password change. However, it is important to note that a backup device cannot be deleted from DRS if that backup device is part of an existing backup schedule. In order to remove an existing backup device from a DRS configuration, you must first ensure that the device has been removed from any backup schedules in which it might be configured.

Access to network storage location configuration will not be affected by the password change. In order to configure network storage locations, you must have access to a Secure File Transfer Protocol (SFTP) server. In addition to backing up data to devices that are directly connected to a Master Agent, DRS can back up to network storage locations by using SFTP.

Reference:

[Cisco: Disaster Recovery System Administration Guide for Release 8.5\(1\): What is the Disaster Recovery System?](#)

QUESTION 7

You are manually provisioning an IP phone by using UCM Administration. You want to replace the conference call button on the user's IP phone with a speed dial button.

Which of the following fields should you update?

- A. Device Pool
- B. Phone Security Profile
- C. MAC Address
- D. Phone Button Template

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

Explanation:

You should update the Phone Button Template field to ensure that the IP phone you are provisioning by using Cisco Unified Communications Manager (UCM) Administration replaces the conference call button with a speed dial button. Phone button templates are used to add or arrange IP phone buttons for a given device or group of devices. You can create or edit phone button templates by clicking Device > Device Settings > Phone Button Template in UCM. When you are manually provisioning an IP phone in UCM Administration, you must fill in the MAC Address field, the Device Pool field, the Phone Button Template field, and the Phone Security Profile field.

You do not need to update the Device Pool field to ensure that the IP phone you are provisioning provides the user with a Mobility option. Although required when manually provisioning an IP phone in UCM Administration, the Device Pool field specifies a given set of characteristics that are to be applied to IP phones within the pool, such as region, date and time groups, softkey templates, and more. However, Device Pool does not configure an IP phone with a Mobility button.

You do not need to update the Phone Security Profile field to ensure that the IP phone you are provisioning provides the user with a Mobility option. The Phone Security Profile field is used to create or modify the security configuration of devices to which the profile is applied. For example, you can assign a profile that supports UCM authentication or encryption to a device that supports those features.

You do not need to update the MAC Address field to ensure that the IP phone you are provisioning provides the user with a Mobility option. The MAC Address field contains the Media Access Control (MAC) address of the device that you are provisioning. The MAC address is a hardware address that is assigned by the device manufacturer.

Reference:

QUESTION 8

Which of the following cannot be watched by the Presence feature of UCM?

- A. an MGCP trunk
- B. an SCCP line
- C. a SIP line
- D. a SIP trunk

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A Media Gateway Control Protocol (MGCP) trunk cannot be watched by the Presence feature of Cisco Unified Communications Manager (UCM). Presence enables an IP phone user to monitor other directory numbers (dns) in real time by displaying a status icon beside dns that appear in speed-dial lists or directory lists, such as the Missed Calls list, on an IP phone. The icon can represent one of the following three states:

- Unknown - The registration status of the device that is associated with the directory dn cannot be determined.
- On-hook - The device that is associated with the dn is registered and currently in the on-hook state.
- Off-hook - The device that is associated with the dn is registered and currently in the off-hook state.

Devices that can send Presence requests for information about dns are called watchers. Session Initiation Protocol (SIP) Uniform Resource Identifiers (URIs) or dns that can be monitored by Presence are known as presence entities, or presentities. Presence can send and receive presence requests and responses only on Skinny Client Control Protocol (SCCP) lines, SIP lines, and SIP trunks. If Presence requests or responses are sent to an MGCP trunk or to an H.323 trunk, those requests are rejected by UCM.

Reference:

Cisco: Presence: Understanding How Presence Works with Route Lists

QUESTION 9

A caller from the PSTN attempts to connect to an extension that does not exist on your company's VoIP network.

Which of the following settings in the Call Forward and Pickup Settings section of the UCM Administration Directory Number Configuration page would direct such callers to voice mail?

- A. Forward All
- B. Forward Busy External
- C. Forward Busy Internal
- D. Forward No Answer External
- E. Forward No Answer Internal

F. Forward Unregistered External

Correct Answer: F

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, the Forward Unregistered External setting in the Call Forward and Pickup Settings section of the Cisco Unified Communications Manager (UCM) Administration Directory Number Configuration page would direct a caller from the public switched telephone network (PSTN) to voice mail if that caller attempted to connect to an extension that does not exist on your company's Voice over IP (VoIP) network. The Directory Number Configuration page enables a UCM administrator to configure several settings related to directory numbers (dns), including the following: call forwarding, call pickup, call waiting, line display text, ring settings, and voice mailboxes. In contrast to the Forward Unregistered External setting, the Forward Unregistered Internal setting would forward internal callers to a specific voice mailbox if the internal caller dialed a nonexistent dn.

The Forward All setting forwards all callers, internal or external, to a specific voice mailbox. This is the same behavior as the CFwdAll softkey that appears on a Cisco IP phone. However, an administrator can configure this behavior for a user by accessing the Directory Number Configuration page if the user for some reason does not have access to the CFwdAll softkey.

The Forward Busy External setting forwards any calls from the PSTN that arrive while the given dn is already in use. Similarly, the Forward Busy Internal setting forwards any internal calls that arrive while the given dn is already in use.

The Forward No Answer External setting forwards any calls from the PSTN that go unanswered by the user. Similarly, the Forward No Answer Internal setting forwards any internal calls that go unanswered by the user.

Reference:

Cisco: Directory Number Configuration: Directory Number Configuration Settings

QUESTION 10

You are integrating an existing Cisco UCM system with a new CUPS server. You will be using Cisco Unified Personal Communicator in both its softphone mode and its desk phone control mode. You navigate to Cisco Unified Serviceability > Tools > Service Activation and ensure that TFTP and the Cisco AXL Web Service are both enabled.

Which of the following services must also be enabled on the UCM system to complete the integration?

- A. Cisco CTIManager
- B. Cisco DirSync
- C. Cisco Extension Mobility
- D. Cisco Messaging Interface

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

The Cisco CTIManager server must also be enabled to integrate an existing Cisco Unified Communications Manager (UCM) system with a Cisco Unified Presence (CUPS) server and to use Cisco Unified Personal Communicator in both its softphone mode and its desk phone control mode. The Cisco Computer Telephony Integration (CTI) feature is a development system that enables programmers to create applications that can connect to and communicate with a Cisco Unified Communications system. By using CTI, programmers can create server software and desktop applications that interface directly with UCM, CUPS, and other Cisco Voice over IP (VoIP) products. In order to use Cisco Unified Personal Communicator in desk phone control mode, the Cisco CTIManager service must be enabled and started on UCM. Unified Personal Communicator communicates with the desk phone by using the CTI Quick Buffer Encoding (CTIQBE) protocol.

Cisco CallManager, Cisco Trivial File Transfer Protocol (Cisco TFTP), and Cisco Administrative Extensible Markup Language (AXL) Web Service must also be enabled and started in order to integrate CUPS and UCM in the configuration described in this scenario. The Cisco TFTP service is required to enable Cisco Unified Personal Communicator to operate in softphone mode. The Cisco AXL Web Service is required to enable the synchronization of data between CUPS and UCM. Finally, the CallManager service, which is also called the Cisco Unified Communications Service, is required for UCM to use software call processing, signaling, and control.

The Cisco Directory Synchronization (DirSync) service is not required to integrate CUPS with UCM. The Cisco DirSync service enables an administrator to keep the UCM database synchronized with external directories, such as Microsoft Active Directory.

The Cisco Extension Mobility service is not required to integrate CUPS with UCM. Extension Mobility enables a user to log in to an IP phone that is capable of extension mobility service and to use that IP phone with the same features and settings as the user's typical desk phone.

The Cisco Messaging Interface service is not required to integrate CUPS with UCM. Messaging Interface enables the connection of Simplified Message Desk Interface (SMDI) voice mail systems to UCM. The SMDI protocol defines how voice mail systems interact with telephone systems.

Reference:

[Cisco: Cisco Unified Communications Manager configuration for integration with IM and Presence Service: Verify Required Services Are Running on Cisco Unified Communications Manager](#)

[Cisco: Integrating Cisco Unified Presence Server with Cisco Unified Communications Manager: Verify that Required Services are Running on CUCM](#)

QUESTION 11

Which of the following commands should you issue to set the maximum number of extensions that you can configure on a CME router? (Choose two.)

- A. ephone
- B. ephone-dn
- C. max-dn
- D. max-ephones
- E. telephony-service
- F. dnwebedit

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You should issue the telephony-service command and the max-dn command to set the maximum number of directory numbers (dns), or extensions, that you can configure on a Cisco Unified Communications Manager Express (CME) router. Issuing the telephony-service command puts the router into telephony-service configuration mode, where you can issue commands that configure telephony settings on the router, such as the max-dn and max-ephones commands.

A CME router requires three values in order to configure basic telephony service: an IP address, a max-dn value, and a max-ephones value. The maximum value of the max-dn parameter varies based on the router model, the IOS version, and the amount of memory. If you do not issue the max-dn command, you will not be able to configure any ephone-dns on the router.

You should issue the dn-webedit command to enable the addition of ephone-dns by using the browser-based graphical user interface (GUI). By default, you cannot add an extension to CME by using the browser-based GUI. The dn-webedit command should be issued in telephony-service configuration mode.

You should issue the max-ephones command to set the maximum number of phones, not the maximum number of extensions, that you can configure on a router. Like the max-dn command, the max-ephones command must be issued in telephony-service configuration mode. The maximum value of the max-ephones parameter varies based on the router model and the IOS version. If you do not issue the max-ephones command, you will not be able to configure any ephones on the router.

You cannot issue the ephone-dn command to set the maximum number of extensions that you can configure on a router. The ephone-dn command configures an ephone-dn. The syntax of the ephone-dn command is ephone-dn dn-tag [dual-line | octo-line]. Issuing the ephone-dn command puts the router into ephone-dn configuration mode. To set the extension number for an ephone-dn, you should issue the number command in ephone-dn configuration mode.

You cannot issue the ephone command to set the maximum number of extensions that you can configure on a router. The ephone command configures an ephone. The syntax of the ephone command is ephone phonetag. Issuing the ephone command puts the router into ephone configuration mode. To associate a physical IP phone with an ephone, you should issue the ma-address mac-address command in ephone configuration mode, where mac-address is the Media Access Control (MAC) address of the IP phone.

Reference:

[Cisco: Cisco Unified CME Commands: max-dn](#)

[Cisco: Cisco Unified CME Commands: max-ephones](#)

QUESTION 12

Which of the following terms describes LFI?

- A. a QoS model
- B. a queuing method
- C. a link efficiency mechanism
- D. a resource reservation method
- E. a congestion avoidance mechanism

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:**Explanation:**

Link fragmentation and interleaving (LFI) is a link efficiency mechanism. Without LFI, small packets, such as voice packets, can become stuck behind large packets as the large packets are transmitted through an interface, thereby causing delay and jitter. LFI breaks up large data packets into small pieces and then interleaves the small packets among the fragments of the large packet. Another link efficiency mechanism used by Voice over IP (VoIP) is Compressed Real-time Transport Protocol (cRTP), which compresses the Layer 3 and Layer 4 headers of voice packets to a fraction of their original size.

LFI is a Quality of Service (QoS) feature, not a QoS model. QoS enables a network to treat a specific type of traffic with a different priority than other types of traffic.

For example, QoS can ensure that voice traffic gets higher priority on a network than data traffic. QoS models include the best-effort model, the Integrated Services (IntServ) model, and the Differentiated Services (DiffServ) model. Each QoS model handles packet flows in a different manner. For example, IntServ requires that applications reserve their end-to-end bandwidth requirements, and DiffServ prioritizes packets by traffic class. Because of some inherent shortcomings in the IntServ model, Cisco recommends using DiffServ when delivering voice traffic.

LFI is not a resource reservation method. When IntServ is used, bandwidth resources must be reserved for each traffic flow. These resources are reserved from the source to the destination by Resource Reservation Protocol (RSVP).

LFI is not a queuing method. Queuing methods deal with congestion management. Each queuing method handles network congestion in a different manner. Queuing methods employed by Cisco routers include first-in-first-out (FIFO) queuing, priority queuing (PQ), custom queuing (CQ), round robin (RR), weighted RR (WRR), weighted fair queuing (WFQ), class-based WFQ (CBWFQ), and low latency queuing (LLQ). By default, Cisco devices use FIFO queuing for interfaces faster than 2.048 Mbps and use WFQ for serial interfaces at 2.048 Mbps or lower.

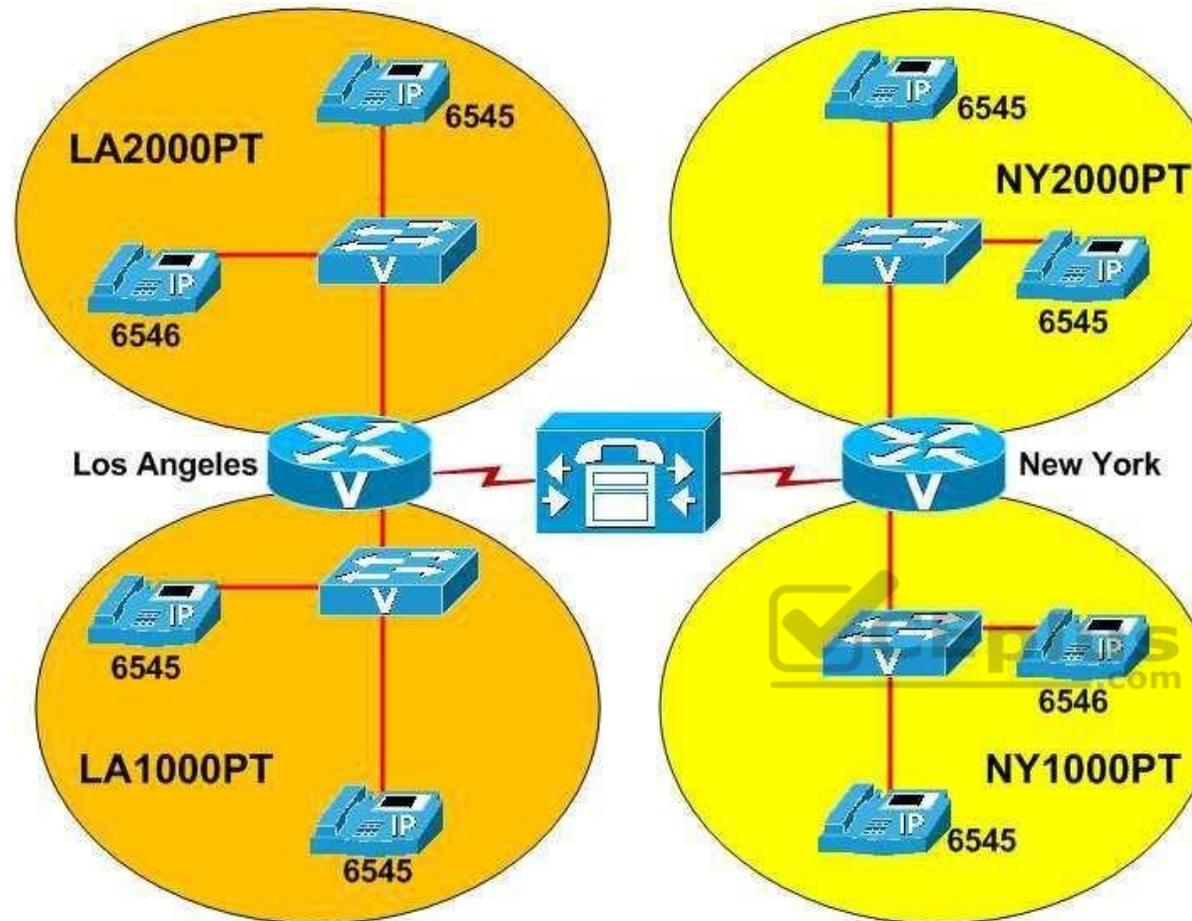
LFI is not a congestion avoidance mechanism. Congestion avoidance mechanisms mitigate tail drop, which occurs when a router drops new packets because its queues are too full to accept them. Congestion avoidance mechanisms employed by Cisco routers include random early detection (RED), weighted RED (WRED), and class-based WRED (CBWRED).

Reference:

[Cisco: Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2: Chapter: Link Efficiency Mechanisms Overview](#)

QUESTION 13

View the Exhibit.



You administer the VoIP network above.

The VoIP network is divided into four partitions. Two of the partitions are in Los Angeles, and two are in New York.

Which of the following are true? (Choose two.)

- A. The dn 6545 is not shared.
- B. The dn 6545 is shared within LA1000PT.
- C. The dn 6545 is shared between LA1000PT and LA2000PT.
- D. The dn 6546 is not shared.
- E. The dn 6546 is shared within NY1000PT.
- F. The dn 6546 is shared between NY1000PT and NY2000PT.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The directory number (dn) 6546 is not shared. However, the dn 6545 is shared within the LA1000PT partition. You can segregate a Voice over IP (VoIP) network into partitions in order to facilitate the use of different route patterns for different subsets of users. For example, if users in the LA1000PT partition should not be allowed to make long distance phone calls, you can restrict long distance phone calls in LA1000PT without affecting the route patterns in the other three partitions.

Any dn that is configured in more than one partition will not be shared between the two partitions, because the partitions are treated as individual VoIP networks. Because a dn can be configured in more than one partition, the same dn can present different line identification information depending on its configuration within the given partition. By contrast, a dn that is configured on multiple devices within the same partition is considered to be a shared dn, or a shared line.

The dn 6545 has been configured in all four partitions of the VoIP network. However, dn 6545 has been configured multiple times in only two of the partitions: LA1000PT and NY2000PT. Therefore, dn 6545 has been configured as a shared line in both the LA1000PT partition and the NY2000PT partition of the VoIP network. In Cisco Unified Communications Manager (UCM) Administration, you can configure a dn as a shared line by navigating to the device on which you want the shared line to appear and adding the dn for the shared line to that device.

The dn 6546 has been configured in two of the four partitions of the VoIP network. However, dn 6546 has not been configured more than once in the same partition. The dn 6546 is configured on one device in the LA2000PT partition and on one device in the NY1000PT partition. Because it is not configured more than once within the same partition, dn 6546 is not a shared dn.

Reference:

Cisco: Cisco Unified Communications Manager System Guide, Release 8.0(2): Shared Line Appearance

QUESTION 14

Which of the following Cisco Jabber features are not supported when UCM IM and Presence Service is running in IM-only mode? (Choose two.)

- A. audio calls
- B. IM
- C. Presence
- D. video calls
- E. XMPP integration

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Neither the audio call feature nor the video call feature of Cisco Jabber is supported when Cisco Unified Communications Manager (UCM) instant message (IM) and Presence Service is running in IM-only mode. The UCM IM and Presence Service enables a company to reduce communications delays in project

collaboration by providing real-time, always available communications channels. For example, the IM and Presence Service supports persistent chat rooms, which are chat rooms that remain available even after the last user exits the room, and the ability to review IM history.

The UCM IM and Presence Service has two modes of operation: IM-only and Cisco Unified Communications mode. In IM-only mode, Cisco Jabber and third-party Extensible Messaging and Presence Protocol (XMPP) clients can connect to and use UCM for IM and Presence services. In Cisco Unified Communications mode, the IM and Presence Service supports IM, Presence, XMPP federation, and audio and video calls. XMPP federation allows Cisco Jabber clients to communicate with clients that are registered to a different Cisco Jabber cluster.

To place an audio or video call from Cisco Jabber, a user will typically click the Contacts button to search the list of contacts. Next, the user should click on the contact to call and press the phone icon. However, IM messaging will be the only available option if UCM is configured in IM-only mode.

Reference:

[Cisco: Cisco Unified Communications Manager IM and Presence Service 9.0 Data Sheet](#)

QUESTION 15

Which of the following are voice messaging products that can be installed on a Cisco UCS? (Choose two.)

- A. CME
- B. UCM
- C. Unity
- D. CUE
- E. Unity Connection



Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cisco Unity and Cisco Unity Connection are voice messaging products that can be installed on a Cisco Unified Computing System (UCS). A UCS is a virtualized system of Voice over IP (VoIP) platforms that can help lower administrative overhead by consolidating multiple VoIP software platforms into a single hardware platform. In addition to a UCS installation, Unity can be installed on a Microsoft Windows server. Unity Connection can also be installed as a separate appliance. Unity supports a maximum of 15,000 voice mailboxes. Unity Connection supports a maximum of 250 voice messaging ports and 20,000 voice mailboxes. However,

Unity Connection also supports two different types of users: users with a mailbox and users without a mailbox. Unity Connection supports voice-enabled features, such as voice navigation and voice dialing; it can also be used to listen to audio translations of email messages and has an automated attendant feature.

Cisco Unity Express (CUE) is not a voice messaging product that can be installed on a UCS. CUE is typically installed in a module slot on a Cisco Unified Communications Manager Express (CME) router. CUE provides voice mail messaging, automated attendant services, and interactive voice response (IVR) services. CUE can support a maximum of 250 voice mailboxes, depending on the license that is installed.

CME is not a voice messaging product that can be installed on a UCS. CME is a call processing platform that is based on IOS and contained within a Cisco Integrated Services Router (ISR). CME supports a maximum of 350 IP phones.

Cisco Unified Communications Manager (UCM) is a call processing platform, not a voice messaging product. However, UCM can be installed in a UCS. UCM supports a maximum of 30,000 IP phones per cluster.

Reference:

[Cisco: Cisco Voice Messaging: Cisco Unity and Unity Connection Virtualization](#)

[Cisco: Unified Communications Deployment Models: Design Considerations for Running Virtual Unified Communications Applications on B-Series Blade Servers](#)

QUESTION 16

Which of the following Cisco Unity Connection services notifies components of changes to the database?

- A. Connection DB Event Publisher
- B. Connection CM Database Event Listener
- C. Connection Message Transfer Agent
- D. Connection Branch Sync Service

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Connection DB Event Publisher service, which is a Cisco Unity Connection base service, notifies components of changes to the Unity Connection database. Many Cisco Unity Connection services, including base services, can be managed from the Control Center in Cisco Unity Connection Serviceability. However, some status-only services, including Connection DB, Connection Server Role Manager, and Connection Serviceability, cannot be managed from the Control Center and can be deactivated only from a command-line interface (CLI).

The Connection Message Transfer Agent does not notify components of changes to the Unity Connection database. The Connection Message Transfer Agent is a critical Unity Connection service that enables voice mail messages to be delivered to the message store. Although Unity Connection will operate without this service, voice mail messages cannot be delivered without it.

The Connection CM Database Event Listener does not notify components of changes to the Unity Connection database. However, the Connection CM Database Event Listener, which is an optional Unity Connection service, is capable of detecting changes in the Cisco Unified Communications Manager (UCM) database. The Connection Branch Sync Service does not notify components of changes to the Unity Connection database. The Connection Branch Sync Service, which is an optional Unity Connection service, enables Unity Connection's Survivable Remote Site Voicemail (SRSV) function.

Reference:

[Cisco: Managing Services in Cisco Unity Connection 10.x \(PDF\)](#)

QUESTION 17

Which of the following is true of both the Cisco Unified Personal Communicator and the Cisco Unified Client Services Framework phone types in UCM?

- A. Device names must begin with UPC.
- B. Device names can be no longer than 15 characters.

- C. Device names can contain uppercase letters only.
- D. Device names can contain numbers and uppercase letters only.
- E. Device names have no naming convention.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Softphone device names can be no longer than 15 characters for both the Cisco Unified Personal Communicator and the Cisco Unified Client Services Framework phone types in Cisco Unified Communications Manager (UCM). A softphone is software that behaves like a phone, enabling a user to have voice conversations over a typical workstation network connection. Softphone mode is an operational mode that Unified Personal Communicator uses to act as a softphone. In order to use Unified Personal Communicator as a softphone with UCM, you must add a device to UCM that enables the registration of Unified Personal Communicator in softphone mode.

The Cisco Unified Personal Communicator device type naming convention requires that the name begin with the letters UPC and be derived from the UCM user name. The Cisco Unified Client Services Framework device type name has no such naming convention. However, neither the Cisco Unified Personal Communicator device type name nor the Cisco Unified Client Services Framework device type name can exceed 15 characters. In addition, the Cisco Unified Personal Communicator device type cannot contain characters other than uppercase letters and numbers. By contrast, Cisco Unified Client Services Framework device type names can contain uppercase letters, lowercase letters, and numbers.

For example, if you were to configure the user Joe Public with a UCM user name of jpublic, the softphone device name associated with the Cisco Unified Personal Communicator device type would be UPCJPUBLIC. Similarly, the user name of j_public or j.public would have an associated softphone device name of UPCJPUBLIC. If two UCM user names are similar enough to result in identical softphone device names, softphone registration problems can occur in UCM. Therefore, it is important to be aware of the Cisco Unified Personal Communicator naming convention when you are assigning user names and configuring softphone devices.

You can configure a softphone device in UCM by clicking Device > Phone > Add New in the UCM administrative graphical user interface (GUI) and selecting either Cisco Unified Personal Communicator or Cisco Unified Client Services Framework from the Phone Type dropdown field. You must configure the Phone Type field with Cisco Unified Personal Communicator if the user is using Unified Personal Communicator version 7.0. You must configure the Phone Type field with Cisco Unified Client Services Framework if the user is using Unified Personal Communicator version 8.0 or later.

Reference:

Cisco: Configuring Basic Features for Cisco Unified Personal Communicator: (Cisco Unified Personal Communicator Release 8.x) Guidelines for Configuring the Softphone Device Name

QUESTION 18

Users are reporting garbled voice mail message recordings left by callers from the PSTN.

Which of the following actions should you perform first?

- A. Confirm that the connection to the caller is clear.

- B. Obtain a sniffer capture at the closest point to Unity Connection.
- C. Use network analysis tools to check for latency and packet loss.
- D. Modify the target decibels configured in AGC.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When troubleshooting garbled voice mail message recordings left by callers from the public switched telephone network (PSTN), you should first confirm that the connection to the caller is clear. For example, a voice mail message could become garbled if a mobile phone caller is traveling through an area with a weak or intermittent signal. If this is the case, there is nothing you can do to solve the issue. You can confirm that the connection is clear by asking the mobile caller to place another call to the voice mail system or by placing calls to the voice mail system from other mobile phones.

If voice mail messages are still garbled when the connection is clear, you should next use network analysis tools to check for latency and packet loss. Network analysis tools enable you to determine whether the network itself is causing the garbled audio stream. For example, mismatched packet size configurations among voice devices on the network could cause packet loss or delay that might affect the quality of voice mail recordings.

As a final troubleshooting step, you should obtain a sniffer capture at the closest point of the recording to Cisco Unity Connection. This will help you determine whether the audio stream is being garbled before or after Unity Connection records it. If the stream is not garbled before Unity Connection records it, there might be a problem with Unity Connection itself.

You do not need to modify the target decibels configured in Automatic Gain Control (AGC). AGC is a Unity Connection feature that enables Unity Connection to automatically adjust the audio volume of calls. You can disable or adjust AGC settings if users report that the audio volume of voice mail recordings is always too loud or always too quiet. However, the AGC feature does not typically produce garbled recordings.

Reference:

[Cisco: Troubleshooting Guide for Cisco Unity Connection Release 8.x: Troubleshooting a Garbled Audio Stream in the Network](#)

QUESTION 19

None of your company's Cisco Jabber clients are able to automatically retrieve configurations from your company's UCM 8.6 deployment.

Which of the following is most likely the reason?

- A. A service profile has not been configured in UCM.
- B. The _cisco-uds SRV record has not been configured in DNS.
- C. Automatic configuration is not selected in Jabber's Advanced settings.
- D. The users have not been configured with the IM and Presence Service.
- E. UCM releases earlier than 9 do not support automatic configuration.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, the most likely reason that your company's Cisco Jabber clients are not able to automatically retrieve configurations is that Cisco Unified Communications Manager (UCM) releases earlier than 9 do not support the automatic configuration of Cisco Jabber clients by using service profiles. Cisco Jabber's Advanced settings dialog box features an Automatic option that allows Cisco Jabber to automatically configure itself as long as all of the following are true:

- UCM is operating at release 9 or later.
- A correct _cisco-uds Service (SRV) record has been configured on the Domain Name System (DNS) server.
- Automatic is selected in Advanced settings.
- An instant message (IM) and Presence Service profile has been configured in UCM.
- The IM and Presence Service profile has been correctly applied to end users in UCM User Management.

There is not enough information in the scenario to determine whether a service profile has not been configured, whether the DNS record is missing, whether automatic configuration is not selected, or whether the users have not been configured with the IM and Presence Service. Even if that information were provided, the UCM deployment in this scenario is running release 8.6, which does not support the automatic configuration of Cisco Jabber clients.

Reference:

[Cisco: Configure the Clients: Introduction to Client Configuration](#)

**QUESTION 20**

How many Subscriber servers can be added to a UCM cluster?

- A. one
- B. two
- C. six
- D. eight

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A Cisco Unified Communications Manager (UCM) cluster can support up to eight Subscriber servers. Subscriber servers typically handle call routing, dial tone, receiving digits, and the streaming of on-hold music in a UCM cluster. In medium to large environments, the Subscriber servers perform most of the work in connecting and maintaining calls so that the performance of the Publisher server is not hindered. A UCM cluster is an environment that contains a Publisher server and up to eight Subscriber servers. Each server in the UCM cluster has a unique configuration.

The Publisher server in a UCM cluster has two roles. It holds the master writable copy of the IBM Informix database for the cluster, and it acts as a Trivial File Transfer Protocol (TFTP) server for IP phone configuration downloads. The Publisher server is the only server that contains a writable copy of the IBM Informix database that stores directory numbers (dns), calling permissions, route plans, and other information. The Publisher server replicates the data that is stored in the master database to the Subscriber servers, all of which then store their own read-only copies of the database.

A Cisco Unified Presence (CUPS) server cluster can support up to six servers. CUPS is server software that centralizes network traffic from several different communications services so that it can all be transmitted over the same Cisco Voice over IP (VoIP) network. CUPS uses industry-standard Jabber XCP for communication between different instant messaging (IM) clients; Extensible Message and Presence Protocol (XMPP) is the protocol that establishes the IM sessions. In addition, Jabber XCP facilitates other features such as file and application sharing and video conferencing.

Reference:

[Cisco: Cisco Unified Communications System 8.x SRND: Call Processing Architecture](#)

QUESTION 21

Which of the following statements about UCM default phone button templates is not true?

- A. You cannot modify the button assignments within them.
- B. You can copy them and rename the copies to customize them.
- C. You cannot delete them.
- D. You can rename them, but doing so will automatically unassign them.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You cannot rename Cisco Unified Communications Manager (UCM) default phone button templates. However, you can rename custom phone button templates. Renaming an in-use custom phone button template will not break the relationship between that template and its assigned phones. Each phone that has been assigned to that custom template will use that template under its new name.

A phone button template is a UCM feature that enables the application of a configuration for many phones within an organization without configuring each phone individually. Cisco IP phones have standard, or default, phone button templates that can be applied to configure phones with default button settings. The standard phone button template that can be applied to a given IP phone depends on the model of the IP phone.

You cannot modify the button assignments within default phone button templates. However, you can copy default phone button templates and rename the copies to customize them. It is possible to reassign the buttons on an IP phone to functions that differ from the standard phone button template that was originally applied to the phone. Although you cannot modify the buttons on a default phone button template, you can copy the default template and rename the copy, which enables you to base a custom phone button template on a default template.

You cannot delete default phone button templates, even if the default template is not assigned to a phone. You can delete custom phone button templates as long as the custom template is not assigned to any phones and is not the only template for the given model of IP phone.

Reference:

[Cisco: Cisco Unified IP Phones: Phone Button Templates](#)

QUESTION 22

Which of the following can you display by clicking System Reports > CDR Error in the UCM 8.0 CAR GUI?

- A. the current number of billing errors
- B. the call volume for a given period of time
- C. malicious call details
- D. QoS rating information for inbound calls
- E. Route and Line Group Utilization information
- F. the top number of users by maximum length of calls

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can view information about the current number of billing errors by using the System Reports > CDR Error report in the Cisco Unified Communications Manager (UCM) Call Detail Records (CDR) Analysis and Reporting (CAR) graphical user interface (GUI). This report enables a CAR administrator to view the number of errors that occurred when CDR data was loaded into the reporting system.

You can view information about the call volume for a given period of time by using the System Reports > Traffic > Summary by Phone Number report in the UCM CAR GUI. This report enables a CAR administrator to choose a range of time and IP phone extension numbers from which to view call volume information, thereby enabling an administrator to view what extensions were in use at a specific time.

You can view malicious call details by using the System Reports > Malicious Call Details report in the UCM CAR GUI. This report enables a CAR administrator to view call information that is tracked by the UCM Malicious Call Identification (MCID) service. An administrator can choose to view MCID information over a period of time.

You can view Quality of Service (QoS) rating information for inbound calls by using the System Reports > QoS > Detail report in the UCM CAR GUI. The Detail report enables a CAR administrator to choose a UCM network and a period of time for which to view QoS ratings for both inbound and outbound calls. The Detail report can be used to monitor QoS at a user level.

You can display the Route and Line Group Utilization report by using Device Reports > Route Patterns/Hunt Pilots in the UCM CAR GUI. This report enables a CAR administrator to view Route and Line Group Utilization as a percentage; the report can also be used to determine whether capacity needs to be added to an existing Voice over IP (VoIP) implementation.

You can view information about the top number of users by maximum length of calls by using the User Reports menu. The By Duration report can be accessed by clicking User Reports > Top N in the UCM CAR GUI. This report enables a CAR administrator to view users who have made the longest calls over a given period of time, starting with the user who placed the longest call.

Reference:

Cisco: Understanding CAR System Reports: System Reports Summary Description

Cisco: Configuring Traffic System Reports: Configuring Traffic Summary by Phone Number Reports

QUESTION 23

Which of the following is not a benefit of integrating LDAP with UCM?

- A. LDAP users are automatically provisioned in UCM.
- B. LDAP users can be authenticated to UCM by using LDAP passwords.
- C. UCM applications can perform LDAP user lookups.
- D. LDAP passwords can be synchronized with UCM application users.



<https://vceplus.com/>

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Lightweight Directory Access Protocol (LDAP) passwords cannot be synchronized with Cisco Unified Communications Manager (UCM) application users. LDAP synchronization with UCM does not apply to application users. For example, users of the Cisco Unified Personal Communicator application are manually provisioned by using the UCM graphical user interface (GUI) and cannot be created or managed automatically through the corporate directory like UCM users can be.

LDAP users being automatically provisioned in UCM is a benefit of integrating LDAP with UCM. When UCM is configured to synchronize with an LDAP directory, such as OpenLDAP or Microsoft Active Directory, the user ID and all user personal and organizational data that is stored in the LDAP directory, except for passwords, are replicated to the UCM database. It is important to note that the Cisco Directory Synchronization (DirSync) service must be activated before LDAP synchronization can take place.

When LDAP synchronization is configured, UCM configures the synchronized data as read-only data and acknowledges the LDAP directory as the central authority for creating and deleting user accounts. Therefore, UCM prevents administrators from using the UCM GUI to add and delete users. None of the data that was replicated to the UCM database can be modified by using the GUI. However, UCM user data that is not managed by the LDAP directory, such as the user's password and personal identification number (PIN), can be modified in the UCM administrative GUI.

The ability for Cisco UCM applications, such as Unified Personal Communicator, to perform LDAP user lookups is a benefit of integrating LDAP with UCM. When LDAP directory lookups are enabled, not only can a Unified Personal Communicator client search for and view information in the LDAP directory, but the client can also add contacts from the LDAP directory to contact lists. Administrators can configure a limitless number of LDAP custom filters in UCM Administration to filter the results of LDAP searches.

LDAP users being authenticated to UCM by using LDAP passwords, which is also known as single sign-on (SSO), is a benefit of integrating LDAP with UCM. Although user personal and organizational data is not synchronized with the LDAP directory and can be modified separately from the LDAP directory, you can

change the user password only by using the LDAP directory's change-password tool. When a user attempts to authenticate with UCM, the user's credentials are passed to the LDAP directory authentication service. If the credentials are correct, the user is authenticated and permitted to log in to the UCM GUI.

Reference:

[Cisco: LDAP Directory Integration: LDAP Authentication](#)

[Cisco: LDAP Directory Integration: LDAP Synchronization](#)

QUESTION 24

All of your department's IP phones are connected to the same Cisco Catalyst switch. The switch acts as a DHCP server for the voice VLAN. Another administrator power cycles the switch without warning. No calls are in progress.

Which of the following is most likely to occur? A.

The IP phones will reset.

B. The IP phones will disconnect but retain IP configuration information.

C. The IP phones will disappear from the UCM configuration.

D. The IP phones will not be affected by the power cycle.

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Explanation:

Most likely, the IP phones will all reset when the administrator power cycles the switch. When an IP phone is disconnected from Cisco Unified Communications Manager (UCM), the phone will automatically reset in an attempt to reestablish communication. Therefore, if an IP phone suddenly resets or is continuously attempting to register with UCM, it is important to first verify the phone's connectivity to the network switch.

The IP phones will disconnect but will not retain IP information. In this scenario, the IP phones receive their IP configurations from the Dynamic Host Configuration Protocol (DHCP) server that is running on the Cisco Catalyst switch that has been power cycled. When the IP phones reset, they will lose IP configuration information that was obtained from the DHCP server. Similarly, the IP phones will not be able to download configuration files from the Trivial File Transfer Protocol (TFTP) server until connectivity to the switch is restored.

The IP phones will not disappear from the UCM configuration. You can verify that an IP phone exists in the UCM by clicking Device > Phone > Find in UCM Administration and searching for the particular IP phone's Media Access Control (MAC) address. The IP phone will no longer be registered with UCM when it loses connectivity. However, the IP phone's record in the UCM configuration will remain there.

The IP phones will be affected by the power cycle. In addition to registration problems, IP configuration problems, and TFTP configuration problems, IP phones that are powered directly from the Cisco Catalyst switches by using Power over Ethernet (PoE) will not be able to receive power until the switch has restarted.

Reference:

[Cisco: Troubleshooting the Cisco Unified IP Phone: General Troubleshooting Tips for the Cisco Unified IP Phone](#)

QUESTION 25

Your supervisor provides you with a file named users.csv and asks you to add the user accounts from that file to Cisco Unity Connection.

Which of the following tools will you most likely use to accomplish your task?

- A. AXL Web Service
- B. BAT
- C. DirSync
- D. manual entry

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You will most likely use the Cisco Bulk Administration Tool (BAT) to import, or onboard, Cisco Unity Connection users from a file named users.csv. You can access the BAT by clicking Tools > Bulk Administration Tool in the Unity Connection graphical user interface (GUI).

To import users from a comma-separated values (CSV) file, you should first click the Create radio button in the Select Operation area of the BAT. You can also choose Update, Delete, or Export operations from this area, depending on the operation you want the BAT to perform. The Update operation modifies existing user accounts based on the information in the CSV file. The Delete operation deletes existing user accounts based on the information in the CSV file. The Export operation outputs existing user accounts to a CSV file in CSV format.

After you have selected an operation, you should select a type of user to create from the Select Object Type area of the BAT. There are four user types you can create by using the BAT: Users, Users with Mailbox, System Contacts, and Users from LDAP Directory.

In the Override CSV Fields When Creating User Accounts area of the BAT, you can choose either to override CSV-imported fields with default fields from a Unity Connection user template or to allow the direct import of the information from all the fields that are contained within the CSV file you want to import.

After you have configured all the information above, you should click the Browse button in the Select File area to choose the CSV file you want to import. You should also configure a separate CSV file name in the Failed Objects Filename field; the created file stores records that fail during the import process. The file name you configure in the Failed Objects Filename field should be descriptive and different from the name of the file you want to import. For example, if the name of the file you want to import is users.csv, you could name the failed objects file userserr.csv, or something similar. To help troubleshoot CSV import errors, you should review the information in the failed objects file after you have attempted an import. You can review the failed objects file by clicking the Download the Failed Objects File link on the BAT import summary screen.

When you are ready to import the CSV file, click the Submit button to start the import process. Once the import process is complete, the BAT will display the import summary screen.

You cannot use the Cisco Administrative XML Layer (AXL) Web Service to import Unity Connection users from a file named users.csv. The Cisco AXL Web Service is used to import Cisco Unified Communications Manager (UCM) users into Unity Connection. The service must be enabled on both UCM and Unity Connection in order to import users. In addition, UCM users must be assigned a primary extension in UCM in order to be imported into Unity Connection by AXL.

You cannot use the Cisco Directory Synchronization (DirSync) service to import Unity Connection users from a file named users.csv. The DirSync service enables Unity Connection to synchronize with Lightweight Directory Access Protocol (LDAP) directory services, such as Microsoft Active Directory. To enable synchronization between Unity Connection and an LDAP directory, you must select the Cisco DirSync check box in the Directory Services area of the Unity Connection GUI. Because Unity Connection stores users locally, a user that is synchronized with Unity Connection from LDAP will continue to be stored locally even if that user is later deleted from the LDAP database.

You would not use manual entry to import Unity Connection users from a file named users.csv. Although you can manually create new users in Unity Connection, manually parsing and populating the new user information from the CSV would be time-consuming and prone to human error.

Reference:

[Cisco: Managing Cisco Unity Connection 8.x User Accounts in Bulk: Using the Cisco Unity Connection 8.x Bulk Administration Tool to Manage User Accounts and Contacts](#)

[Cisco: Using the Cisco Unity Connection 8.x Bulk Administration Tool: Creating User Accounts in Cisco Unity Connection 8.x](#)

QUESTION 26

Which of the following is true of the Cisco Unified Serviceability System Overview report?

- A. It cannot contain a complete set of system reports.
- B. It can only be generated automatically.
- C. It is only available to CAR administrators.
- D. It does not contain traffic summary reports.



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Cisco Unified Serviceability System Overview Report is only available to Call Detail Records (CDR) Analysis and Reporting (CAR) administrators. There are three CAR user levels: administrators, managers, and individual users. Only administrators can generate system reports. Managers can generate user reports, department reports, and Quality of Service (QoS) reports. Users can generate a billing report for calls by each user.

The System Overview report can contain a complete set of system reports. In addition, the System Overview report can be generated manually. CAR administrators can choose which automatically or manually generated system reports will appear on the System Overview report by clicking Tools > CDR Analysis and Reporting > System Reports > System Overview in Cisco Unified Serviceability and then selecting the appropriate reports in the System Overview window.

The System Overview report contains all of the following sections:

- Top 5 Users based on Charge: lists the five users whose calls have cost the most over a given period of time
- Top 5 Destinations based on Charge: lists the five called numbers that have cost the most over a given period of time
- Top 5 Calls based on Charge: lists the five calls that have cost the most over a given period of time
- Top 5 Users based on Duration: lists the five users who have spent the most time on calls over a given period of time
- Top 5 Destinations based on Duration: lists the five called numbers on which users have spent the most time over a given period of time

- Top 5 Calls based on Duration: lists the five longest calls over a given period of time
- Traffic Summary Report -Hour of Day: displays the volume of calls for a given hour of the day
- Traffic Summary Report -Day of Week: displays the volume of calls for a given day of the week
- Traffic Summary Report -Day of Month: displays the volume of calls for a given day of the month
- Quality of Service Report -Summary: displays the number of calls that fell within QoS parameters over a given period of time
- Gateway Summary Report: displays the call classification, QoS, duration, and number of calls for each voice gateway over a given period of time

Reference:

Cisco: Configuring System Overview System Reports (PDF)

QUESTION 27

Which of the following devices is not supported by UCM's call preservation feature?

- A. a Cisco IP phone
- B. an annunciator
- C. a transcoder
- D. a Cisco VG248 Analog Phone Gateway

Correct Answer: B

Section: (none)

Explanation



Explanation/Reference:

Explanation:

Of the available choices, an annunciator is not supported by Cisco Unified Communications Manager's (UCM's) call preservation feature. The call preservation feature enables some Voice over IP (VoIP) devices to continue active sessions even if UCM fails or communication between UCM and the device is interrupted. An annunciator is a Skinny Call Control Protocol (SCCP) device that can play recorded messages or tones to other VoIP devices. Annunciators are often used to inform callers about the reason for a call's failure.

Cisco IP phones, transcoders, and the Cisco VG248 Analog Phone Gateway are all supported by UCM's call preservation feature. When a UCM server fails, other UCM servers and supported devices in a cluster can detect the failure. UCM is then able to ensure that active calls remain active until either the users hang up or media stops streaming between the devices. Similarly, if UCM does not fail but loses connectivity to a device that is involved in an active call, both UCM servers and connected devices will detect the failure. The active call will remain active until the users end the call or media stops streaming between the devices.

When a supported device other than UCM fails, that device will no longer stream media. Thus the device is no longer able to participate in its active call. However, UCM will detect this failure and any other devices that might have been active on the same call will remain connected and active.

Reference:

Cisco: Device Support: Call Preservation

QUESTION 28

A user presses an IP phone softkey labeled QRT.

Which of the following is the user most likely attempting to do?

- A. generate a troubleshooting report for the administrator
- B. generate local status messages
- C. view call statistics for an in-progress call on the IP phone
- D. view call statistics for a disconnected call on the IP phone

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, the user is most likely attempting to generate a troubleshooting report for the administrator by pressing an IP phone softkey labeled QRT. The Cisco Quality Report Tool (QRT) can be configured as an extended function to enable users to send QRT information to Cisco Unified Communications administrators directly from the user's IP phone. The report can then be displayed from the Tools menu within Cisco Unified Serviceability.

The QRT tool collects a variety of available source device information, destination device information, Real-time Information Server (RIS) information, Cisco CallManager service and CTIManager service information, CallManager database information, and end-user information when a user presses the QRT softkey. An administrator can then analyze that information to troubleshoot quality issues or other issues that occurred during a given call.

A user would not press the QRT softkey to generate local status messages. To generate local status messages, the user can press settings > Status > Status Messages on the IP phone.

A user would not press the QRT softkey to view call statistics for an in-progress call on the IP phone. To view call statistics for an in-progress call, the user can press the IP phone's help button twice while the call is in progress.

A user would not press the QRT softkey to view call statistics for a disconnected call on the IP phone. To view call statistics for a disconnected call, the user can press settings > Status > Call Statistics on the IP phone.

Reference:

[Cisco: Quality Report Tool: Understanding Quality Report Tool \(QRT\)](#)

QUESTION 29

You connect Ethernet Port A on a Cisco TelePresence MCU 5300 Series device to the network. The device is currently using the default settings. A DHCP server exists on the network.

Which of the following will be displayed when you issue the status command?

- A. The default static IPv4 address will be displayed.
- B. The default static IPv6 address will be displayed.
- C. A dynamic IPv4 address will be displayed.
- D. A dynamic IPv4 address and a dynamic IPv6 address will be displayed.

E. No address will be displayed.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A dynamic IP version 4 (IPv4) address will be displayed when you issue the status command on the Cisco TelePresence multipoint control unit (MCU) 5300 Series device. By default, Ethernet Port A is configured to use a dynamically assigned IPv4 address from a Dynamic Host Configuration Protocol (DHCP) server. Although IPv6 addressing is disabled by default, the MCU supports both IPv4 and IPv6 addressing.

To configure Ethernet Port A to use a static IPv4 address on Ethernet Port A, you should issue the static A ip-address subnet-mask [default-gateway] command. To configure Ethernet Port A to receive an IPv4 address from a DHCP server, you should issue the dhcp 4 A command.

Reference:

[Cisco: Cisco TelePresence MCU 5300 Series: Getting started](#) (PDF)

QUESTION 30

Which of the following is true of a CUPS ad-hoc chat room?

- A. The room cannot be created or managed by users.
- B. Users cannot invite other users to the room.
- C. The presence status of users cannot be viewed in the room.
- D. The room is deleted when the last user logs out.



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A Cisco Unified Presence (CUPS) ad-hoc chat room is deleted when the last user logs out. CUPS maintains no records or transcripts related to the ad-hoc chat room. There are two types of CUPS chat rooms: ad-hoc and persistent. Ad-hoc chat rooms are temporary. Persistent chat rooms are always available in CUPS, even after all users have logged out. Support for persistent chat rooms must be specifically enabled when configuring CUPS.

Another difference between ad-hoc chat rooms and persistent chat rooms is that persistent chat rooms enable the recording of transcripts of the discussions that occur within the room. Persistent chat rooms therefore enable users to collaborate on and store information about long-term collaborative projects by using CUPS instant messaging (IM) and Presence.

Both ad-hoc chat rooms and persistent chat rooms can be created or managed by users. In addition, both ad-hoc chat rooms and persistent chat rooms allow users to invite other users to the room. Finally, users can view the presence status of other users in a CUPS chat room regardless of the type of chat room.

Reference:

Cisco: Configuring Chat on Cisco Unified Presence: Chat Rooms on Cisco Unified Presence
www.vceplus.com - Free Questions & Answers - Online Courses - Convert VCE to PDF - VCEplus.com

QUESTION 31

The IP phone at extension 1001 is not a member of any pickup group. The IP phone at extension 1101 is a member of pickup group 5001 and is currently ringing.

Which of the following call pickup methods can be used by the phone at extension 1001 to answer the call from extension 1101?

- A. Local Group Pickup
- B. Directed Call Pickup
- C. Different Group Pickup
- D. The phone cannot answer a call ringing on another phone if it has not been assigned to a pickup group.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The IP phone at extension 1001 can use the Directed Call Pickup method to answer the call from extension 1101 in this scenario. Call Pickup is a Cisco Unified Communications Manager Express (CME) feature that enables a user at one IP phone to answer a call that is ringing on another IP phone.

There are three ways that a user in a CME environment can answer calls that are ringing on other phones: Local Group Pickup, Directed Call Pickup, and Different Group Pickup. With Local Group Pickup, a member of a pickup group can press the appropriate softkey and then dial an asterisk (*) to pick up a call from another phone within the same group. The softkey used, typically either GPickUp or PickUp, is dependent on the CME configuration. With Different Group Pickup, a member of one pickup group can press the appropriate softkey and then dial the group number of the ringing phone from a different pickup group to pick up that call. With Directed Call Pickup, any phone can be used to press the appropriate softkey and to dial the directory number (dn) of a ringing phone to answer that call.

The IP phone at extension 1001 cannot use Local Group Pickup, nor can it use Different Group Pickup. An IP phone must be assigned to a pickup group in order to use either of those methods to answer a call ringing on another phone. However, a phone does not have to be assigned to a pickup group in order to use the Directed Call Pickup feature of CME.

Reference:

[Cisco: Configuring Call-Coverage Features: Call Pickup](#)

QUESTION 32

Which of the following is a client-side application that enables an administrator to monitor devices on a Cisco VoIP network in real time by using HTTPS?

- A. CAR
- B. RTMT
- C. Unified Serviceability
- D. Unified Reporting

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Cisco Unified Real-time Monitoring Tool (RTMT) is a client-side application that enables an administrator to monitor devices on a Cisco Voice over IP (VoIP) network in real time by using Secure Hypertext Transfer Protocol (HTTPS). RTMT uses HTTPS to connect to VoIP devices and gather information, such as device status and performance statistics, in real time. The data that is gathered by RTMT can then be used to pinpoint problems on the VoIP network or to monitor performance thresholds.

To access RTMT, you should first ensure that the Cisco RTMT Reporter Servlet and Cisco Serviceability Reporter services are running in the Cisco Unified Communications Manager (UCM) environment. Next, you should install the RTMT plugin on a workstation by clicking Application > Plugins in the UCM administrative graphical user interface (GUI). After you have installed the plugin, you should launch the Real-time Monitoring Tool application on the workstation, type the appropriate IP address and credential information for accessing the UCM server or cluster, select the Secure Connection check box, and then click OK.

Cisco Unified Reporting is not a client-side application that enables an administrator to monitor devices on a Cisco VoIP network in real time by using HTTPS. Unified Reporting is a browser-based troubleshooting tool that uses HTTPS to access information that is provided by other reporting tools, such as RTMT and Cisco Unified Call Detail Records (CDR) Analysis and Reporting Tool (CAR). However, Unified Reporting does not provide access to feature activation tools and network service activation tools. You can access Unified Reporting by clicking Navigation > Cisco Unified Reporting from within the UCM administrative GUI or by using the HTTPS address `https://ip-address:8443/cucreports/`, where ip-address is the IP address of the UCM server or cluster. For example, after you have navigated to Cisco Unified Reporting, you could navigate to System Reports > Unified CM Data Summary > Generate Report to monitor system activities.

Cisco Unified Serviceability is not a client-side application that enables an administrator to monitor devices on a Cisco VoIP network in real time by using HTTPS. Unified Serviceability is a browser-based troubleshooting tool that uses HTTPS to access information that is provided by other reporting tools, such as RTMT and Cisco Unified CAR. In addition, Unified Serviceability provides access to several feature services that can be activated by using the Service Activation window, including database services, CDR services, and security services. You can access Unified Serviceability by clicking Navigation > Cisco Unified Serviceability from within the UCM administrative GUI, or by using the HTTPS address `https://ip-address:8443/ccmservice/`, where ip-address is the IP address of the UCM server or cluster.

CAR is not a client-side application that enables an administrator to monitor devices on a Cisco VoIP network in real time by using HTTPS. CAR generates CDR reports, Quality of Service (QoS) reports, traffic reports, and billing reports. In addition, CAR reports are not real-time reports. You can access CAR by clicking Tools > CDR Analysis and Reporting in Unified Serviceability if you are a system administrator or by using the HTTPS address `https://ip-address:8443/car/Logon.jsp`, where ip-address is the IP address of the UCM server or cluster, if you are a CAR administrator or user.

Reference:

Cisco: Understanding Cisco Unified RTMT: Understanding Cisco Unified Real-time Monitoring Tool

QUESTION 33

Which of the following are functions that are often provided by an ITSP but are not typically provided by the PSTN? (Choose two.)

- A. QoS
- B. call setup and teardown

- C. audio signal compression
- D. call supervision
- E. call routing

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Quality of Service (QoS) and audio signal compression are functions that are often provided by an Internet telephony service provider (ITSP) but are not typically provided by the public switched telephone network (PSTN). ITSPs enable customers to use Voice over IP (VoIP) to make phone calls over the Internet.

QoS is a VoIP technique that ensures call quality and integrity by mitigating delay and dropped packets, which can interrupt the flow of a VoIP call. Typical QoS techniques include buffer management and the use of multiple transmission queues to separate types of multimedia packets. Because voice traffic is sent in real time, quality is critical.

Audio signal compression replaces consecutive repeating audio signals with code that instructs an endpoint to play one specific signal a given number of times. The bandwidth consumed by a call is reduced when compression is used.

Call setup and teardown, call supervision, and call routing are all functions that are provided by ITSPs and the PSTN. Call setup involves the series of events between a phone going off-hook and establishing a connection; these events include dial-tone signals and ring signals. Call supervision involves the change in the state of a line or trunk port, such as line seizure, answer, or disconnect. Call routing involves selecting the path on which a call is transported from a source endpoint to a destination endpoint. On a VoIP network, voice gateways are responsible for call routing.

Reference:

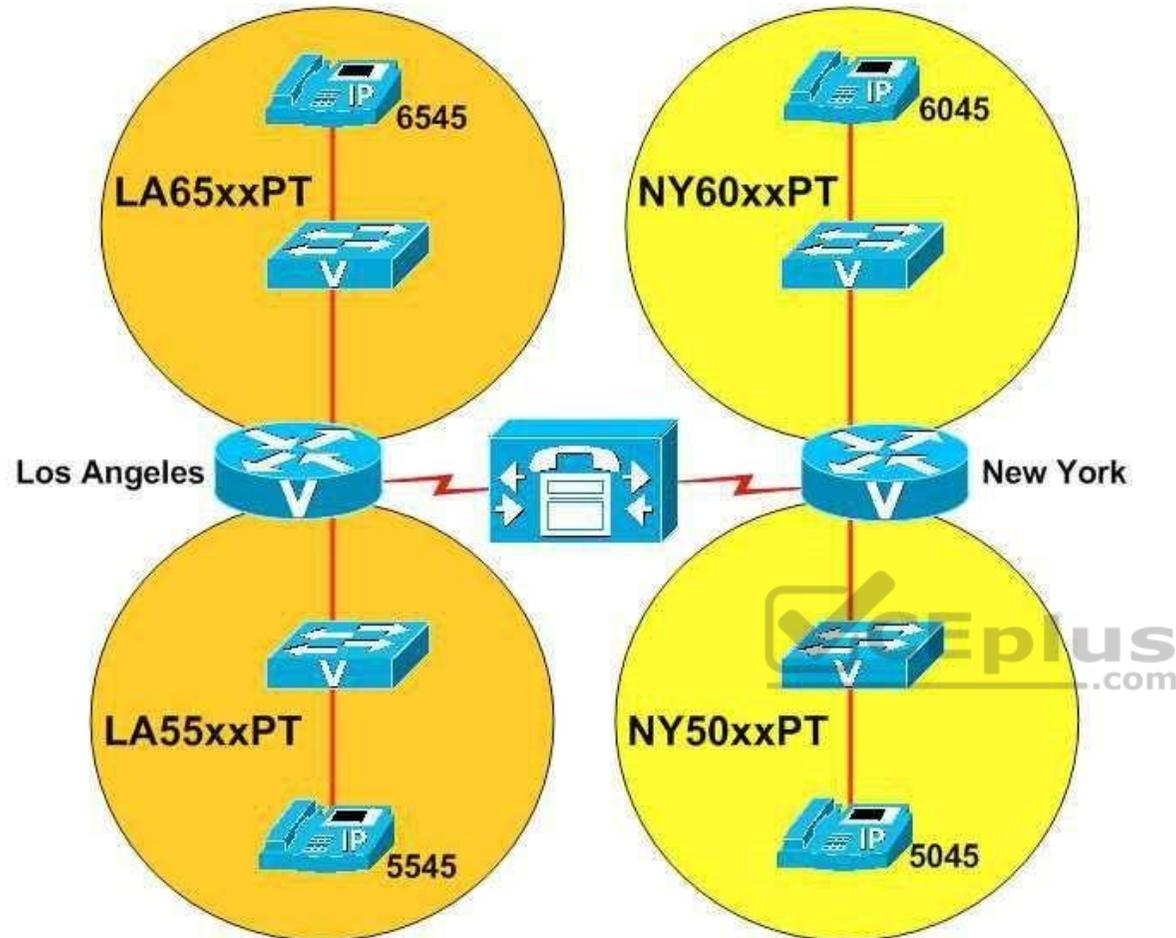
[Packetizer: Understanding VoIP: How Does VoIP Work?](#)

[Internet Telephony: The Basics of Internet Telephony](#)

[Cisco: Voice Network and Signaling Control: Signaling System 7 U.S. PSTN Features](#)

QUESTION 34

View the Exhibit.



You administer the VoIP network shown in the diagram above.

The IP phone user that has been assigned dn 5545 dials 6045 and receives a busy signal.

Which of the following is most likely the problem?

- A. The dn 6045 is listed in the <None> search space.
- B. The IP phone at 5545 is using a device search space.
- C. The IP phone at 5545 is using a line search space.
- D. The IP phone at 5545 is using a search space that does not include NY60xxPT.
- E. The IP phone at 5545 is using a search space that does not include NY50xxPT.

- F. The IP phone at 5545 is using a search space that does not include LA65xxPT.
- G. The IP phone at 5545 is using a search space that does not include LA55xxPT.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The problem is most likely that the IP phone at extension 5545 is using a search space that does not include the NY60xxPT partition. A partition is a logical grouping of Voice over IP (VoIP) route patterns and directory numbers (dns). A search space is an ordered list of partitions that a device is allowed to search for patterns that match a dialed number. A device that is not able to match a dialed number in any of the search spaces that are assigned to the device will generate a busy signal. For example, an administrator could segregate local and long distance route patterns into two partitions named LocalPT and LongDistancePT, respectively. The administrator could then assign devices that should not be able to make long distance calls to a search space named Local that includes only the LocalPT partition. Thus devices that have been assigned to only the Local search space could not make long distance calls.

In the network shown above, the NY60xxPT partition contains an IP phone that has been assigned the dn 6045. When the user at the IP phone that has been assigned the extension 5545 attempts to dial 6045, the user receives a busy signal. Therefore, it is most likely that the IP phone that has been assigned extension 5545 has not been assigned a search space that includes the NY60xxPT partition.

It is not likely a problem that the IP phone at 5545 is using a device search space. It is also not likely a problem that the IP phone at 5545 is using a line search space. A device search space is a search space that is assigned to a device itself. The information in a device search space will be searched no matter which line on a device is chosen for the outgoing call. A line search space, on the other hand, is a search space that is assigned to a single line on a device, not to the device itself. The information in a line search space will be searched when the user chooses the line to which the search space is assigned as the outgoing line for the call.

If a device is configured with both a device search space and a line search space, the device will combine the two search spaces and search the information that is contained in the line search space first. For example, if you assign the Local search space to a device and the LongDistance search space to a line on the same device, the LongDistance search space will be searched first, even if the user dials a local extension. If the same route pattern or dn exists in both search spaces, the LongDistance search space will be used to break the tie.

It is not likely that dn 6045 is listed in the <None> search space. Any VoIP endpoint can match the route pattern or dn that is contained within the <None> search space because every VoIP endpoint is assigned the <None> search space by default. The <None> search space contains the <None> partition. The <None> partition initially contains all the dns that are configured in the VoIP network. Therefore, you should move dns from the <None> partition to a custom partition to limit specific pattern matching to specific endpoints. The IP phone at 5545 would be able to call the IP phone at 6045 if 6045 were listed in the <None> search space.

It is not likely that the IP phone at 5545 is using a search space that does not include the NY50xxPT partition, does not include the LA55xxPT partition, or does not include the LA65xxPT partition. Nothing in the scenario indicates that the IP phone at 5545 is receiving a busy signal when the user attempts to dial extensions that are included in those partitions.

Reference:

Cisco: Partitions and Calling Search Spaces: Understanding Partitions and Calling Search Spaces

QUESTION 35

Which of the following interfaces handles the exchange of availability information between UCM and CUPS?

- A. AXL/SOAP
- B. LDAP
- C. SIP
- D. XMPP

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A Session Initiation Protocol (SIP) interface handles the exchange of availability information between Cisco Unified Communications Manager (UCM) and Cisco Unified Presence Server (CUPS). UCM and a CUPS server together are the primary components of a Cisco Presence deployment. A UCM SIP trunk interface must point to the CUPS server in order for availability information to be exchanged between the two systems. CUPS is also capable of sending SIP subscribe messages to UCM over the SIP trunk if UCM is configured as a Presence gateway.

The Extensible Messaging and Presence Protocol (XMPP) interface does not handle the exchange of availability information between UCM and CUPS. However, the XMPP interface is used to handle the exchange of availability information between UCM and XMPP clients, such as instant messaging (IM) clients that are developed by third parties.

The Lightweight Directory Access Protocol (LDAP) interface does not handle the exchange of availability information between UCM and CUPS. However, the LDAP interface is used to synchronize user information between UCM and CUPS in order to create a single sign-on (SSO) user experience or to perform contact searches. For example, a Cisco Unified Personal Communicator user can be authenticated to both the CUPS server and UCM by connecting directly to the CUPS server. LDAP is a directory protocol that is used by other servers, such as CUPS, to perform contact lookups. LDAP listens on Transmission Control Protocol (TCP) port 389 unencrypted or on port 636 over Secure Sockets Layer (SSL). Third-party XMPP clients can also use LDAP to search the database and add users as contacts.

The Cisco Administrative Extensible Markup Language (AXL)/Simple Object Access Protocol (SOAP) interface does not handle the exchange of availability information between UCM and CUPS. However, the AXL/SOAP interface is used to handle database synchronization tasks from UCM to the CUPS database. For synchronization to start, the Sync Agent service must be started on the CUPS server.

Reference:

[Cisco: Cisco Unified Presence Features and Functions: Cisco Unified Presence Components](#)

QUESTION 36

A user wants to adjust the contrast on a Cisco IP Phone 7961.

Which of the following should you instruct the user to do?

- A. press the help button on the IP phone

- B. press the services button on the IP phone
- C. press the settings button on the IP phone
- D. press the directories button on the IP phone

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, you should instruct the user to press the settings button on the IP phone in order to enable the user to adjust the contrast on a Cisco IP Phone 7961. The Cisco IP Phone 7961 series includes a bank of buttons with iconography designed to represent the button's functions. For example, the settings button is represented by a selected check box. The Contrast function is a user preference because it can be adjusted on a per-user basis. Therefore, the user should press settings > User Preferences > Contrast to change the contrast on the IP phone. A typical bank of buttons for a Cisco IP Phone 7961 series appears in the following exhibit:





You should not instruct the user to press the services button. The services button, which is represented by a globe icon, is used to launch IP phone applications. The applications that are available from the services button are dependent on the Cisco Unified Communications deployment and user privilege levels.

You should not instruct the user to press the directories button. The directories button, which is represented by an open book icon, is used to display lists of missed calls, received calls, placed calls, or local directory contacts. If configured, the directories button can also be used to access a custom Personal Speed Dial directory.

You should not instruct the user to press the help button. The help button, which is represented by a question mark (?), is used to provide the end user with information about the specific features of the IP phone. You can press the help button twice while on a call on an IP phone to view statistical information about the call, such as the codec that is being used by the IP phone, the codec that is being used by the calling phone, and packet error information.

Reference:

[Cisco: Cisco Unified IP Phone 7961G](#)

QUESTION 37

You deploy VoIP on an existing LAN without implementing QoS.

Which of the following issues is least likely to occur as a result?

- A. jitter
- B. packet delays
- C. packet drops
- D. VoIP hopping

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, Voice over IP (VoIP) hopping is least likely to occur as a result of a failure to implement Quality of Service (QoS) on the LAN. VoIP hopping is a form of virtual LAN (VLAN) hopping; it is a data security risk associated with VoIP devices and data devices that are connected to the same physical port on a switch. Many IP phones contain switching technology that enables an administrator to daisy chain a workstation to the phone, causing both the workstation and the IP phone to use the same physical connection to the switch.

Jitter, packet delays, and packet drops could all result from deploying VoIP on an existing LAN without implementing QoS. Jitter is a variation in delay, which can cause packets to arrive out of sequence or at a different rate than they were sent. As a result, the end user might experience choppiness in the audio connection. Thus shorter packet roundtrip times contribute to better voice quality. The effects of VoIP issues like jitter and latency on a network can be analyzed by using data analysis techniques such as Mean Opinion Score (MOS) or R-Factor.

Congested networks often cause dropped packets. Dropped packets can cause clips, or breaks, in the audio stream. However, voice traffic is more tolerant of dropped packets than of delayed packets, because a small amount of packet loss is not noticeable to the human ear. Packet loss can be mitigated by implementing QoS and congestion avoidance mechanisms, increasing bandwidth, and increasing buffer space. In addition, some codecs can correct small amounts of packet loss.



Bandwidth is also crucial to the successful deployment of a VoIP network. A lack of bandwidth can lead to issues such as serialization delay. Serialization delay is the time required to place a packet onto a medium, such as a copper or fiber-optic cable. Serialization delay is directly related to the clocking method and the bandwidth of the line.

Reference:

[Cisco: Network Infrastructure: Impairments to IP Communications if QoS is Not Employed](#)

[Symantec: VoIP Hopping: A Method of Testing VoIP security or Voice VLANs](#)

QUESTION 38

Which of the following cannot be displayed by using the CAR System Reports menu? (Choose two.)

- A. the current number of billing errors
- B. the call volume for a given period of time
- C. malicious call details
- D. QoS rating information for inbound calls
- E. Route and Line Group Utilization information
- F. the top number of users by maximum length of calls

Correct Answer: EF

Section: (none)

Explanation



Explanation/Reference:

Explanation:

You cannot display Route and Line Group Utilization information by using the Call Detail Records (CDR) Analysis and Reporting (CAR) System Reports menu. In addition, you cannot display the top number of users by maximum length of calls by using the CAR System Reports menu. CAR is a reporting system that can be used to examine a variety of statistics about a Cisco Unified Communications system, including system load and performance.

You can display Route and Line Group Utilization information by using the Device Reports menu. The Route and Line Group Utilization report can be accessed by clicking Device Reports > Route Patterns/Hunt Pilots in the Cisco Unified Communications Manager (UCM) CAR graphical user interface (GUI). This report enables a CAR administrator to view Route and Line Group Utilization as a percentage? the report can also be used to determine whether capacity needs to be added to an existing Voice over IP (VoIP) implementation.

You can display information about the top number of users by maximum length of calls by using the User Reports menu. The By Duration report can be accessed by clicking User Reports > Top N in the UCM CAR GUI. This report enables a CAR administrator to view users who have made the longest calls over a given period of time, starting with the user who placed the longest call.

You can display information about the current number of billing errors by using the System Reports > CDR Error report in the UCM CAR GUI. This report enables a CAR administrator to view the number of errors that occurred when CDR data was loaded into the reporting system.

You can display information about call volume for a given period of time by using the System Reports > Traffic > Summary by Phone Number report in the UCM CAR GUI. This report enables a CAR administrator to choose a range of time and IP phone extension numbers from which to view call volume information, thereby enabling an administrator to view what extensions were in use at a specific time.

You can display malicious call details by using the System Reports > Malicious Call Details report in the UCM CAR GUI. This report enables a CAR administrator to view call information that is tracked by the UCM Malicious Call Identification (MCID) service. An administrator can choose to view MCID information over a period of time.

You can display Quality of Service (QoS) rating information for inbound calls by using the System Reports > QoS > Detail report in the UCM CAR GUI. The Detail report enables a CAR administrator to choose a UCM network and a period of time for which to view QoS ratings for both inbound and outbound calls. The Detail report can be used to monitor QoS at a user level.

Reference:

Cisco: Understanding CAR Device Reports: Device Reports Summary Descriptions

Cisco: Understanding CAR User Reports: User Reports Summary Description

Cisco: Configuring route pattern and Hunt Pilot Device Reports: Configuring Route Pattern/Hunt Pilot Utilization Reports

Cisco: Configuring Top N User Reports: Configuring Top N by Duration Reports

QUESTION 39

You want to enable a new set of features in Cisco Unified Serviceability.

Which of the following should you do?

- A. Click Trace > Service Activation.
- B. Click Alarm > Service Activation.
- C. Click Tools > Service Activation.
- D. Click Tools > Serviceability Reports Archive > Service Activation.



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You should click Tools > Service Activation in Cisco Unified Serviceability if you want to enable a new set of features. The Service Activation option under the Tools menu enables you to select individual services to activate or select all services at once. After you have selected the services you want to enable, you should click the Save button to activate those services.

You should not click Tools > Serviceability Reports Archive > Service Activation, because the Service Activation option is not available under the Serviceability Reports Archive option. However, you can access the Service Statistics Report by navigating to Tools > Serviceability Reports Archive in Cisco Unified Serviceability. The Cisco Unified Serviceability Reports Archive contains all of the following types of statistical reports:

- Device Statistics Report
- Server Statistics Report
- Service Statistics Report
- Call Activities Report
- Alert Summary Report

-Performance Protection Report

You should not click Alarm > Service Activation, because the Service Activation option is not available under the Alarm menu. The Cisco Unified Serviceability Alarm menu helps identify problems that exist with the Cisco Unified Communications system. The Alarm menu can be used as part of the troubleshooting process.

You should not click Trace > Service Activation, because the Service Activation option is not available under the Trace menu. The Trace menu can be used to access voice application tracing tools that can be used in troubleshooting efforts.

Reference:

[Cisco: Configuring Services: Activating and Deactivating Feature Services](#)

QUESTION 40

Which of the following signaling methods can be used by FXS and FXO interfaces? (Choose two.)

- A. delay dial
- B. ground start
- C. immediate start
- D. loop start
- E. wink start



Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Loop start and ground start signaling can be used by foreign exchange station (FXS) and foreign exchange office (FXO) interfaces. An FXO interface is typically used to connect an analog device to the public switched telephone network (PSTN). In addition, if a private branch exchange (PBX) is configured with an FXS port, the FXO interface on an analog device can terminate an analog trunk from a PBX. FXO interfaces are commonly found on standard telephones, fax machines, and analog modems. Thus devices that have FXO interfaces typically connect to the PSTN by using plain old telephone service (POTS) lines.

Cisco Analog Voice Gateways, such as the VG202 and the VG204, come with FXS ports that enable you to connect FXO devices, such as corded analog telephones or cordless analog telephone bases, to Cisco Unified Communications Manager. The VG202 supports up to a maximum of two analog devices. The VG204 supports up to a maximum of four analog devices.

When a loop start phone handset is picked up, two wires are connected, which completes the electrical circuit loop. The PSTN central office (CO) detects the closed circuit and sends a dial tone to the phone. By default, FXS and FXO interfaces are configured to use loop start signaling. Loop start signaling is susceptible to a problem called glare, which occurs when an incoming call seizes the same line as an outgoing call. Although glare is not typically a problem on residential lines, it can be a problem on business lines that receive high call volumes.

Ground start signaling was developed to address the problems caused by glare on FXS and FXO interfaces. Trunk lines and PBXs typically use ground start signaling to separate incoming calls from outgoing calls. When a ground start PBX detects a phone going off-hook, the PBX grounds two wires to alert the PSTN CO that an outgoing call is about to occur.

Immediate start, wink start, and delay dial signaling are used by ear and mouth (E&M) interfaces, not by FXS and FXO interfaces. E&M interfaces have two signaling paths: an E-lead and an M-lead. When an outgoing call is made with immediate start signaling, the phone goes off-hook on the E-lead, pauses for a short time, and sends dual-tone multi-frequency (DTMF) tones or pulses to specify the call destination. Like loop start signaling, immediate start signaling is susceptible to glare.

Wink start signaling was developed to address the problems caused by glare on E&M interfaces. When an outgoing call is made with wink start signaling, the phone goes off-hook on the E-lead, waits for a pulse, or wink, to be sent over the M-lead to indicate that the line is clear, and then sends DTMF tones or pulses to specify the call destination. By default, E&M interfaces are configured to use wink start signaling.

When an outgoing call is made with delay dial signaling, the source detects whether the destination is on-hook or off-hook. If the destination is on-hook, the source sends DTMF tones or pulses to specify the call destination. If the destination is off-hook, the source will wait until the destination is on-hook before sending DTMF tones or pulses.

Reference:

Cisco: Analog Signaling: Introduction

[Cisco: Voice Port Configuration Overview: Telephony Signaling Interfaces](#)



QUESTION 41

Which of the following is not a method of upgrading firmware on Cisco IP phones?

- A. direct Internet download
- B. load server download
- C. peer firmware sharing
- D. traditional TFTP server download

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Direct Internet download is not a method of upgrading firmware on Cisco IP phones. There are many software applications and devices that, when connected to the Internet, can be configured to automatically update. However, for security and continuity reasons, Cisco IP phone updates typically fall under the authority of a Cisco Unified Communications Manager (UCM) administrator.

Both load server download and traditional Trivial File Transfer Protocol (TFTP) server download are methods of updating the firmware on Cisco IP phones. When using the traditional TFTP server download method, each IP phone independently downloads the new image from the TFTP server in an "every man for himself" style strategy. When firmware images were small, this strategy was acceptable even when the IP phones were on a network at a separate location from UCM.

Over time, IP phone firmware sizes have increased, which could cause slow upgrades over WAN links. In addition, the traditional TFTP download method could create high CPU usage on the UCM TFTP server.

You can also update the firmware on an individual IP phone by using the traditional TFTP method. First, you should make a note of the existing Phone Load Name value for the phone model you want to upgrade by navigating to Device > Device Settings > Device Defaults in UCM Administrator. This is important because installing the new firmware image will automatically overwrite the value of the Phone Load Name field in Device > Device Settings > Device Defaults. You should then upload the new firmware to UCM by navigating to Software Upgrades > Install/Upgrade.

After you upload the new firmware, specify the name of the new firmware in the Phone Load Name field for the specific IP phone that you want to upgrade by using UCM Administration's Device > Phone menu. Next, navigate to Device > Device Settings > Device Defaults and replace the new value of the Phone Load Name field with its original value. This will prevent other IP phones from downloading the new firmware after you restart the TFTP service.

Finally, you should restart the TFTP service in Cisco Unified Serviceability. After the service restarts, the IP phone you edited in UCM Administration should download the new firmware, upgrade the firmware, and restart. Other IP phones might restart as well. However, those IP phones will not be upgraded.

In contrast to the traditional TFTP server method, the load server download method enables the administrator of the LAN on which the IP phone operates to provide his or her own local TFTP server for firmware upgrades instead of relying on a remotely located default UCM TFTP server. This means that IP phones on remote networks will be able to download firmware updates in approximately the same amount of time it would take for an IP phone that is local to UCM. In addition, the TFTP load can be balanced among multiple TFTP servers at multiple sites. One disadvantage to the load server download method is that the local administrator is responsible for copying the firmware update to the TFTP server. Therefore, the TFTP upload and server configuration is subject to human error.

Peer firmware sharing is a method of updating the firmware on Cisco IP phones. When peer firmware sharing is implemented, only one Cisco IP phone at a location is responsible for downloading the new firmware. The firmware is then distributed to the other IP phones on the LAN in a parent-child hierarchy. The downloading phone distributes the firmware to its children. Those children then distribute the firmware to their children, and so on. No one parent in the hierarchy can have more than two children. Some disadvantages to the peer firmware sharing method are that the hierarchies are limited to their own subnets and are specific to phone model. In addition, peer firmware sharing must be enabled on each IP phone.

Reference:

[Cisco: Unified IP Phone Firmware Distribution Methods](#)

[Cisco: Upgrade IP Phone Firmware Individually](#)

QUESTION 42

Which of the following is not available from the Device Statistics Report in Cisco Unified Serviceability?

- A. the number of registered phones per server
- B. the number of H.323 gateways in the cluster
- C. the number of trunks in the cluster
- D. the number of open CTI lines

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The number of open Computer Telephony Integration (CTI) lines is available from the Cisco Unified Serviceability Service Statistics Report, not the Device Statistics Report. You can access the Service Statistics Report by navigating to Tools > Serviceability Reports Archive in Cisco Unified Serviceability. The Cisco Unified Serviceability Reports Archive contains all of the following types of statistical reports:

- Device Statistics Report
- Server Statistics Report
- Service Statistics Report
- Call Activities Report
- Alert Summary Report
- Performance Protection Report

Each report type contains statistical information, including charts, about the given activity. The Device Statistics Report contains information about the number of registered phones per server, the number of H.323 gateways in the cluster, and the number of trunks in the cluster.

Reference:

- Cisco: Understanding Serviceability Reports Archive: Device Statistics Report
- Cisco: Understanding Serviceability Reports Archive: Service Statistics Report

QUESTION 43

You have registered one non-Cisco IP phone with UCM. Every other IP phone on the network is a Cisco IP phone.

Which of the following statements is most likely true?

- A. Only one H.323 endpoint is registered with UCM.
- B. Only one SCCP endpoint is registered with UCM.
- C. Only one SIP endpoint is registered with UCM.
- D. Only one MGCP endpoint is registered with UCM.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most likely, only one Session Initiation Protocol (SIP) endpoint is registered with Cisco Unified Communications Manager (UCM) if you have registered one nonCisco IP phone with UCM and every other IP phone on the network is a Cisco IP phone. SIP is an Internet Engineering Task Force (IETF) standard call signaling protocol that is supported by a wide variety of IP telephony vendors. A call signaling protocol is responsible for the setup, maintenance, and teardown of a voice call. For example, call signaling protocols can detect and report when a phone is off-hook.

SIP uses a text-based signaling method, which is easier to understand and troubleshoot than the binary method used by other protocols, such as Skinny Client Control Protocol (SCCP) and H.323. For example, SIP uses text-based INVITE requests and ACK requests to invite a user to participate in a call and to acknowledge that user's response to the INVITE, respectively. Although SIP is typically used as a peer-to-peer call signaling protocol, it can also operate in client/

server mode. SIP is most commonly used by Internet telephony service providers (ITSPs). Therefore, many non-Cisco IP phones and video phones are SIP phones.

More than one SCCP endpoint would be registered with UCM in this scenario, where you registered only one non-Cisco IP phone with UCM and every other IP phone on the network is a Cisco IP phone. By default, Cisco IP phones use SCCP, which is a Cisco-proprietary client/server call signaling protocol intended to be an alternative to H.323. Although a few third-party IP phones support SCCP, SIP is more widely supported on non-Cisco IP phones. SIP can be supported by Cisco IP phones with a firmware replacement.

Neither Cisco IP phones nor third-party IP phones typically use Media Gateway Control Protocol (MGCP). MGCP is a client/server call signaling protocol. MGCP is an IETF-standard protocol that can be used on some Cisco IP phones with a firmware replacement.

Neither Cisco IP phones nor third-party IP phones typically use H.323. H.323 is an International Telecommunication Union (ITU) standard, peer-to-peer call signaling protocol. Peer-to-peer call signaling protocols do not require a call processing platform, because the voice gateways provide their own call signaling and call routing. Therefore, you would be more likely to register a non-Cisco SIP IP phone than an H.323 IP phone with UCM. Although UCM supports H.323, Cisco IP phones do not, because H.323 consumes a large amount of processor and memory resources.

Reference:

[Cisco: Chap 6: SIP Messages and Compliance Information for Cisco VoIP Infrastructure Solution for SIP: Requests](#)

QUESTION 44

Which of the following is not true of a CUPS ad-hoc chat room?



- A. The room can be created or managed by users.
- B. Users can invite other users to the room.
- C. The presence status of users can be viewed in the room.
- D. The room remains available in CUPS when the last user logs out.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A Cisco Unified Presence (CUPS) ad-hoc chat room is deleted when the last user logs out. CUPS maintains no records or transcripts related to the ad-hoc chat room. There are two types of CUPS chat rooms: ad-hoc and persistent. Ad-hoc chat rooms are temporary. Persistent chat rooms, on the other hand, are always available in CUPS, even after all users have logged out. Support for persistent chat rooms must be specifically enabled when configuring CUPS.

Another difference between ad-hoc chat rooms and persistent chat rooms is that persistent chat rooms enable the recording of transcripts of the discussions that occur within the room. Persistent chat rooms therefore enable users to collaborate on and store information about long-term collaborative projects by using CUPS instant messaging (IM) and Presence.

Both ad-hoc chat rooms and persistent chat rooms can be created or managed by users. In addition, both ad-hoc chat rooms and persistent chat rooms allow users to invite other users to the room. Finally, users can view the presence status of other users in a CUPS chat room regardless of the type of chat room.

Reference:

Cisco: Configuring Chat on Cisco Unified Presence: Chat Rooms on Cisco Unified Presence

QUESTION 45

Which of the following tasks cannot be automatically synchronized when an LDAP directory is integrated with UCM?

- A. user provisioning
- B. user password creation
- C. user authentication
- D. user lookups

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

User passwords cannot be automatically synchronized when a Lightweight Directory Access Protocol (LDAP) directory is integrated with Cisco Unified Communications Manager (UCM). When UCM is configured to synchronize with an LDAP directory, such as OpenLDAP or Microsoft Active Directory, the user ID and all user personal and organizational data that is stored in the LDAP directory, except for passwords, are replicated to the UCM database. It is important to note that the Cisco Directory Synchronization (DirSync) service must be activated before LDAP synchronization can take place.

When LDAP synchronization is configured, UCM configures the synchronized data as read-only data and acknowledges the LDAP directory as the central authority for creating and deleting user accounts. Therefore, UCM prevents administrators from using the UCM graphical user interface (GUI) to add and delete users. None of the data that was replicated to the UCM database can be modified by using the GUI. However, UCM user data that is not managed by the LDAP directory, such as the user's password and personal identification number (PIN), can be modified in the UCM administrative GUI.

User lookups can be automatically synchronized when the LDAP directory of an organization has been integrated with UCM. When LDAP directory lookups are enabled, not only can UCM applications users, such as a Cisco Unified Personal Communicator client, search for and view information in the LDAP directory, but they can also add to their contact lists from the LDAP directory. Administrators can configure a limitless number of LDAP custom filters in UCM Administration to filter the results of LDAP searches.

User authentication can be automatically synchronized when the LDAP directory of an organization has been integrated with UCM. When a user attempts to authenticate with UCM, the user's credentials are passed to the LDAP directory authentication service. If the credentials are correct, the user is authenticated and permitted to log in to the UCM GUI.

User provisioning can be automatically synchronized when the LDAP directory of an organization has been integrated with UCM. When UCM is integrated with LDAP, provisioning a user in LDAP will automatically add that same user account to UCM. Having this integration prevents the administrator from having to make manual adjustments in two locations in the event that an account needs to be modified, created, or removed.

Reference:

[Cisco: LDAP Directory Integration: LDAP Authentication](#)

[Cisco: LDAP Directory Integration: LDAP Synchronization](#)

QUESTION 46

View the Exhibit.



Based on the network topology above, which of the following command sets could you issue on Router1 so that calls are routed to Phone2?

- A. dial-peer voice 1 voip
destination-pattern 555.... port
1/0/0
- B. dial-peer voice 1 pots
destination-pattern port
1/0/0
- C. dial-peer voice 1 voip
destination-pattern 555....
port 1/0/1
- D. dial-peer voice 1 pots
destination-pattern 5550717
port 1/0/1



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You could issue the following command set on Router1 so that calls are routed to Phone2:

```
dial-peer voice 1 pots
destination-pattern .....
port 1/0/0
```

The dial-peer voice tag [pots | voip] command is used to define how calls are routed to destination endpoints on either the public switched telephone network (PSTN) or a Voice over IP (VoIP) network. To define call routing for the PSTN, you should issue the dial-peer voice command with the pots keyword. The tag value is any number in the range from 1 through 2147483647 that you assign to the dial peer as an identifier. To define call routing for a VoIP network, you should issue the dial-peer voice command with the voip keyword. In this scenario, Phone2 is connected to the PSTN. Therefore, dial peer 1 should be configured as a pots dial peer.

The destination-pattern command is used to match both inbound and outbound dial peers. The sequence of dialed digits that will be matched for a dial peer can contain the digits 0 through 9, the asterisk (*), and the pound sign (#). In addition, you can use a period (.) as a wildcard symbol to refine the dialing pattern or to match multiple dial strings for a single dial peer. In the command set above, dial peer 1 is configured to match destinations that contain seven digits. Each digit in the pattern is represented by a single .wildcard. Phone2 is addressed with a seven-digit telephone number; therefore, the dial peer's destination-pattern command should be configured to match a sevendigit pattern.

The port command is used by a voice router to match inbound plain old telephone service (POTS) dial peers and to determine where to route outgoing POTS dial peers. In this scenario, the Cisco Unified Communications Manager Express (CME) router port connected to the PSTN is foreign exchange office (FXO) port 1/0/0. Therefore, the dial peer should be configured to send traffic from Router1 destined for Phone2 through port 1/0/0.

Issuing the following command set on Router1 will not route calls to Phone2:

```
dial-peer voice 1 voip  
destination-pattern 555....  
port 1/0/0
```

Although the destination-pattern command will match the Phone2 telephone number and the port command is configured for the port on Router1 that is connected to the PSTN, the dial-peer voice command has been issued with the voip keyword. Phone2 is connected to the PSTN, not to the VoIP network. In addition, the session target command, not the port command, must be issued to route a voip dial peer. The session target command configures a dial peer with a network address for routing voice traffic over an IP network. The network address can be an IP address or a host name, depending on whether a Domain Name System (DNS) server is configured and available to resolve host names.

Issuing the following command set on Router1 will not route calls to Phone2:

```
dial-peer voice 1 voip  
destination-pattern 555....  
port 1/0/1
```

Although the destination-pattern command will match the Phone2 telephone number, the port command is configured for the foreign exchange station (FXS) 1/0/1 port on Router1, not the outbound port that is connected to the PSTN. In addition, the dial-peer voice command has been issued with the voip keyword. Therefore, the previous command set is an invalid configuration.

Issuing the following command set on Router1 will not route calls to Phone2:

```
dial-peer voice 1 pots  
destination-pattern 5550717  
port 1/0/1
```

Although the dial-peer voice command is correctly configured and the destination-pattern command will explicitly match the telephone number for Phone2, an incorrect port has been specified for the outbound traffic. The command set above would work if the port 1/0/0 command were issued instead of the port 1/0/1 command. You cannot connect an FXS port to the PSTN.

Reference:

[Cisco: Understanding Inbound and Outbound Dial Peer Matching on IOS Platforms: Non DID Case](#)

QUESTION 47

You click Administrator's Login Account in the CME GUI's Configure System Parameters menu.

Which of the following are you most likely configuring?

- A. a customer administrator
- B. an LDAP administrator
- C. a phone administrator
- D. a system administrator

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, you are most likely configuring a customer administrator if you click Administrator's Login Account in the Configure System Parameters menu. A Cisco Unified Communications Manager Express (CME) environment supports three types of users: system administrator, customer administrator, and phone user. A customer administrator account enables a reseller to give customers administrative control over some of the CME features that are available to those customers. In order for a customer administrator to log on to the graphical user interface (GUI), the system administrator must first create a customer administrator account for that user. After clicking Administrator's Login Account in the GUI, you should enter appropriate values in the Admin User Name (username) field, the Admin User Type (Customer) field, and both password fields. Finally, click the Change button to create the user.

You can also create a customer administrator by using the command-line interface (CLI). Customer administrator accounts are configured in the CLI by issuing the web admin customer name user-name password string command in telephony service configuration mode, where username is the user name you want to assign to the customer administrator and string is the password you want to associate with the user name.

You are not configuring a phone administrator. Phone users, not phone administrators, can manage IP phone settings either by using the telephone keypad or by logging on to the CME browser-based GUI. To create a phone user by using the CLI, you should issue the username user-name password password command in ephone configuration mode, where username is the user name you want to assign to the user and password is the password you want to assign to the user. You should issue the username user-name password password command only in ephone configuration mode of the device that you want to assign to the user you are creating. For example, if you want user John to be able to manage the device settings of ephone 5 by using the CME GUI, you should issue the following commands on the CME router:

```
ephone 5 username john  
password b0s0n
```

To create a phone user account in the CME GUI, you should click Configure > Phones > Add Phone in the GUI, which opens the Add Phone window. In the Login Account area of the Add Phone window, you should assign the phone user a user name and password and then associate the phone user with either an existing device or a new device. Finally, click the Change button to create the user. You can also change an existing user's password by clicking Configure > Phones in the GUI. Scroll through the list of Media Access Control (MAC) addresses in the Phone Physical ID (MAC Address) column until you find the phone you want to modify. Click on the phone you want to modify, change the password, and then click the Change button.

You are not configuring a system administrator. The system administrator account must be configured from the CLI before the system administrator account can access the GUI. You can enable GUI access for a system administrator by issuing the web admin system name admin password string command in telephony service configuration mode.

You are not configuring a Lightweight Directory Access Protocol (LDAP) administrator. You cannot directly synchronize users in an LDAP directory, such as Microsoft Active Directory, with CME. However, you can synchronize users in an LDAP directory with other Cisco Unified Communications products, such as Cisco Unity Connection.

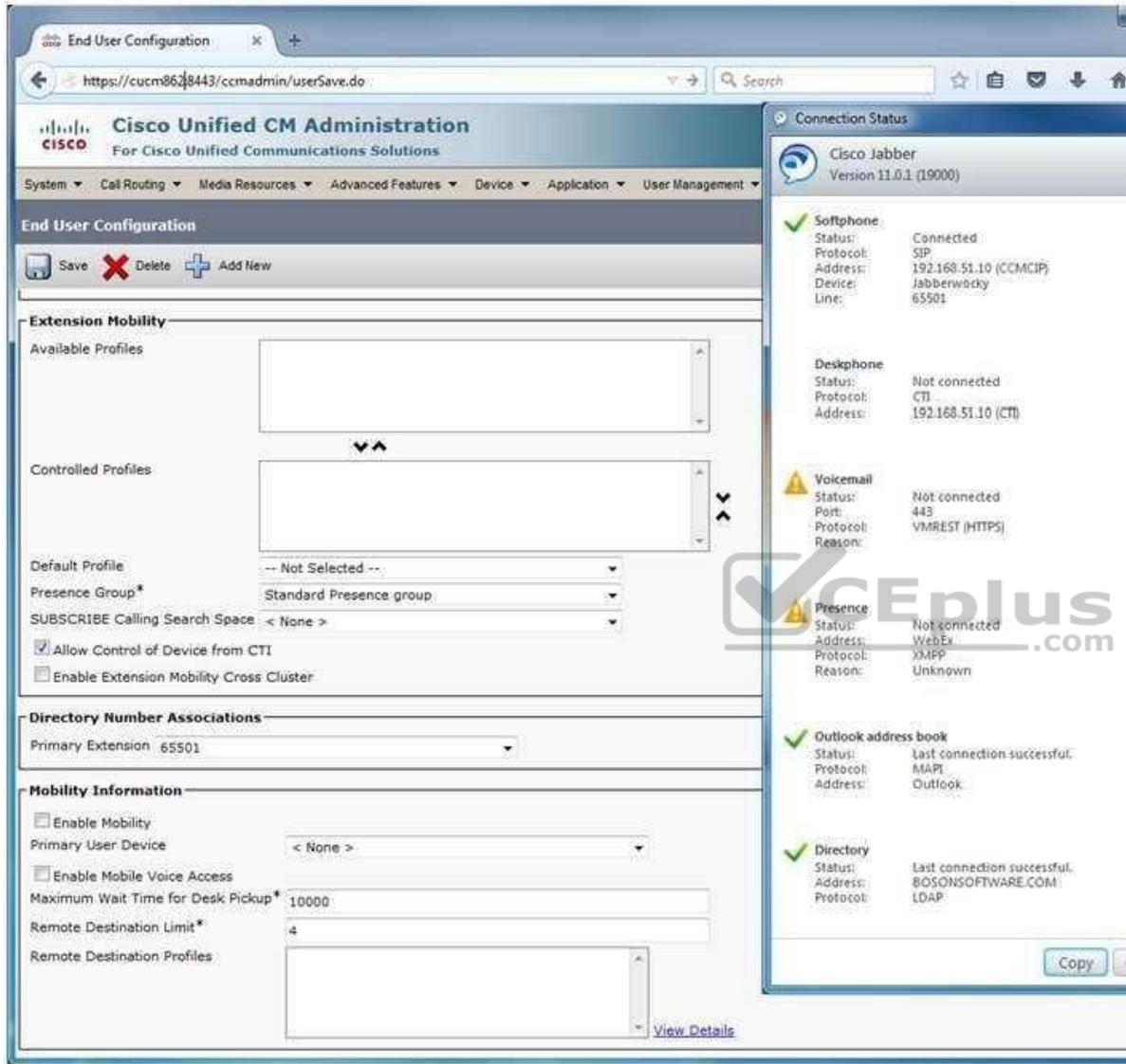
Reference:

[Cisco: Enabling the GUI: Enabling GUI Access for Customer Administrators](#)

QUESTION 48

You are the administrator for your company's UCM network. Examine the exhibit below, and answer the question:





The screenshot shows the Cisco Unified CM Administration interface for End User Configuration. The main configuration area includes:

- Extension Mobility:** Available Profiles and Controlled Profiles lists are empty. Default Profile is set to "-- Not Selected --". Presence Group is "Standard Presence group". SUBSCRIBE Calling Search Space is "< None >". The checkbox "Allow Control of Device from CTI" is checked, and "Enable Extension Mobility Cross Cluster" is unchecked.
- Directory Number Associations:** Primary Extension is set to "65501".
- Mobility Information:** "Enable Mobility" is unchecked. Primary User Device is "< None >". "Enable Mobile Voice Access" is unchecked. Maximum Wait Time for Desk Pickup is "10000". Remote Destination Limit is "4". Remote Destination Profiles list is empty.

The right-hand pane shows the **Connection Status** for the Cisco Jabber user (Version 11.0.1 (19000)):

- Softphone:** Status: Connected. Protocol: SIP. Address: 192.168.51.10 (CCMCIP). Device: Jabberwocky. Line: 65501.
- Deskphone:** Status: Not connected. Protocol: CTI. Address: 192.168.51.10 (CTI).
- Voicemail:** Status: Not connected. Port: 443. Protocol: VMREST (HTTPS). Reason: (empty).
- Presence:** Status: Not connected. Address: WebEx. Protocol: XMPP. Reason: Unknown.
- Outlook address book:** Status: Last connection successful. Protocol: MAPI. Address: Outlook.
- Directory:** Status: Last connection successful. Address: BOSONSOFTWARE.COM. Protocol: LDAP.

Which of the following is not true of the end-user configuration?

- A. The end user's primary extension is 65501.
- B. The end user is not configured to control a desk phone from Cisco Jabber.
- C. The end user can log in to a temporary IP phone as if it were a permanent workstation.

D. The end user cannot currently use Cisco Jabber for IM and Presence information.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The end user cannot log in to a temporary IP phone as if it were a permanent workstation, because Extension Mobility has not been configured for this user. Extension Mobility enables a user who works at a shared workstation to log in to and use an IP phone as if the phone were at a permanent workstation. For example, if the user programmed speed-dial options on an IP phone, those options would be stored in the user's device profile and made available to the user at any IP phone that is subscribed to Extension Mobility, as long as the user is able to log in to that IP phone.

In order for an Extension Mobility user to properly log in to and log out of an IP phone, both the IP phone and the device profile that stores the user's preferences must be subscribed to the Extension Mobility service. In this scenario, no device profile has been associated with the end user. In addition, if the IP phone is not subscribed to Extension Mobility, the user will not be able to log in to Extension Mobility from the IP phone and an error message will appear on the IP phone's display. In addition, if the Extension Mobility Uniform Resource Locator (URL) is not correctly configured in UCM, the user will not be able to log in to Extension Mobility from the IP phone and an error message will appear on the IP phone's display.

The end user cannot currently use Cisco Jabber for IM and Presence information. Cisco Jabber relies on Cisco Unified Presence (CUPS) and the Extensible Messaging and Presence Protocol (XMPP) for instant messaging (IM) and Presence functionality. However, in this scenario, Cisco Jabber is unable to connect to a CUPS server.

There is not enough information in this scenario to determine whether the end user has been configured to control a desk phone from Cisco Jabber. Based on the Connection Status window, you can determine only that the Cisco Jabber client is not currently connected to a desk phone.

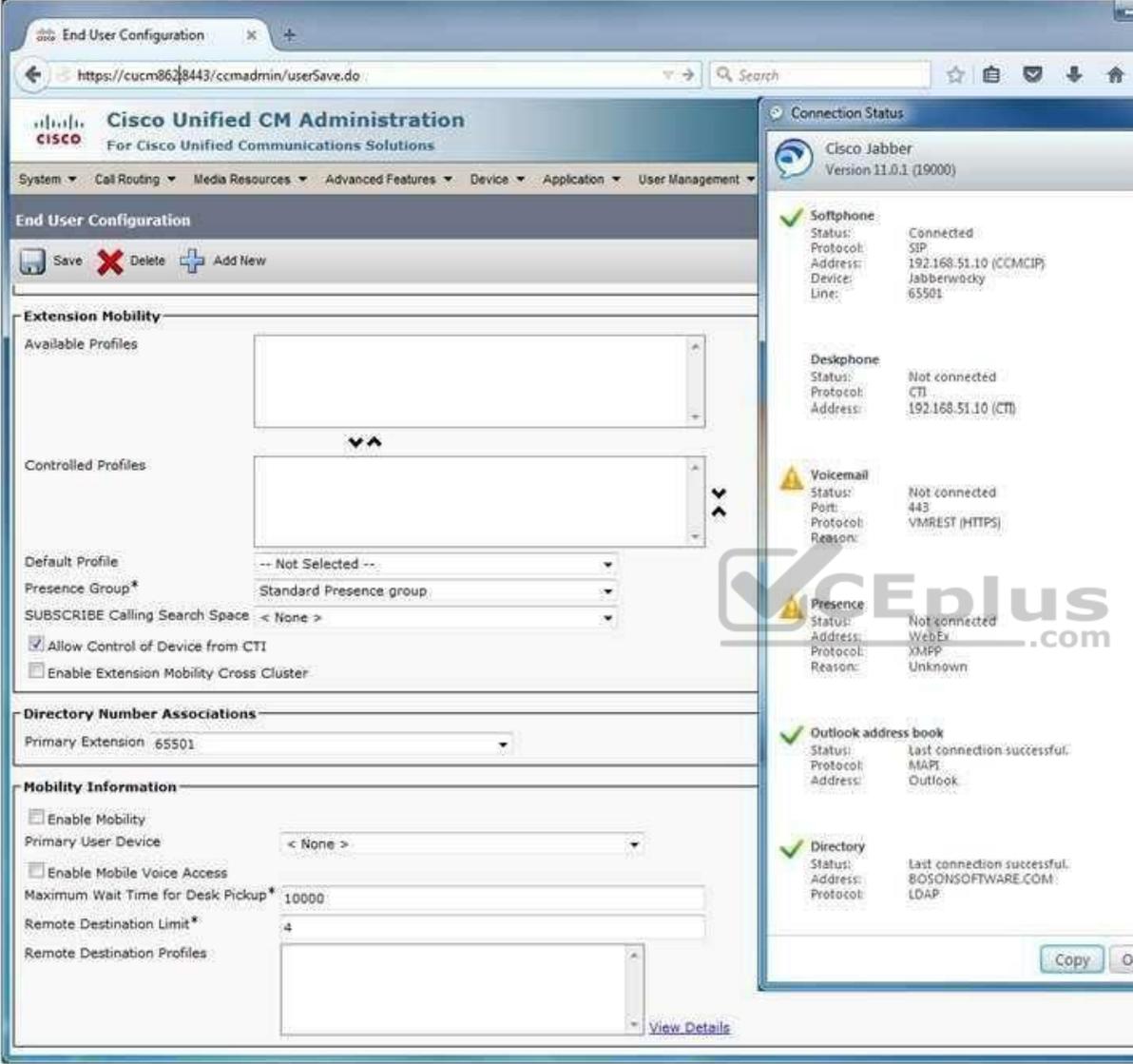
The end user's primary extension is 65501. The 65501 value has been configured in the Primary Extension field.

Reference:

[Cisco: Extension Mobility and Phone Login Features](#)

QUESTION 49

You are the administrator for your company's UCM network. Examine the exhibit below, and answer the question:



The screenshot shows the Cisco Unified CM Administration interface for user configuration. The main configuration area is titled "End User Configuration" and includes sections for "Extension Mobility", "Directory Number Associations", and "Mobility Information".

- Extension Mobility:**
 - Available Profiles: (Empty list)
 - Controlled Profiles: (Empty list)
 - Default Profile: -- Not Selected --
 - Presence Group*: Standard Presence group
 - SUBSCRIBE Calling Search Space: < None >
 - Allow Control of Device from CTI
 - Enable Extension Mobility Cross Cluster
- Directory Number Associations:**
 - Primary Extension: 65501
- Mobility Information:**
 - Enable Mobility
 - Primary User Device: < None >
 - Enable Mobile Voice Access
 - Maximum Wait Time for Desk Pickup*: 10000
 - Remote Destination Limit*: 4
 - Remote Destination Profiles: (Empty list)

On the right side, a "Connection Status" window is open for "Cisco Jabber Version 11.0.1 (19000)". It displays the following information:

- Softphone:** Status: Connected; Protocol: SIP; Address: 192.168.51.10 (CCMCIP); Device: Jabberwocky; Line: 65501.
- Deskphone:** Status: Not connected; Protocol: CTI; Address: 192.168.51.10 (CTI).
- Voicemail:** Status: Not connected; Port: 443; Protocol: VMREST (HTTPS); Reason: (Empty).
- Presence:** Status: Not connected; Address: WebEx; Protocol: XMPP; Reason: Unknown.
- Outlook address book:** Status: Last connection successful; Protocol: MAPI; Address: Outlook.
- Directory:** Status: Last connection successful; Address: BOSONSOFTWARE.COM; Protocol: LDAP.

At the bottom of the Connection Status window, there are "Copy" and "Print" buttons.

The user named Joe Cambers is not able to use Cisco Jabber's voice mail functionality.

Which of the following is most likely the reason?

- The softphone has no SIP profile.
- The softphone's profile does not allow CTI control.
- The SIP trunk to the CUPS server is down.

- D. The Cisco Unity Connection server either is down or is not installed.
- E. The Cisco Jabber client is configured to require a nonexistent desk phone.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most likely, the reason the user named Joe Cambers is not able to use Cisco Jabber's voice mail functionality is because the Cisco Unity Connection server either is down or is not installed. Cisco Unity Connection is a voice mail platform that integrates with a Cisco Unified Communications Manager (UCM) system. The Cisco Jabber client connects to Cisco Unity Connection by using a Representational State Transfer (REST) interface.

You can display and verify the backend systems to which the Cisco Jabber client is connected by clicking the gear icon and Show Connection Status in the Cisco Jabber home window. Clicking Show Connection Status displays the Connection Status window, which provides the connectivity status of every service to which Jabber is connected or is configured to connect. Services that are preceded by a green check mark have connected successfully. Services that display Not Connected or a caution icon have not connected successfully.

Although the user cannot use Cisco Jabber's IM and Presence functionality in this scenario, it is because the Session Initiation Protocol (SIP) trunk from UCM to the

Cisco Unified Presence (CUPS) server either is down or is not installed. Cisco Jabber relies on CUPS and the Extensible Messaging and Presence Protocol (XMPP) for instant messaging (IM) and Presence functionality. Cisco Unity Connection is not required for IM and Presence functionality.

The softphone has a SIP profile. Based on the value displayed in the SIP Profile field of the UCM Administration page in this scenario, you can determine that the softphone is configured to use the Standard SIP Profile, which is the default UCM SIP profile.

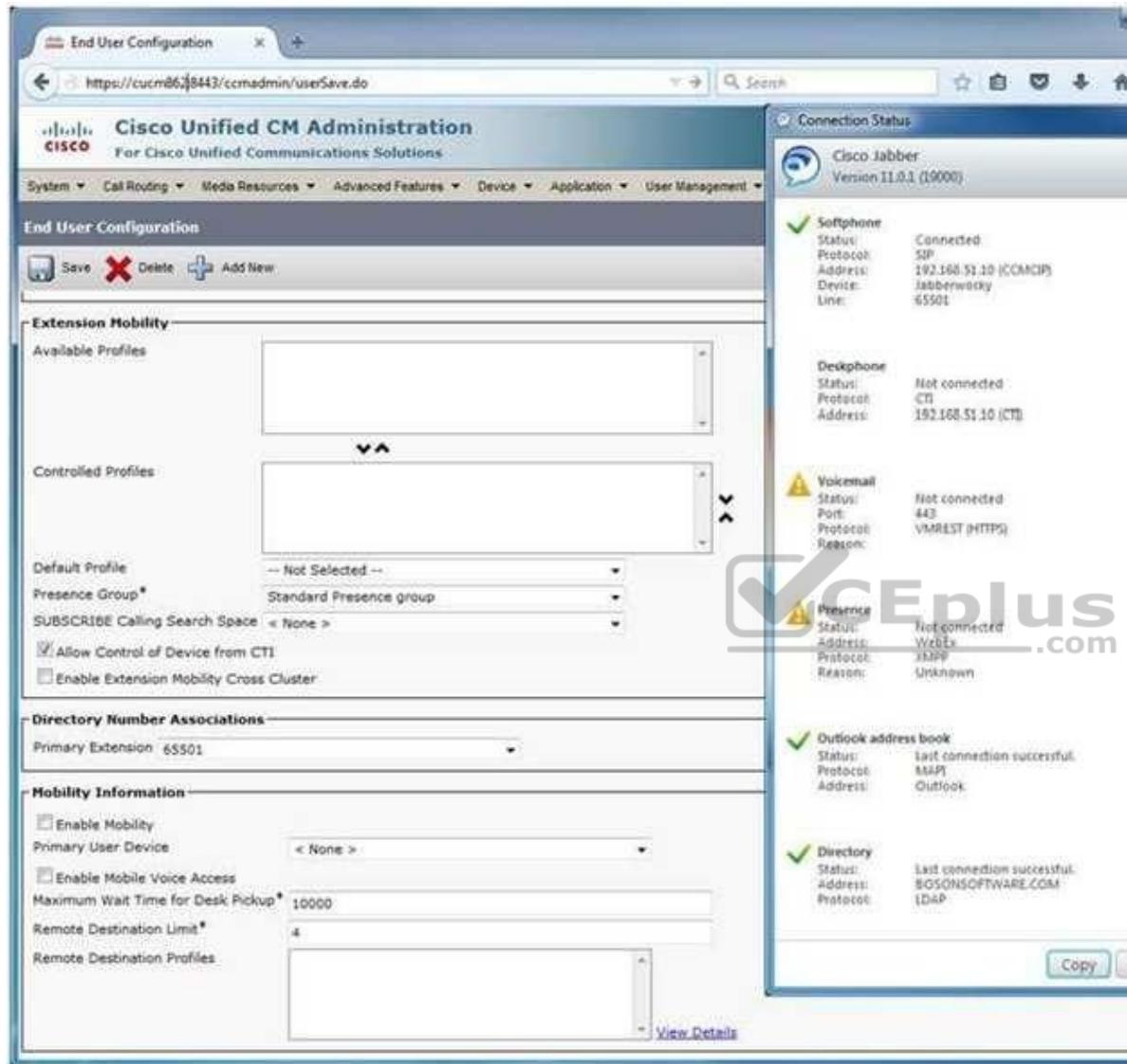
The softphone's profile does allow Computer Telephony Integration (CTI) control. Based on the value displayed in the Allow Control of Device from CTI field, you can determine that CTI control has been enabled for the softphone. However, disabling this option would not disable Jabber's IM functionality. CTI enables the Cisco Jabber client to control aspects of a connected hardware phone, or desk phone. However, the Cisco Jabber client does not require a desk phone. Both Jabber and Cisco Unified Personal Communicator communicate with a desk phone by using the CTI Quick Buffer Encoding (CTIQBE) protocol.

Reference:

[Cisco: Feature Comparison Cisco Messaging Products \(Unity Express, Unity Connection, Unity\)](#)

QUESTION 50

You are the administrator for your company's UCM network. Examine the exhibit below, and answer the question:



The screenshot shows the Cisco Unified CM Administration interface. The main window is titled "End User Configuration" and displays configuration options for a user. The "Extension Mobility" section includes fields for "Available Profiles", "Controlled Profiles", "Default Profile" (set to "-- Not Selected --"), "Presence Group" (set to "Standard Presence group"), and "SUBSCRIBE Calling Search Space" (set to "< None >"). There are checkboxes for "Allow Control of Device from CTI" (checked) and "Enable Extension Mobility Cross Cluster" (unchecked). The "Directory Number Associations" section shows the "Primary Extension" as "65501". The "Mobility Information" section has checkboxes for "Enable Mobility" (unchecked) and "Enable Mobile Voice Access" (unchecked), along with fields for "Primary User Device" (set to "< None >"), "Maximum Wait Time for Desk Pickup" (set to "10000"), "Remote Destination Limit" (set to "4"), and "Remote Destination Profiles".

An overlay window titled "Connection Status" is open on the right, showing the status of various services for the user "Cisco Jabber" (Version 11.0.1 (19000)).

Service	Status	Protocol	Address	Device	Line
Softphone	Connected	SIP	192.168.51.10 (CUCM)	Jabberwocky	65501
Deskphone	Not connected	CTI	192.168.51.10 (CTI)		
Voicemail	Not connected	VMREST (HTTPS)	443		
Presence	Not connected	WebEx	JMP		Unknown
Outlook address book	Last connection successful	MAPI	Outlook		
Directory	Last connection successful	LDAP	BOSONSOFTWARE.COM		

Which of the following is most likely true? A.

The DNS server is down.

B. The UCM server is not configured to use DNS.

C. The UCM server's host name is cucm862.

- D. The end user's user name is Jabberwocky.
- E. The workstation is using a hosts file to resolve the UCM server's name.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most likely, the Cisco Unified Communications Manager (UCM) server's host name is cucm862. Based on the information in the browser's location bar, you can determine that the administrator in this scenario connected to the UCM Administration page by using the Uniform Resource Locator (URL) [https:// cucm862:8443/ccmadmin](https://cucm862:8443/ccmadmin). If the workstation were not able to resolve the host name cucm862 to an IP address, the administrator would not be able to connect to the UCM Administration page.

Although UCM can be deployed with a Domain Name System (DNS) configuration, Cisco recommends that administrators who are deploying UCM in a high availability environment not rely on DNS to connect endpoints to UCM, because doing so could create a single point of failure. Even if DNS is required for systems management purposes, Cisco recommends not using host names to configure endpoints, gateways, and UCM servers.

There is not enough information in the scenario to determine whether the workstation is using a hosts file, or whether the UCM server is configured to use DNS name resolution. Even though the Cisco Jabber client is connecting to the UCM server by using the IP address of 192.168.51.10, the administrator's workstation has been able to resolve the UCM server's host name. The workstation could have resolved the host name of cucm862 by using either a DNS server or a local hosts file.

When Cisco Jabber cannot connect to a server by using either DNS or an IP address, the Cannot communicate with the server message will appear on the Cisco Jabber client's login screen. The same message will appear if the server to which Cisco Jabber is configured to connect is down. In this scenario, the Cisco Jabber client has successfully connected to the UCM device at 192.168.51.10.

The end user's user name is not Jabberwocky. In this scenario, the user's login information has not been provided. Jabberwocky is the name of the Cisco Jabber client endpoint in UCM.

There is not enough information to determine whether a DNS server is down, because the Cisco Jabber client is not relying on DNS to connect to the UCM server. If the Cisco Jabber user logged in with a fully qualified domain name (FQDN), you could surmise that the DNS server is still functional because Cisco Jabber was able to resolve the login credential. However, you do not know what credentials were used to log in.

Reference:

[Cisco: Network Infrastructure: Domain Name System \(DNS\)](#)

QUESTION 51

You issue the show running-config command on a CME router and receive the following partial output:

```
ip dhcp excluded-address 192.168.14.1 192.168.14.9
ip dhcp pool IPPhones
 network 192.168.14.0 255.255.255.0
 default-router 192.168.14.1
!
<output omitted>
!
interface FastEthernet 0/0
 ip address 192.168.14.1 255.255.255.0
 no shutdown
!
<output omitted>
!
dial-peer voice 2 pots
 destination-pattern .11
 port 1/0/2
!
<output omitted>
!
ephone-dn 50
 number 5000
!
ephone-dn 51
 number 5001
!
ephone 20
 button 1:50
!
ephone 21
 button 1:51
 button 2:50
```



Examine the output, and use the information you gather to answer the question.
Which of the following is most likely to occur if a user dials 911?

- A. The call will connect to the 911 service.
- B. The call will fail because .11 is not a valid destination pattern.
- C. The call will connect to the 411 service because 4 comes before 9.

D. The call will fail because the forward-digits 3 command is missing.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The call will fail because the forward-digits 3 command is missing from the configuration. The forward-digits 3 command would enable the router to forward N11 service calls to the public switched telephone network (PSTN). N11 numbers are a group of short telephone numbers that are reserved in the North American Numbering Plan (NANP) for special services, such as emergency calls, telephone directory information, and traffic reports. By default, Cisco Unified Communications Manager Express (CME) only forwards digits matched by wildcards in a destination pattern, not digits that are explicitly defined in the destination pattern. Therefore, the destination-pattern .11 command configures CME to forward only the first digit in the destination pattern when a user dials an N11 service code.

The destination pattern in this configuration is valid. The destination-pattern command is used to match both inbound and outbound dial peers. The sequence of dialed digits that will be matched for a dial peer can contain the digits 0 through 9, the asterisk (*), and the pound sign (#). In addition, you can use a period (.) as a wildcard symbol to refine the dialing pattern or to match multiple dial strings for a single dial peer. The command set in this scenario configures a dial peer on a CME router to match three-digit patterns ending in 11.

The call will not connect to either the 911 service or the 411 service, because the CME router will forward only the first digit of the number. However, if the forward digits 3 command had been issued on the router, the call would connect to the 411 service only if the user dialed 411. Destination pattern matching on the wildcard matches digits one-by-one as the user dials them; it does not match digits to wildcards in a given sort order.

Reference:

[Cisco: Cisco IOS Voice Command Reference: forward-digits](#)

QUESTION 52

You issue the show running-config command on a CME router and receive the following partial output:

```
ip dhcp excluded-address 192.168.14.1 192.168.14.9
ip dhcp pool IPPhones
 network 192.168.14.0 255.255.255.0
 default-router 192.168.14.1
!
<output omitted>
!
interface FastEthernet 0/0
 ip address 192.168.14.1 255.255.255.0
 no shutdown
!
<output omitted>
!
dial-peer voice 2 pots
 destination-pattern .11
 port 1/0/2
!
<output omitted>
!
ephone-dn 50
 number 5000
!
ephone-dn 51
 number 5001
!
ephone 20
 button 1:50
!
ephone 21
 button 1:51
 button 2:50
```



Examine the output, and use the information you gather to answer the question.

You issue the prefix 911 command on the CME router.
Which of the following will occur when a user dials 411?

A. The user will be connected to the 411 service with an outbound prefix of 9.

- B. The user will be connected to the 411 service directly.
- C. The user will be connected to the extension 9114 if it exists.
- D. The user will be connected to an operator.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If you issue the prefix 911 command on the Cisco Unified Communications Manager Express (CME) router, a user who dials 411 will be connected to the extension

9114 if it exists in the system. The prefix command is used to add one or more digits to the front of the dial string before the dial string is forwarded to the destination network. Issuing the prefix 911 command in this scenario will add 911 to the front of the dial string. The last two digits in the destination pattern, 1 and 1, were explicitly matched. By default, CME only forwards digits matched by wildcards in a destination pattern, not digits that are explicitly defined in the destination pattern. Therefore, the dial string 9114 would be forwarded to the public switched telephone network (PSTN).

The destination-pattern command is used to match both inbound and outbound dial peers. The sequence of dialed digits that will be matched for a dial peer can contain the digits 0 through 9, the asterisk (*), and the pound sign (#). In addition, you can use a period (.) as a wildcard symbol to refine the dialing pattern or to match multiple dial strings for a single dial peer. The command set in this scenario configures a dial peer on a CME router to explicitly match the pattern 9114. By default, CME only forwards digits matched by wildcards in a destination pattern, not digits that are explicitly defined in the destination pattern. Therefore, the destination-pattern .11 command configures CME to forward only the first of the digits in the destination pattern when a caller dials 411.

Reference:

[Cisco: Cisco IOS Voice Command Reference: prefix](#)

QUESTION 53

Which of the following interfaces handles the exchange of availability information between third-party clients and a Cisco Presence deployment?

- A. AXL/SOAP
- B. LDAP
- C. SIP
- D. XMPP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Extensible Messaging and Presence Protocol (XMPP) interface handles the exchange of availability information between third-party clients and a Cisco Presence deployment. Cisco Unified Communications Manager (UCM) and Cisco Unified Presence (CUPS) server together are the primary components of a Cisco Presence deployment.

The Session Initiation Protocol (SIP) interface does not handle the exchange of availability information between third-party clients and a Cisco Presence deployment. However, a SIP trunk interface does handle the exchange of availability information between UCM and a CUPS server. A UCM SIP trunk interface must point to the CUPS server in order for availability information to be exchanged between the two systems. CUPS is also capable of sending SIP subscribe messages to UCM over the SIP trunk if UCM is configured as a Presence gateway.

The Lightweight Directory Access Protocol (LDAP) interface does not handle the exchange of availability information between third-party clients and a Cisco Presence deployment. However, the LDAP interface is used to synchronize user information between UCM and CUPS in order to create a single sign-on (SSO) user experience. For example, a Cisco Unified Personal Communicator user can be authenticated to both the CUPS server and UCM by connecting directly to the CUPS server. LDAP is a directory protocol that is used by other servers, such as CUPS to perform contact lookups. LDAP listens on Transmission Control Protocol (TCP) port 389 unencrypted or on port 636 over Secure Sockets Layer (SSL). Third-party XMPP clients can also use LDAP to search the database and add users as contacts.

The Cisco Administrative Extensible Markup Language (AXL)/Simple Object Access Protocol (SOAP) interface does not handle the exchange of availability information between third-party clients and a Cisco Presence deployment. However, the AXL/SOAP interface is used to handle database synchronization tasks from UCM to the CUPS database. For synchronization to start, the Sync Agent service must be started on the CUPS server.

Reference:

[Cisco: Cisco Unified Presence Features and Functions: Cisco Unified Presence Components](#)

QUESTION 54

Which of the following URLs cannot be used to access Cisco Unified Operating System Administration?

- A. <http://ip-address/admin>
- B. <http://ip-address/ccmadmin>
- C. <http://ip-address/cmplatform>
- D. <http://ip-address/cuadmin>
- E. <http://ip-address/cupadmin>

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You cannot use the Uniform Resource Locator (URL) <http://ip-address/admin> to access Cisco Unified Operating System Administration. However, you can use <http://ip-address/admin>, where ip-address is the IP address that has been assigned to the Cisco Unity Express (CUE) network module, to access the CUE browserbased administrative graphical user interface (GUI). CUE is a voice mail messaging system that is typically installed in a Cisco Unified Communications Manager Express (CME) router module slot. Both CUE and CME can be administered by using either a command-line interface (CLI) or the browser-based GUI.

You can use the URL <http://ip-address/cmplatform>, where ip-address is the IP address of a Cisco Unified Communications Manager (UCM) server, a Cisco Unity Connection server, or a Cisco Unified Presence (CUPS) server, to access Cisco Unified Operating System Administration. Cisco Unified Operating System Administration is a browser-based GUI that can be used to modify operating system and network settings that are common across components of a Cisco Unified

Communications network. For example, you can verify Dynamic Host Configuration Protocol (DHCP) settings by using the Unified Operating System Administration GUI.

You can use the URL `http://ip-address/ccmadmin`, where `ip-address` is the IP address of a UCM server, to access Cisco Unified Operating System Administration. The URL `http://ip-address/ccmadmin` launches the UCM administrative GUI. You can then click Navigation > Cisco Unified OS Administration to enter Cisco Unified Operating System Administration.

You can use the URL `http://ip-address/cuadmin`, where `ip-address` is the IP address of a Unity Connection server, to access Cisco Unified Operating System Administration. The URL `http://ip-address/cuadmin` launches the Cisco Unity Connection administrative GUI. You can then click Navigation > Cisco Unified OS Administration to enter Cisco Unified Operating System Administration.

You can use the URL `http://ip-address/cupadmin`, where `ip-address` is the IP address of a CUPS server, to access Cisco Unified Operating System Administration. The URL `http://ip-address/cupadmin` launches the CUPS administrative GUI. You can then click Navigation > Cisco Unified OS Administration to enter Cisco Unified Operating System Administration.

Reference:

[Cisco: Log in to Cisco Unified Communications Operating System Administration](#)

Cisco: Getting Started with Cisco Unified Operating System Administration

QUESTION 55

Another administrator deletes the IPSec trust store from UCM's Security > Certificate Management page. Which of the following is most likely to be affected by this change?

- A. encryption of DRS backups made prior to the change
- B. encrypted communication between DRS Master Agents and Local Agents
- C. addition of new backup devices to a DRS schedule
- D. deletion of old backup devices from a DRS schedule
- E. access to network storage location configuration

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, encrypted communication between Cisco Unified Communications Manager (UCM) Disaster Recovery System (DRS) Master Agents and Local Agents is most likely to be affected by this change. Master Agents store component registrations, maintain scheduled tasks, and store backup data on a locally attached device. Local Agents, which are installed and activated by default on each cluster node, are responsible for running backup and restore scripts on the local server. DRS uses Secure Sockets Layer (SSL) to both authenticate and encrypt data between a Master Agent and a Local Agent. In addition, DRS uses IP Security (IPSec) for public key infrastructure (PKI) encryption. The deletion of the IPSec trust store from UCM's security configuration can cause DRS to function improperly.

Encryption of DRS backups will not likely be affected by this change. DRS uses the existing cluster security password when performing encryption on a backup. If the cluster security password is modified by using the command-line interface (CLI) or by a fresh UCM installation, you might not be able to decrypt and restore

that backup. Workarounds to this issue include remembering the old cluster security password that was used to encrypt the data or immediately performing a fresh backup when the cluster security password changes.

The addition or deletion of backup devices to a DRS schedule will not be affected by this change. However, it is important to note that a backup device cannot be deleted from DRS if that backup device is part of an existing backup schedule. In order to remove an existing backup device from a DRS configuration, you must first ensure that the device has been removed from any backup schedules in which it might be configured.

Access to network storage location configuration will not be affected by this change. In order to configure network storage locations, you must have access to a Secure File Transfer Protocol (SFTP) server. In addition to backing up data to devices that are directly connected to a Master Agent, DRS can back up to network storage locations by using SFTP.

Reference:

[Cisco: Disaster Recovery System Administration Guide for Release 8.5\(1\): What is the Disaster Recovery System?](#)

QUESTION 56

You administer a Cisco CME router with CUE installed. You issue the show running-config command on the router and receive the following partial output:

```
ephonedn 51
number 70...
mwi on
!
ephonedn 52
number 71...
mwi off
```



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

- A. When a caller dials 70123, the MWI light for extension 70123 will turn on.
- B. When a caller dials 70123, the MWI light for extension 123 will turn on.
- C. When a caller dials 71123, the MWI light for extension 71123 will turn off.
- D. The MWI lights cannot be turned on manually from an IP phone.
- E. When a caller leaves a message for extension 123, the MWI light for extension 123 will turn on.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When a caller dials 70123 or when a caller leaves a message for extension 123, the message waiting indicator (MWI) light for extension 123 will turn on. The MWI light appears on a user's IP phone when a new voice mail message is received in the user's Cisco Unity Express (CUE) voice mailbox.

To configure MWI, you must create two ephone-dns: one ephone-dn to turn the MWI light on when the user receives a message, and one ephone-dn to turn the

MWI light off when the user retrieves all of his or her messages. When CUE receives a voice mail message for a user, CUE will send a code to the Cisco Unified Communications Manager Express (CME) router to indicate that the user's MWI light should be turned on. When the user retrieves the message, CUE will send another code to CME to indicate that the user's MWI light should be turned off.

The MWI codes can be any number of any length as long as they are not the same as any existing extension numbers. To configure the MWI code that CUE will send to CME, you should issue the number command with the MWI code plus a number of periods equal to the number of digits in the users' extensions. For example, if you want to create MWI code 70 and your system is configured to use three-digit extensions, you should issue the number 70... command in ephone-dn configuration mode.

Finally, the ephone-dn that is configured with the MWI code must also be configured with the mwi on or the mwi off command, depending on whether the ephonedn should be responsible for turning the MWI light on or off, respectively. For example, the following command set configures ephone-dn 51 to turn on the MWI light for any three-digit extension that is prefaced by the MWI code 70:

```
ephone-dn 51
number 70...
mwi on
```

Similarly, the following command set configures ephone-dn 52 to turn off the MWI light for any threedigit extension that is prefaced by the MWI code 71:

```
ephone-dn 52
number 71...
mwi off
```



After CME receives a dialed string from CUE that contains the MWI code, CME will match the dialed digits to the ephone-dn number pattern, strip off the explicitly matched MWI code, and change the state of the MWI light for the extension that matches the remaining forwarded digits. In this scenario, CUE will send the digit string 70123 to CME when the user at extension 123 receives a voice mail message? CME will then strip off MWI code 70 and turn on the MWI light for extension 123.

The MWI light on an IP phone can be turned on or off manually if a user dials the MWI code plus any extension number, provided that the MWI code can be dialed on an IP phone keypad. For example, if a user dials 70123 from the keypad of an IP phone connected to a CME router that is configured with the command sets shown above, the MWI light will turn on for the IP phone that has been assigned extension 123, even though extension 123 has not received a new voice mail message.

To prevent users from being able to turn the MWI light on or off at will without having to leave or listen to a voice mail message, you can configure the MWI code by using a character from A through D in the digits. The characters ranging from A through D are included in the dual-tone multi-frequency (DTMF) signaling standard but are not included on typical telephone keypads. For example, the following command set configures ephone-dn 51 to turn on the MWI light for any three-digit extension that is prefaced by the MWI code A7:

```
ephone-dn 51
number A7...
mwi on
```

The MWI light for extension 70123 will not turn on when a caller dials 70123. The ephone-dns in this scenario are configured to turn the MWI light on or off for IP phones with three-digit extensions. Extension 70123 is a five-digit extension. Therefore, the MWI light for extension 70123 will not turn on; the MWI light for extension 123 will turn on, even if extension 123 has not received a new voice mail message.

Similarly, the MWI light for extension 71123 will not turn off when a caller dials 71123. The ephone-dns in this scenario are configured to turn the MWI light on or off for IP phones with three-digit extensions. Extension 71123 is a five-digit extension. Therefore, the MWI light for extension 71123 will not turn off? the MWI light for extension 123 will turn off, even if extension 123 contains new voice mail messages.

Reference:

[Cisco: Troubleshooting Unity Express Message Waiting Indication \(MWI\) Problems: MWI with Cisco CallManager Express](#)

[Cisco: Connecting Multiple Cisco Unified CallManager Express Systems with VoIP: DTMF Digits](#)

QUESTION 57

You are upgrading the firmware on all Cisco IP Phone 7961s that are connected to your company's network.

Which of the following upgrade methods is most likely to require high bandwidth?

- A. individual IP phone upgrades
- B. load server download
- C. peer firmware sharing
- D. traditional TFTP server download

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

Explanation:

Of the available choices, the traditional Trivial File Transfer Protocol (TFTP) server download method of IP phone firmware upgrade is most likely to require high bandwidth. When using the traditional TFTP server download method, each IP phone independently downloads the new image from the TFTP server in an "every man for himself" style strategy. When firmware images were small, this strategy was acceptable even when the IP phones were on a network at a separate location from Cisco Unified Communications Manager (UCM). Over time, IP phone firmware sizes have increased, which could cause slow upgrades over WAN links. In addition, the traditional TFTP download method could create high CPU usage on the UCM TFTP server.

You can also update the firmware on an individual IP phone by using the traditional TFTP method. First, you should make a note of the existing Phone Load Name value for the phone model that you want to upgrade by navigating to Device > Device Settings > Device Defaults in UCM Administrator. This is important because installing the new firmware image will automatically overwrite the value of the Phone Load Name field in Device > Device Settings > Device Defaults. You should then upload the new firmware to UCM by navigating to Software Upgrades > Install/Upgrade.

After you upload the new firmware, specify the name of the new firmware in the Phone Load Name field for the specific IP phone you want to upgrade by using UCM Administration's Device > Phone menu. Next, navigate to Device > Device Settings > Device Defaults and replace the new value of the Phone Load Name field with its original value. This will prevent other IP phones from downloading the new firmware after you restart the TFTP service.

Finally, you should restart the TFTP service in Cisco Unified Serviceability. After the service restarts, the IP phone you edited in UCM Administration should download the new firmware, upgrade the firmware, and restart. Other IP phones might restart as well. However, those IP phones will not be upgraded.

In contrast to the traditional TFTP server method, the load server download method enables the administrator of the LAN on which the IP phone operates to provide his or her own local TFTP server for firmware upgrades instead of relying on a remotely located default UCM TFTP server. This means that IP phones on remote networks will be able to download firmware updates in approximately the same amount of time it would take for an IP phone that is local to UCM. In addition, the TFTP load can be balanced among multiple TFTP servers at multiple sites. One disadvantage to the load server download method is that the local administrator is responsible for copying the firmware update to the TFTP server. Therefore, the TFTP upload and server configuration is subject to human error.

Peer firmware sharing is a method of updating the firmware on Cisco IP phones. When peer firmware sharing is implemented, only one Cisco IP phone at a location is responsible for downloading the new firmware. The firmware is then distributed to the other IP phones on the LAN in a parent-child hierarchy. The downloading phone distributes the firmware to its children. Those children then distribute the firmware to their children, and so on. No one parent in the hierarchy can have more than two children. Some disadvantages to the peer firmware sharing method are that the hierarchies are limited to their own subnets and are specific to phone model. In addition, peer firmware sharing must be enabled on each IP phone.

Reference:

[Cisco: Unified IP Phone Firmware Distribution Methods](#)

[Cisco: Upgrade IP Phone Firmware Individually](#)

QUESTION 58

Which of the following dial peer commands will not match dial strings 3331, 3332, and 3333?

- A. destination-pattern .T
- B. destination-pattern 33T
- C. destination-pattern
- D. destination-pattern 333.
- E. destination-pattern 333(123)
- F. destination-pattern 3+[123] G. destination-pattern 333[^49]



Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The dial peer command destination-pattern 333(123) will not match dial strings 3331, 3332, and 3333. The destination-pattern command is used to match both inbound and outbound dial peers; a dial peer defines a logical route to a telephony endpoint. The sequence of dialed digits that will be matched for a dial peer can contain the digits 0 through 9, the asterisk (*), and the pound sign (#). In addition, you can use the following symbols to refine the dialing pattern or to match multiple dial strings for a single dial peer:

.	The period matches any dialed digit.
,	The comma inserts a one-second pause.
%	The percent sign indicates that the preceding digit occurs zero or more times.
+	The plus sign indicates that the preceding digit occurs one or more times. When placed at the start of the string, the plus sign indicates an E.164 standard number.
?	The question mark indicates that the preceding digit occurs zero or one time.
[]	Square brackets indicate a range or a set of characters.
^	The caret can be used within square brackets to indicate characters that should not match.
()	Parentheses indicate a sequence of characters, often used with repeating patterns.
T	The T character is placed at the end of a string to indicate any string of zero or more digits.

Parentheses are used to indicate a specific sequence of characters. Therefore, the dial peer command destination-pattern 333(123) will match only the dial string 333123. Parentheses are often used with the %, +, and ? characters to indicate a repeating pattern. For example, the destination-pattern 333(123)% command matches 333, 333123, 333123123, 333123123123, and so on.

The following dial peer commands will match dial strings 3331, 3332, and 3333: destination-pattern .T

-destination-pattern 33T destination-pattern

-destination-pattern 333.

-destination-pattern 3+[123]

-destination-pattern 333[^49]

The dial peer command destination-pattern .T is used to indicate any string of up to 32 digits. The T character is used at the end of a string to instruct the router to wait for the complete dial string to be entered before matching a call to a dial peer. Cisco recommends that you use the destination-pattern .T command rather than the destination-pattern T command because the destination-pattern .T command requires that the caller dial a digit. By default, a dial peer with the destinationpattern T command will be matched if an outbound caller takes the phone off-hook for 10 seconds.

The dial peer command destination-pattern 33T matches any dial string of up to 32 digits that begins with 33. Not only will the dial peer command destinationpattern 33T match 3331, 3332, and 3333, it will also match 334567 and 3331234, among others. However, if a dial string matches multiple dial peers, the longest explicit match is chosen. For example, if one dial peer contains the destination-pattern 333T command and another dial peer contains the destination-pattern 3334T command, a call from a caller dialing 3334000 would match the second dial peer.

The dial peer command destination-pattern matches any four-digit dial string. The period is used as a wildcard character that matches any digit. Therefore, the destination-pattern command matches dial strings 3331, 3332, 3333, 0000, 1257, and 6538, among many others.

The dial peer command destination-pattern 333. matches any four-digit dial string that begins with 333. Not only will the destination-pattern 333. command match 3331, 3332, and 3333, it will also match 3330, 3334, 3335, 3336, and so on.

The dial peer command destination-pattern 3+[123] matches any dial string that contains one or more 3s and ends with a 1, 2, or 3. The plus sign indicates that the preceding digit can occur one or more times. The square brackets are used to indicate that the pattern should match any of the bracketed digits for that digit position. Therefore, not only does the destination-pattern 3+[123] command match the dial strings 3331, 3332, and 3333, it also matches the dial strings 31, 32, 33, 331, 332, 333, 333331, 3333332, and 3333333333, among many others.

The dial peer command destination-pattern 333[^49] matches any dial string that starts with 333 and ends with a digit that is not 4 through 9. The caret symbol (^) can be used within square brackets to indicate characters that should not match. The dash can be used between two digits within brackets to indicate a range of characters. Therefore, the destination-pattern 333[^49] command matches the dial strings 3330, 3331, 3332, 3333, and 333*, but the command does not match the dial strings 3334, 3335, 3336, 3337, 3338, and 3339.

Reference:

[Cisco: Cisco IOS Voice Command Reference: destination-pattern](#)

QUESTION 59

Which of the following protocols does Cisco Unified Personal Communicator use to connect to UCM in softphone mode?

- A. CCMCIP
- B. HTTPS
- C. IMAP
- D. IMAP over SSL
- E. IMAP over TLS
- F. SIP
- G. XMPP

Correct Answer: F

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cisco Unified Personal Communicator uses Session Initiation Protocol (SIP) to connect to Cisco Unified Communications Manager (UCM) in softphone mode. SIP is a call signaling protocol that is used by UCM to communicate with collaboration endpoints, such as Unified Personal Communicator and Cisco Jabber. Unified Personal Communicator is software that enables a user to connect to several different communication services from a single application. For example, you can use Unified Personal Communicator to place phone calls, download voice mails, and instant message (IM) another user.

SIP is an Internet Engineering Task Force (IETF) standard call signaling protocol. Although SIP is typically used as a peer-to-peer call signaling protocol, it can also operate in client/server mode. A softphone is software that behaves like a phone, enabling a user to have voice conversations over a typical workstation network connection. Softphone mode is an operational mode that Unified Personal Communicator uses to act as a softphone.

Unified Personal Communicator does not use Extensible Messaging and Presence Protocol (XMPP) to connect to UCM in softphone mode. XMPP is an open Extensible Markup Language (XML) IM and presence protocol. Unified Personal Communicator uses XMPP to establish IM sessions with Cisco Unified Presence

(CUPS). CUPS is server software that centralizes network traffic from several different communications services so that it can all be transmitted over the same Cisco Voice over IP (VoIP) network. CUPS also uses XMPP to communicate with IM clients? it uses SIP and SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) to integrate with third-party clients and applications.

Cisco Jabber, which also uses SIP and XMPP, is an application that is intended to integrate CUPS server services, such as user availability, with Microsoft Office. Cisco Jabber is also an IM client, a voice and video call client, and a desktop sharing client.

Unified Personal Communicator does not use Cisco Unified Communications Manager IP Phone (CCMCIP) service to connect to UCM in softphone mode. CCMCIP is used in desk phone mode. The difference between softphone mode and desk phone mode is that Unified Personal Communicator uses a physical IP phone as a proxy for voice conversations in desk phone mode. In softphone mode, Unified Personal Communicator handles the voice conversations itself.

Unified Personal Communicator does not use Secure Hypertext Transfer Protocol (HTTPS) to connect to UCM in softphone mode. Unified Personal Communicator uses HTTPS to establish encrypted connections to a conferencing server. In addition, Hypertext Transfer Protocol (HTTP) can be used to connect to a conferencing server without encryption.

Unified Personal Communicator does not use Internet Message Access Protocol (IMAP), IMAP over Secure Sockets Layer (SSL), or IMAP over Transport Layer Security (TLS) to connect to UCM in softphone mode. Unified Personal Communicator uses IMAP to communicate with a voice mail server. IMAP over SSL is used to encrypt communications between Unified Personal Communicator and the voice mail server. IMAP over TLS is used to encrypt voice mail transmissions specifically between Unified Personal Communicator and Cisco Unity Connection.

Reference:

[Cisco: About Cisco Unified Personal Communicator: How Cisco Unified Personal Communicator Fits into Your Network](#)

[Cisco: Glossary for Cisco Unified Personal Communicator: softphone](#)

[Cisco: Preparing To Use Cisco Unified Personal Communicator: Choosing Softphone or Desk Phone Mode](#)

[Cisco: Release Notes for Cisco Unified Personal Communicator Release 8.0: Network Ports Used by Cisco Unified Personal Communicator](#)

QUESTION 60

With which of the following control components do UCM media resources interact when UCM needs to locate resources to establish a conference call?

- A. call control
- B. media control
- C. MTP control
- D. MOH control

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cisco Unified Communications Manager (UCM) media resources interact with UCM's call control component when UCM needs to locate resources to establish a conference call. The UCM Media Resource Manager is responsible for connecting the media streams that comprise conferencing features, among others. When troubleshooting media resource problems, such as conference call failures, it is important to first investigate the UCM media resources configuration. UCM media

resources are available directly from the UCM server on which the services are enabled. In addition, the UCM Media Resource Manager enables UCM to provide those services to other UCM servers in a cluster.

UCM media resources do not interact with UCM's media control component when UCM needs to locate resources to establish a conference call. UCM media resources interact with UCM's media control component in order to locate resources to establish a media termination point (MTP) or to transcode compression types. The UCM media control component is responsible for managing the creation and teardown of media streams for a given endpoint.

UCM media resources do not interact with UCM's MTP control component when UCM needs to locate resources to establish a conference call. UCM media resources interact with UCM's MTP control component in order to reserve transcoders within a UCM cluster.

UCM media resources do not interact with UCM's music on hold (MOH) control component when UCM needs to locate resources to establish a conference call. UCM media resources interact with UCM's call control component in order to locate resources to establish an MOH session. Because the MOH control enables UCM to redirect a caller to an audio server, UCM media resources also interface with the MOH control when establishing such a session.

Reference:

[Cisco: Media Resource Management: Understanding Media Resources](#)

QUESTION 61

Which of the following is a function of the BAT?

- A. using a CSV file to update users
- B. generating Cisco Unity Connection reports
- C. synchronizing with LDAP
- D. using an XML-based service to import new users



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Using a comma-separated values (CSV) file to update users is a function of the Bulk Administration Tool (BAT). The BAT enables administrators to import, or onboard, users and modify user settings by importing CSV files. For example, to use the BAT to modify the voice mail message length limit in Cisco Unity Connection, you could export the voice mail users to a CSV file, change the message length limit value for each user in the CSV file, and then import the CSV file again. You can access the BAT by clicking Tools > Bulk Administration Tool in the Unity Connection graphical user interface (GUI).

Generating Cisco Unity Connection reports is a function of the Connection Reports Data Harvester service, not the BAT. Cisco Unity Connection reports can be accessed in Cisco Unified Serviceability, which enables an administrator to view reports and manage Cisco Unified Communications Manager (UCM) features. Cisco Unified Serviceability is a browser-based troubleshooting tool that uses Secure Hypertext Transfer Protocol (HTTPS) to access information that is provided by other reporting tools, such as Cisco Unified Real-Time Monitoring Tool (RTMT) and Call Detail Records (CDR) Analysis and Reporting (CAR) tool. The Connection Reports Data Harvester service allows data to be collected from log files and entered into the Cisco Unified Serviceability Reports Archive, which holds information from which reports can be generated. You can verify that the Connection Reports Data Harvester service is running by clicking Navigation > Cisco Unified

Serviceability from within the UCM GUI and then clicking Service Management from the Tools menu. The Connection Reports Data Harvester service can be found under Optional Services. If the service is deactivated, you can click Activate to turn it on.

Using an Extensible Markup Language (XML)based service to import new users is a function of the ability to import from UCM into Unity Connection, not a function of the BAT. The Cisco Administrative XML Layer (AXL) Web Service is used to import UCM users into Unity Connection. The service must be enabled on both UCM and Unity Connection in order to import users. In addition, UCM users must be assigned a primary extension in UCM in order to be imported into Unity Connection by AXL.

Synchronizing existing Unity Connection users with Lightweight Directory Access Protocol (LDAP) directory services, such as Microsoft Active Directory, is a function of the Cisco Directory Synchronization (DirSync) service, not the BAT. To enable Unity Connection to synchronize with an LDAP directory, you must select the Cisco DirSync check box in the Directory Services area of the Unity Connection GUI. In addition, you can import new users from LDAP either by using the BAT to import a CSV file or by using the Users > Import Users tool to import into Unity Connection LDAP information that was previously imported into UCM. Because Unity Connection stores users locally, a user that is synchronized with Unity Connection from LDAP will continue to be stored locally even if that user is later deleted from the LDAP database.

Reference:

[Cisco: Working with Users: Updating Users](#)

QUESTION 62

You are troubleshooting voice audio problems on your company's VoIP network. The network carries both data and VoIP traffic. You have obtained the following measurements:

- Jitter: 50 ms
- Packet loss: 1 percent
- End-to-end delay: 150 ms

Which of the following best describes why your company's network is experiencing voice audio problems?

- A. The jitter is too high.
- B. The packet loss is too high.
- C. The end-to-end delay is too high.
- D. VoIP traffic should not be carried on the same network as data traffic.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Your company's network is most likely experiencing voice audio problems because the jitter is too high. Short delays and low packet loss on a Voice over IP (VoIP) network help protect the rate at which bits flow over the network. Cisco recommends a maximum jitter of 30 ms for VoIP traffic. Jitter is a variation in delay, which can cause voice traffic to arrive at different times, thereby causing breaks, or choppiness, in the audio stream. Jitter can be mitigated by implementing Quality of Service (QoS) mechanisms. The effects of VoIP issues like jitter and latency on a network can be analyzed by using data analysis techniques such as Mean Opinion Score (MOS) or R-Factor.

It is not likely that the reason your company's network is experiencing voice audio problems is because packet loss is too high. Cisco recommends a maximum packet loss of 1 percent for VoIP traffic. Packet loss is often caused when networks become congested and packets are dropped. Dropped packets can cause clips, or breaks, in the audio stream. However, voice traffic is more tolerant of dropped packets than of delayed packets because a small amount of packet loss is not noticeable to the human ear. Some codecs can correct small amounts of packet loss. On networks with limited bandwidth, a low-bitrate codec can mitigate packet loss. However, the overall quality of the audio will be reduced. Packet loss can also be mitigated by implementing QoS mechanisms.

It is not likely that the reason your company's network is experiencing voice audio problems is because end-to-end delay is too high. Cisco recommends a maximum end-to-end delay of 200 ms. The International Telecommunication Union (ITU) considers an end-to-end delay of 150 ms or less to be acceptable for high voice quality. Delay, which is also called latency, can introduce interruptions in conversation flow, causing the speakers at each end of the circuit to interrupt each other. End-to-end delay can be mitigated by implementing QoS mechanisms.

It is not likely that the reason your company's network is experiencing voice audio problems is because VoIP traffic is carried on the same network as data traffic. VoIP traffic can be carried on the same network as data traffic. However, data traffic is usually more tolerant of dropped packets and delay than VoIP traffic. Therefore, VoIP traffic is typically given priority over data traffic.

Reference:

[Cisco: Quality of Service for Voice over IP](#) (PDF)

QUESTION 63

You want an IP phone to use a line prompt instead of an MWI lamp to display information about a new message.

Which of the following line appearance fields should you modify in UCM?

- A. Display
- B. External Phone Number Mask
- C. Line Text Label
- D. Visual Message Waiting Indicator Policy

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You should modify the Visual Message Waiting Indicator Policy field in the Cisco Unified Communications Manager (UCM) administrative graphical user interface (GUI). The Visual Message Waiting Indicator Policy field configures the behavior of the message waiting indicator (MWI) lamp and of the MWI line prompt on an IP phone. For example, configuring the Visual Message Waiting Indicator Policy field to Light and Prompt will configure the IP phone to turn on the MWI lamp that is located on the IP phone's handset when a new voice mail message arrives. In addition, the IP phone will display a new message prompt beside the associated line button on the IP phone. However, configuring the Visual Message Waiting Indicator Policy field to Prompt Only will display the new message prompt beside the line button but will not turn on the MWI lamp. You can configure the Visual Message Waiting Indicator Policy field differently for each line that is associated with the IP phone. For example, if the IP phone is configured with a shared line in addition to a primary line, you could configure the Visual Message Waiting Indicator Policy field for the shared line to None so that the IP phone never displays MWI information for the shared line.

You should not modify the Line Text Label line appearance field. The contents of the Line Text Label field are displayed beside the associated line button of an IP phone. The field is typically configured with the name of the user that is associated with the line. If the Line Text Label field is not configured, the directory number (dn) that is associated with the line will be displayed instead. For example, if user John Public has been assigned extension 4000, the dn 4000 will be displayed beside the associated line button on the main screen of John Public's IP phone unless you configure the Line Text Label field. If you configure the Line Text Label field with the name John Public, then that name will appear beside the line button on the main screen of the IP phone.

You should not modify the Display (Internal Caller ID) field. When the Display (Internal Caller ID) field is blank, the dn that is associated with the calling device is shown on the display of the called device. Otherwise, the contents of the Display (Internal Caller ID) field are shown on the display of the called device. You can configure the Display (Internal Caller ID) field with a name or a description of up to 30 characters in length. If you configure the Display (Internal Caller ID) field, you should also configure the ASCII Display (Internal Caller ID) field with similar information. The contents of the ASCII Display (Internal Caller ID) field are displayed on called devices that do not support Unicode character sets. You cannot use nonASCII characters in the ASCII Display (Internal Caller ID) field.

You should not modify the External Phone Number Mask field. UCM transmits the contents of the External Phone Number Mask field as caller ID information when an internal user places an outgoing call to an external party. The information in the External Phone Number Mask field can be a string that consists of up to 24 numbers, the international escape character +, and X wildcards that represent the extension number. The X wildcards should always be at the end of the string. For example, a user that has been assigned extension number 4000 on the internal Voice over IP (VoIP) network might also be assigned a direct inward dial (DID) number of (555) 5554000. Therefore, you could configure the External Phone Number Maskfield with the string 555555XXXX. The number 5555554000 would then be displayed on the caller ID systems of any external parties who are called by the user at extension 4000. If the user at extension 4000 was not assigned a DID number, you could configure the External Phone Number Mask field with your company's main public switched telephone network (PSTN) number instead.

Reference:

Cisco: Directory Number Configuration: Directory Number Configuration Settings

QUESTION 64

Which of the following QoS features reduces the jitter of voice packets by preventing them from being delayed behind larger data packets in a queue?

- A. CAR
- B. LLQ
- C. cRTP
- D. LFI

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Link fragmentation and interleaving (LFI) is a Quality of Service (QoS) feature that reduces the jitter of voice packets by preventing them from being delayed behind larger data packets in a queue. LFI helps reduce the latency in voice packets by fragmenting large packets into smaller packets. Once this is accomplished, voice packets can be woven, or interleaved, between the fragmented data packets from a different flow and can pass through the network device much quicker than if the voice packets had to wait for the large data packets to be transmitted.

QoS enables a network to treat a specific type of traffic with a different priority than other types of traffic. For example, QoS can ensure that voice traffic gets higher priority on a network than data traffic. QoS models include the best-effort model, the Integrated Services (IntServ) model, and the Differentiated Services (DiffServ) model. Each QoS model handles packet flows in a different manner. For example, IntServ requires that applications reserve their end-to-end bandwidth requirements, and DiffServ prioritizes packets by traffic class. Because of some inherent shortcomings in the IntServ model, Cisco recommends using DiffServ when delivering voice traffic.

Low latency queuing (LLQ) is a queuing method that is useful for transmitting voice, video, and mission-critical traffic. However, if a large data packet is being sent, LLQ cannot interrupt the transmission of the large data packet in order to send a small voice packet, regardless of the size of the priority queue. Therefore, LLQ does not reduce the jitter of voice packets by preventing them from being delayed behind larger data packets in a queue.

Although Compressed Real-time Transport Protocol (cRTP) reduces delay, it does not reduce the jitter of voice packets by preventing them from being delayed behind larger data packets in a queue. To reduce the size of the IP header, cRTP associates a hash number with the 40byte IP header. After the first voice packet is sent with the full 40byte header, subsequent packets in the same flow use only the hash number that was associated with the header. This reduces the IP header size from 40 bytes to as low as two bytes if a checksum is not used. If a checksum is used, the header is reduced to four bytes.

Committed Access Rate (CAR) does not reduce the jitter of voice packets by preventing them from being delayed behind larger data packets in a queue. CAR is a traffic policing mechanism that you can use when traffic exceeds the configured bandwidth limitations. When CAR is used, packets that exceed the bandwidth limits are remarked with a lower priority and forwarded instead of being dropped.

Reference:

[Cisco: Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2: Chapter: Link Efficiency Mechanisms Overview](#)

QUESTION 65

Which of the following statements are correct regarding the restart and reset commands? (Choose three.)

- A. The reset command reboots phones faster than the restart command does.
- B. IP phones receive IP addressing information from a DHCP server after you issue either the reset command or the restart command.
- C. IP phones download configuration files from a TFTP server after you issue either the reset command or the restart command.
- D. You can issue either the reset command or the restart command after making changes to an ephone.
- E. You can issue either the reset command or the restart command after making changes to an ephone-dn.
- F. You can issue either the reset command or the restart command after changing date and time settings.

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The following statements are correct regarding the restart and reset commands:

-You can issue either the reset command or the restart command after making changes to an ephone.

-You can issue either the reset command or the restart command after making changes to an ephone-dn.

-IP phones download configuration files from a Trivial File Transfer Protocol (TFTP) server after you issue either the reset command or the restart command.

On a Cisco Unified Communications Manager Express (CME) router, the reset command performs a hard reset of the phone, similar to powering down the device and powering it back up again. When you issue the reset command, the phone contacts the Dynamic Host Configuration Protocol (DHCP) server to receive IP configuration information, including the IP address of the TFTP server. The phone then contacts the TFTP server and downloads the most recent phone configuration information. In addition, the IP phone will unregister and reregister with the Cisco call processor platform. You can also reset an IP phone by pressing the settings button on the IP phone's keypad and then pressing the *****#**** key sequence. In Cisco Unified Communications Manager (UCM), you can reset a phone from the graphical user interface (GUI) by clicking Device > Phone > Reset.

You must issue the reset command after performing the following tasks:

- Updating the phone's firmware
- Modifying the DHCP scope
- Changing the IP address of the TFTP server
- Changing Uniform Resource Locators (URLs)
- Changing the date and time settings
- Changing the language displayed on the phone
- Changing the call progress tones for the phone -
- Changing the voice mail access number

The restart command performs a soft reboot of the phone, so it reboots phones much quicker than the reset command does. When you issue the restart command on a CME router, the phone does not contact the DHCP server to receive new IP configuration information. However, it does contact the TFTP server to download the most recent phone configuration information. In addition, the phone will unregister and reregister with the call processor platform.

You can issue either the reset command or the restart command after performing the following tasks:

- Adding or deleting a phone button
- Associating a button with a new ephone-dn
- Modifying an extension on an ephone-dn
- Modifying speed-dial numbers on an ephone -
- Enabling call park

Reference:

[Cisco: Resetting and Restarting Phones: Differences between Resetting and Restarting IP Phones](#)

QUESTION 66

An end user wants to use SNR so that incoming calls to the user's IP phone simultaneously ring the user's mobile phone. You have already enabled Mobility on the end user's phone record in UCM. However, the user is not able to successfully configure SNR from the UCM Self Care portal. Which of the following should you examine to troubleshoot the issue? (Choose two.)

- A. Application Dial Rules
- B. Remote Destination Profile
- C. Remote Destination
- D. SNR assignment schedule

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You should examine the Remote Destination Profile and the Remote Destination in Cisco Unified Communications Manager (UCM) Administration to troubleshoot the issue. Before a user can enable Single Number Reach (SNR), an administrator must perform the following actions:

- Create a Remote Destination Profile
- Create a Remote Destination
- Enable Mobility on the end user's phone

In this scenario, you have already enabled Mobility on the end user's phone. However, there is not enough information to determine whether the Remote Destination Profile and Remote Destination have been configured. You should therefore begin troubleshooting there.

You do not need to examine the SNR assignment schedule. Because the end user has not yet been able to configure SNR, no SNR assignment schedule has been created. SNR assignment schedules enable users to configure specific days and spans of time during which the SNR configuration will be enabled. For example, if a user wanted to ensure that a given SNR was operational Monday through Friday from 8 a.m. until 6 p.m., the user could configure an SNR assignment schedule for those days and times.

You do not need to examine the Application Dial Rules. Application Dial Rules are used to add or remove digits from numbers that users dial.

Reference:

[Cisco: Cisco Unified Communications Manager Features and Services Guide, Release 8.5\(1\): Configuring Cisco Unified Mobility](#)

QUESTION 67

You have installed Cisco Unified Communications ELM. A warning message appears at the top of the interface.

Which of the following is most likely the problem?

- A. You are using ELM in Dashboard View.
- B. You are using ELM in License Usage View.
- C. You are using ELM in Demo mode.
- D. You are using ELM in Table View.
- E. You are using ELM in Chart View.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most likely, the problem is that you are using the Cisco Unified Communications Enterprise License Manager (ELM) in Demo mode. ELM requires that you install a license file before you can use it outside of Demo mode. If a warning appears at the top of the graphical user interface (GUI), you have most likely not installed a license file. ELM handles all licensing for Cisco Unified Communications Manager (UCM) and Cisco Unity Connection from version 9.0 forward. For example, you might use ELM to determine how many licenses remain available for a given Cisco Unified Communications product.

Although you might be using ELM in Dashboard View, this would not cause a warning message to appear at the top of the GUI. Dashboard view displays an overview of products installed, license updates, and license synchronization times. Dashboard View also enables you to quickly determine whether any license alerts or synchronization failures have occurred.

Although you might be using ELM in License Usage View, this would not cause a warning message to appear at the top of the GUI. License Usage View enables you to examine the licenses that have been installed in ELM and how those licenses are being used.

Although you might be using ELM in the License Usage View's Table View, this would not cause a warning message to appear at the top of the GUI. Table View is one of two views that you can select from License Usage View. In Table View, you can see the types of licenses in use, the number of licenses required, the number of licenses installed, the number of licenses not used, and whether the license type is in compliance. From Table view, you can also individually select and view specifics for each license, such as its description and usage chart.

Although you might be using ELM in License Usage View's Chart View, this would not cause a warning message to appear at the top of the GUI. Chart View is one of two views that you can select from License Usage View. In Chart View, you can see a graphical representation of the number of licenses that have been installed, the number of licenses that have been borrowed from a higher tier, the number of licenses required, and the number of licenses that have been loaned to a lower tier. Insufficient licenses are identified by a red X.

Reference:

[Cisco: Enterprise License Manager User Guide: System Status Information](#)

QUESTION 68

You want Cisco Unified Serviceability to automatically notify you if the Cisco Tomcat service goes down.

Which of the following should you do?

- A. Click Trace > Configuration.
- B. Click Alarm > Configuration.
- C. Click Tools > Service Activation.
- D. Click Tools > Serviceability Reports Archive.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You should click Alarm > Configuration to configure Cisco Unified Serviceability to automatically notify you if the Cisco Tomcat service goes down. The Cisco Unified Serviceability Alarm menu helps identify problems that exist with the Cisco Unified Communications system. Cisco Unified Serviceability alarms use Simple Network Management Protocol (SNMP) and Syslog to generate data that can be used as part of the troubleshooting process.

You should not click Tools > Serviceability Reports Archive to configure Cisco Unified Serviceability to automatically notify you if the Cisco Tomcat service goes down. The Cisco Unified Serviceability Reports Archive contains all of the following types of statistical reports:

- Device Statistics Report
- Server Statistics Report
- Service Statistics Report
- Call Activities Report
- Alert Summary Report
- Performance Protection Report

You should not click Tools > Service Activation in Cisco Unified Serviceability to configure Cisco Unified Serviceability to automatically notify you if the Cisco Tomcat service goes down. The Service Activation option under the Tools menu enables you to select individual services to activate or select all services at once. After you have selected the services you want to enable, you should click the Save button to activate those services.

You should not click Trace > Configuration to configure Cisco Unified Serviceability to automatically notify you if the Cisco Tomcat service goes down. The Trace menu can be used to configure parameters for voice application debugging tools that can be used in troubleshooting efforts. However, the tools available through the Trace menu are typically logged for later manual review.

Reference:

[Cisco: Configuring Alarms: Configuring an Alarm for a Service](#)

QUESTION 69

You are manually configuring Cisco Jabber to connect to your company's UCM 8.6 deployment. You want to manually configure Jabber clients to connect to the following servers:

- TFTP: 192.168.51.10
- CTI: 192.168.51.9
- CCMCIP: 192.168.51.9

Which of the following should you do?

- A. Click Advanced settings in each Jabber client, and configure the servers.
- B. Navigate to UCM Administrator's Service Profiles, and configure the servers.
- C. Navigate to UCM Administrator's User Management, and configure the servers.
- D. Edit DNS settings, and configure SRV records for each of the services.

Correct Answer: A

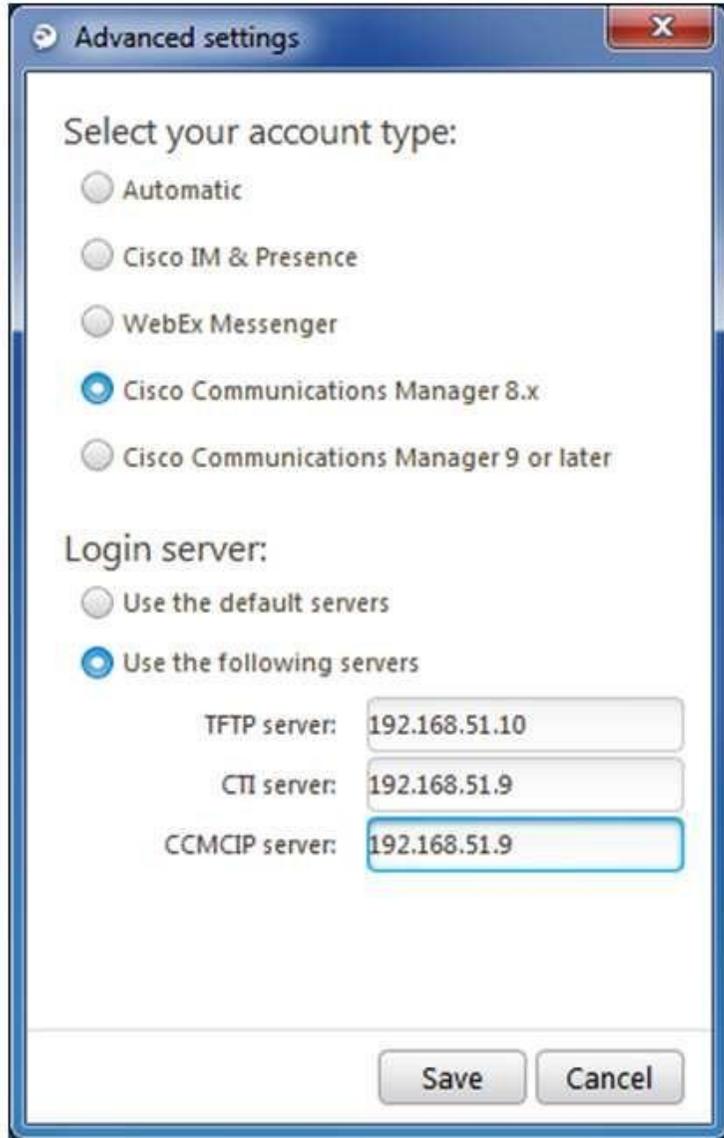
Section: (none)

Explanation

Explanation/Reference:

Explanation:

You should click Advanced settings in each Cisco Jabber client and configure the IP addresses of the servers in the appropriate fields if you are manually configuring Cisco Jabber to connect to your company's Cisco Unified Communications Manager (UCM) 8.6 deployment. Cisco Jabber's Advanced settings dialog box contains several fields that can be used to configure how Cisco Jabber connects to UCM services, as shown in the following exhibit:



Advanced settings

Select your account type:

- Automatic
- Cisco IM & Presence
- WebEx Messenger
- Cisco Communications Manager 8.x
- Cisco Communications Manager 9 or later

Login server:

- Use the default servers
- Use the following servers

TFTP server: 192.168.51.10

CTI server: 192.168.51.9

CCMCIP server: 192.168.51.9

Save Cancel

In the exhibit above, the Cisco Jabber account type is configured to Cisco Communications Manager 8.x. In addition, the login server is configured to Use the following servers and the appropriate IP addresses have been configured in each of the server fields. Cisco Jabber's Advanced settings dialog box features an Automatic option that allows Cisco Jabber to automatically configure itself as long as all of the following are true:

1. UCM is operating at release 9 or later.
2. A correct _cisco-uds Service (SRV) record has been configured on the Domain Name System (DNS) server.
3. Automatic is selected in Advanced settings.
4. An instant message (IM) and Presence Service profile has been configured in UCM.
5. The IM and Presence Service profile has been correctly applied to end users in UCM User Management.

There is not enough information in the scenario to determine whether a service profile has been configured, whether the DNS record is available, whether automatic configuration is selected, or whether the users have been configured with the IM and Presence Service. Even if that information were provided, the UCM deployment in this scenario is running release 8.6, which does not support the automatic configuration of Cisco Jabber clients.

You do not need to navigate to UCM Administrator's Service Profiles and configure the servers. However, you would navigate to UCM Administrator's Service Profiles and create an IM and Presence Service profile if you were configuring UCM to enable the automatic configuration of Jabber clients.

You do not need to navigate to UCM Administrator's User Management and configure the servers. However, you would navigate to UCM Administrator's User Management to apply an IM and Presence Service profile to the user accounts that would be associated with Cisco Jabber installations if you were configuring UCM to enable the automatic configuration of Jabber clients.

You do not need to edit DNS settings and configure SRV records for each of the services. However, you would configure an SRV record named _cisco-uds if you were configuring UCM to enable the automatic configuration of Cisco Jabber clients.

Reference:

[Cisco: Configure the Clients: Introduction to Client Configuration](#)

QUESTION 70

Which of the following can you display by clicking User Reports > Top N in the UCM 8.0 CAR GUI?

- A. the top number of billing errors
- B. the top call volume for a given period of time
- C. the top QoS rating information for inbound calls
- D. the top number of users by maximum length of calls

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can display information about the top number of users by maximum length of calls by using the User Reports menu. The By Duration report can be accessed by clicking User Reports > Top N in the Cisco Unified Communications Manager (UCM) Call Detail Records (CDR) Analysis and Reporting (CAR) graphical user

interface (GUI). This report enables a CAR administrator to view users who have made the longest calls over a given period of time, starting with the user who placed the longest call.

You can view information about the call volume for a given period of time by using the System Reports > Traffic > Summary by Phone Number report in the UCM CAR GUI. This report enables a CAR administrator to choose a range of time and IP phone extension numbers from which to view call volume information, thereby enabling an administrator to view what extensions were in use at a specific time.

You can view information about the current number of billing errors by using the System Reports > CDR Error report in the UCM CAR GUI. This report enables a CAR administrator to view the number of errors that occurred when CDR data was loaded into the reporting system.

You can view Quality of Service (QoS) rating information for inbound calls by using the System Reports > QoS > Detail report in the UCM CAR GUI. The Detail report enables a CAR administrator to choose a UCM network and a period of time for which to view QoS ratings for both inbound and outbound calls. The Detail report can be used to monitor QoS at a user level.

Reference:

Cisco: Understanding CAR System Reports: System Reports Summary Description

Cisco: Configuring Traffic System Reports: Configuring Traffic Summary by Phone Number Reports

QUESTION 71

Which of the following enables an administrator to view reports and manage UCM features?

- A. CAR
- B. RTMT
- C. Unified Serviceability
- D. Unified Reporting

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cisco Unified Serviceability enables an administrator to view reports and manage Cisco Unified Communications Manager (UCM) features. Unified Serviceability is a browser-based troubleshooting tool that uses Secure Hypertext Transfer Protocol (HTTPS) to access information that is provided by other reporting tools, such as Cisco Unified Real-Time Monitoring Tool (RTMT) and Cisco Unified Call Detail Records (CDR) Analysis and Reporting Tool (CAR).

Unified Serviceability provides access to several feature services that can be activated by using the Service Activation window, including database services, CDR services, and security services. You can access Unified Serviceability by clicking Navigation > Cisco Unified Serviceability from within the UCM administrative graphical user interface (GUI) or by using the HTTPS address <https://ipaddress:8443/ccmservice/>, where ip-address is the IP address of the UCM server or cluster.

You cannot manage UCM features by using Cisco Unified Reporting. Similar to Unified Serviceability, Unified Reporting is a browser-based troubleshooting tool that uses HTTPS to access information that is provided by other reporting tools, such as RTMT and CAR. However, Unified Reporting does not provide access to feature activation tools and network service activation tools. You can access Unified Reporting by clicking Navigation > Cisco Unified Reporting from within the

UCM administrative GUI or by using the HTTPS address `https://ipaddress:8443/cucreports/`, where ip-address is the IP address of the UCM server or cluster. For example, after you have navigated to Cisco Unified Reporting, you could navigate to System Reports > Unified CM Data Summary > Generate Report to monitor system activities.

You cannot manage UCM features by using CAR. CAR generates CDR reports, Quality of Service (QoS) reports, traffic reports, and billing reports. CAR reports are not real-time reports. You can access CAR by clicking Tools > CDR Analysis and Reporting in Unified Serviceability if you are a system administrator or by using the HTTPS address `https://ipaddress:8443/car/Logon.jsp`, where ip-address is the IP address of the UCM server or cluster, if you are a CAR administrator or user.

You cannot manage UCM features by using RTMT. RTMT is a client-side application that enables an administrator to monitor devices on a Cisco Voice over IP (VoIP) network in real time. RTMT uses HTTPS to connect to VoIP devices and gather information, such as device status and performance statistics, in real time. The data that is gathered by RTMT can then be used to pinpoint problems on the VoIP network or to monitor performance thresholds. To access RTMT, you should first ensure that the Cisco RTMT Reporter Servlet and Cisco Serviceability Reporter services are running in the UCM environment. Next, you should install the RTMT plugin on a workstation by clicking Application > Plugins in the UCM administrative graphical user interface (GUI). After you have installed the plugin, you should launch the Real-Time Monitoring Tool application on the workstation, type the appropriate IP address and credential information for accessing the UCM server or cluster, select the Secure Connection check box, and then click OK.

Reference:

Cisco: Understanding Services: Understanding Services

QUESTION 72

Which of the following best describes the purpose of the UCM DNA?

- A. It records outbound dialed numbers for later review in RTMT.
- B. It analyzes dialed numbers to determine how the call should be billed.
- C. It is used to test dial plans both before and after deployment.
- D. It maintains real-time device registration status information.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Cisco Unified Communications Manager (UCM) Dialed Number Analyzer (DNA) is used to test dial plans both before and after deployment. A dial plan is a set of rules, or route plan, that determines how calls reach their destinations. A Voice over IP (VoIP) dial plan enables a company to route calls between geographically dispersed sites while keeping the calls on-network. On-network calls are calls routed over a single network, such as an IP data network. By contrast, off-network calls are calls that are routed through multiple telephony networks, such as those routed over the public switched telephone network (PSTN). DNA and verification of the calling search space are both ways to troubleshoot error recordings when attempting to make off-network calls.

DNA does not record outbound dialed numbers for later review in the Cisco Unified Real-Time Monitoring Tool (RTMT). DNA initially displays results in a new browser window. However, you can export data from DNA in the form of an Extensible Markup Language (XML) file, not log data that is displayed by RTMT.

DNA does not maintain real-time device registration status information. The Cisco Real-time Information Server (RIS) maintains device registration statuses, performance counter information, and information about critical alarms in real time. Similar to DNA, the Cisco RIS Data Collector, which transmits data to the RIS, runs as a UCM service. If you notice that UCM-registered devices are not showing up in the UCM Administration pages, you should try restarting the Cisco RIS Data Collector service.

DNA does not analyze dialed numbers to determine how the call should be billed. Billing reports are typically generated by the Cisco Call Detail Records (CDR) Reporting and Analysis (CAR) tool. CAR also generates CDR reports, Quality of Service (QoS) reports, and traffic reports.

Reference:

[Cisco: Cisco Unified Communications Manager Dialed Number Analyzer Guide: Introduction: Dialed Number Analyzer](#)

QUESTION 73

You are deploying CUPS in order to enable your company's users to collaborate with each other.

Which of the following are you most likely to deploy as part of your CUPS installation? (Choose two.)

- A. Cisco UCCX
- B. Cisco UCCE
- C. Cisco Quality Management
- D. Cisco WebEx
- E. Cisco Jabber



Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most likely, you would deploy Cisco WebEx and Cisco Jabber as part of your Cisco Unified Presence (CUPS) installation. Cisco WebEx allows web conferencing in real time and can be deployed as an on-premises CUPS component or in the cloud. Cisco Jabber is an application that enables users to instant message (IM) or place audio or video calls without the use of a desk phone. CUPS integrates with an on-premises deployment of Cisco Unified Communications Manager (UCM).

You would not deploy Cisco Unified Contact Center Express (UCCX) or Cisco Unified Contact Center Enterprise (UCCE) as part of your CUPS installation. Each of these products is used to build business-to-customer contact centers. In addition, you would not deploy Cisco Quality Management as part of your CUPS installation. Cisco Quality Management is a set of applications that integrate with Cisco UCCX.

Reference:

[Cisco: Configuring Conferencing: Configure Conferencing for an On-Premises Deployment](#)

QUESTION 74

Which of the following statements is true?

- A. The auto-reg-ephone command can automatically create an ephone.
- B. The auto assign command can automatically create an ephone.

- C. The auto-reg-ephone command can automatically create an ephone-dn.
- D. The auto assign command can automatically create an ephone-dn.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The auto-reg-ephone command can automatically create an ephone. When an IP phone registers with a router that is configured with the auto-reg-ephone command, the router will associate the Media Access Control (MAC) address of the IP phone with the first unassigned ephone on the router. If all the ephones on the router are associated with IP phones, the router will create a new ephone, provided that the number of configured ephones does not exceed the value of the max-ephones command. The max-ephones command specifies the maximum number of ephones that you can configure on a router.

You can also manually assign an IP phone to an ephone by issuing the mac-address mac-address command in ephone configuration mode, where mac-address is the MAC address of the IP phone you want to assign to the ephone. For example, you can issue the following command set to associate an IP phone with the MAC address 0019:8765:4321 with ephone number 1:

```
telephony-service ephone 1
mac-address
0019.8765.4321
```



The auto-reg-ephone command cannot automatically create an ephone-dn. An ephone-dn must be configured before it can be assigned to buttons on ephones.

The auto assign command cannot automatically create an ephone or an ephone-dn. The auto assign command automatically associates button 1 on an ephone with an existing, unused ephone-dn. The ephone-dn is not automatically created? it must already exist. If no ephone-dn is available, the phone will register but none of the phone's buttons will be associated with ephone-dn extensions.

Reference:

[Cisco: Cisco Unified CME Commands: auto-reg-ephone](#) [Cisco:](#)

[Cisco Unified CME Commands: auto assign](#)

QUESTION 75

A user presses the messages button on a Cisco IP Phone 7961.

Which of the following will most likely happen?

- A. The user will receive a prompt from the voice mail system.
- B. The user will receive directory updates from the administrator.
- C. The user will receive application notifications from the administrator.
- D. The user will receive network notifications from the administrator.
- E. The user will receive system help notifications.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most likely, the user will receive a prompt from the voice mail system if the user presses the messages button on a Cisco IP Phone 7961. The Cisco IP Phone 7961 series includes a bank of buttons with iconography designed to represent the button's functions. For example, the messages button is represented by the back of a standard paper envelope. A typical bank of buttons for a Cisco IP Phone 7961 series appears in the following exhibit:





The user will not receive application notifications from the administrator by pressing the messages button. However, a user can launch Cisco Unified Communications IP phone applications by pressing the services button. The services button, which is represented by a globe icon, is used to launch IP phone applications. The applications that are available from the services button are dependent on the Cisco Unified Communications deployment and user privilege levels.

The user will not receive network notifications from the administrator by pressing the messages button. However, the settings button can enable a user to display information about the network to which the IP phone is connected or to configure some network and device settings. The settings button is represented by a selected check box and can be used to view or modify settings specific to the user or IP phone.

The user will not receive directory updates by pressing the messages button. However, a user can display directory information by pressing the directories button. The directories button, which is represented by an open book icon, is used to display lists of missed calls, received calls, placed calls, or local directory contacts. If configured, the directories button can also be used to access a custom Personal Speed Dial directory.

The user will not receive system help by pressing the messages button. However, the help button, which is represented by a question mark (?), is used to provide the end user with information about the specific features of the IP phone. A user can press the help button twice while on a call on an IP phone to view statistical information about the call, such as the codec that is being used by the IP phone, the codec that is being used by the calling phone, and packet error information.

Reference:

[Cisco: Cisco Unified IP Phone 7961G](#)

QUESTION 76

Which of the following VLANs can you configure on an FXO port?

A. no VLANs



<https://vceplus.com/>

- B. data VLANs
- C. native VLANs
- D. voice VLANs

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

There are no virtual LANs (VLANs) that you can configure on a foreign exchange office (FXO) port. FXO ports connect a voice gateway to the public switched telephone network (PSTN) or to a private branch exchange (PBX). A voice gateway is a router that is responsible for call processing and routing between the PSTN and a Voice over IP (VoIP) network, including the translation of analog voice signals to digital packets and vice versa.

You can configure voice VLANs only on Layer 2 access ports on a Cisco switch. Creating voice VLANs on a switch enables the separation of voice traffic from data traffic on a network. To enable the voice VLAN feature on a Cisco switch, you should issue the `switchport voice vlan {vlan-id | dot1p | none | untagged}` command in interface configuration mode. The `dot1p` keyword configures voice traffic to be sent with a default 802.1p priority of 5 and to use VLAN 0 as the VLAN ID.

The `switchport voice vlan vlan-id` command configures voice traffic to be tagged and sent over a user - specified voice VLAN. Voice traffic will be carried in 802.1Q frames and will be carried on a different VLAN than data traffic. For example, if you issue the `switchport voice vlan 2` command, voice traffic will be tagged with 802.1Q information and sent over VLAN 2.

Similar to the `switchport voice vlan untagged` command, the `switchport voice vlan none` command configures voice traffic to be untagged and sent over the same VLAN as data traffic, which is the native VLAN. When the `none` keyword is used, voice traffic does not use 802.1p priority tagging or Class of Service (CoS), and voice traffic is transmitted with data traffic.

The `switchport voice vlan untagged` command configures voice traffic to be untagged and sent over the native VLAN. However, if data and voice devices are configured to operate on the same VLAN, the voice traffic can experience quality problems, such as jitter or choppiness. Untagged traffic is sent without 802.1Q encapsulation. When the `switchport voice vlan untagged` command is issued, both voice traffic and data traffic are transmitted over the native VLAN. You do not need to specify a voice VLAN when the `switchport voice vlan untagged` command is used.

You can configure data VLANs and native VLANs on both trunk ports and access ports on a Cisco switch. To configure a data VLAN or the native VLAN on an access port, you should issue the `switchport access vlan vlan-id` command, where `vlan-id` is the ID of the data VLAN or the native VLAN you want to configure. To configure a trunk port with the native VLAN, you should issue the `switchport trunk native vlan vlan-id` command, where `vlan-id` is the ID of the native VLAN. In addition, trunk ports are by default configured to allow traffic from all data VLANs that are configured on the switch. You can issue the `switchport trunk allowed vlan remove vlan-id list` command to specifically remove a list of data VLANs from a trunk port. You can add a specific VLAN to a trunk port by issuing the `switchport trunk allowed vlan add vlan-id list` command, where `vlan-id list` is a list of the VLAN IDs you want to add.

Reference:

[Cisco: Understanding Foreign Exchange Office \(FXO\) Voice Interface Cards](#)

[Cisco: Configuring Voice VLAN: Configuring Voice VLAN](#)

QUESTION 77

Which of the following is not a method you can use to update the settings of existing users in Cisco Unity Connection?

- A. the BAT
- B. Bulk Edit mode
- C. editing user templates
- D. LDAP import

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Editing user templates is not a method that you can use to update the settings of existing users in Cisco Unity Connection. If you edit an existing user template, only new user accounts that are created by using that template will be affected by the changes that you make to the template. Any users who have already been created from the template will retain the old template settings.

The Bulk Administration Tool (BAT) is a method you can use to update the settings of existing users in Cisco Unity Connection. The BAT enables administrators to import users, update user settings, and delete users by importing comma-separated values (CSV) files. The BAT is also capable of exporting users to CSV files. For example, to modify the voice mail message length limit by using the BAT, you could export the voice mail users to a CSV file, change the message length limit value for each user in the CSV file, and then import the CSV file again.

Bulk Edit mode is a method you can use to update the settings of existing users in Unity Connection. Bulk Edit mode enables an administrator to select a specific subset of Unity Connection users and make identical changes to every user in that subset at once. For example, you can use Bulk Edit mode to modify the message length limit for all existing users who have voice mail. To edit a subset of users in Bulk Edit mode, you should click Users > Users in Unity Connection's graphical user interface (GUI) and then search for the subset of users you want to edit. When you have found the users you want to edit, select the check boxes beside those users and then click Bulk Edit. You can then modify the settings you want to change and apply the new settings by clicking the Submit button.

A Lightweight Directory Access Protocol (LDAP) import is a method you can use to update the settings of existing users in Unity Connection. The Cisco Directory Synchronization (DirSync) service enables Unity Connection to synchronize with LDAP directory services, such as Microsoft Active Directory. You must select the Cisco DirSync check box in the Directory Services area of the Unity Connection GUI to enable Unity Connection to synchronize with an LDAP directory. Changes you make to the LDAP directory will be reflected in Unity Connection accounts upon resynchronization of those accounts with the LDAP directory.

Reference:

[Cisco: Adding, Modifying, or Deleting a User Template in Cisco Unity Connection 8.x: Modifying a User Template in Cisco Unity Connection 8.x](#)

QUESTION 78

Which of the following Unity Connection features uses an XML-based service to import new users?

- A. import by using the BAT
- B. import from UCM
- C. synchronize with LDAP
- D. manual user entry

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Unity Connection import from Unified Communications Manager (UCM) feature uses an Extensible Markup Language (XML)based service to import, or onboard, new users. The Cisco Administrative XML Layer (AXL) Web Service is used to import UCM users into Unity Connection. The service must be enabled on both UCM and Unity Connection in order to import users. In addition, UCM users must be assigned a primary extension in UCM in order to be imported into Unity Connection by AXL.

You can enable the AXL Web Service in Unity Connection by clicking the Cisco AXL Web Service check box in Database and Admin Services in the Unity Connection administration graphical user interface (GUI). After you have enabled the service, you should configure the IP address, port number, user name, and password of the UCM AXL Web Service server in the AXL Servers area of the Unity Connection administration GUI. You can then click Users > Import Users to find user accounts on the UCM server and import them into Unity Connection.

The Bulk Administration Tool (BAT) does not use an XML-based service to import new users into Unity Connection. The BAT imports, updates, deletes, or exports users in Unity Connection in comma-separated values (CSV) format, not XML. You can access the BAT by clicking Tools > Bulk Administration Tool in the Unity Connection GUI.

Lightweight Directory Access Protocol (LDAP) does not use an XML-based service to import new users into Unity Connection. The Cisco Directory Synchronization (DirSync) service enables Unity Connection to synchronize existing Unity Connection users with LDAP directory services, such as Microsoft Active Directory. To enable Unity Connection to synchronize with an LDAP directory, you must select the Cisco DirSync check box in the Directory Services area of the Unity Connection GUI. In addition, you can import new users from LDAP by either using the BAT to import a CSV file or by using the Users > Import Users tool to import LDAP information that was previously imported into UCM to Unity Connection. Because Unity Connection stores users locally, a user that is synchronized with Unity Connection from LDAP will continue to be stored locally even if that user is later deleted from the LDAP database.

The Unity Connection manual user entry feature does not use an XML-based service to import new users. Instead, manual user entry enables an administrator to create new users one at a time. You can manually create a new user in Unity Connection by clicking Users > Users > Add New in the Unity Connection administration GUI.

Reference:

[Cisco: Cisco CallManager 4.1\(3\) AXL Programming Guide: Introduction](#)

[Cisco: Creating Multiple Cisco Unity Connection 8.x User Accounts from Cisco Unified Communications Manager Users: Importing Cisco Unified Communications Manager Users to Create Cisco Unity Connection 8.x Users \(Cisco Unified Communications Manager Version 5.x and Later\)](#)

QUESTION 79

Which of the following issues is most likely to prompt an administrator to verify a user's primary and proxy SMTP addresses in Cisco Unity Connection? (Select the best answer.)

- A. Secure messages cannot be played in Outlook.
- B. Messages are sent to the wrong email account.
- C. The MWI lamp turns off before a message is read in Outlook.
- D. No Single Inbox features are working.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

An administrator is most likely to verify that the user's primary or proxy Simple Mail Transfer Protocol (SMTP) address in Cisco Unity Connection matches the account to which the user wants voice mail messages relayed if messages are sent to the wrong email account. The Single Inbox feature of Cisco Unity Connection enables the synchronization of voice messages between Cisco Unity Connection and Microsoft Exchange Server mailboxes. For example, a voice mail left for a Cisco Unity Connection user can additionally be delivered to that user's Microsoft Outlook Inbox.

An administrator is not likely to verify a user's primary and proxy SMTP addresses in Cisco Unity Connection if no Single Inbox features are working. However, an administrator might verify that the Cisco Unified Messaging Service is enabled and running in Cisco Unity Connection if no Single Inbox features are working for the group of users that is associated with that Cisco Unified Messaging Service instance. In order for Single Inbox features to be available, the Cisco Unified Messaging Service must be enabled and started.

An administrator is not likely to verify a user's primary and proxy SMTP addresses in Cisco Unity Connection if the message waiting indicator (MWI) lamp turns off before a message is read in Microsoft Outlook. However, an administrator might verify that the Microsoft Outlook Mark Items as Read When Viewed in the Reading Pane check box is clear in the Outlook Options > Mail > Reading Pane dialog box. If this check box is selected, the MWI lamp will turn off when the user selects the message in Outlook's reading pane and there are no more new messages in Unity Connection.

An administrator is not likely to verify a user's primary and proxy SMTP addresses in Cisco Unity Connection if secure messages cannot be played in Outlook. However, an administrator might verify that Cisco Unity Connection ViewMail for Microsoft Outlook is installed on the user's workstation if secure messages cannot be played in Outlook. When Unity Connection delivers a secure voice mail to Microsoft Exchange, only the introductory text of the email is sent to the user. The audio file containing the message remains on Unity Connection. Cisco Unity Connection ViewMail enables users to listen to the voice mail audio files.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/9x/troubleshooting/guide/9xcuctsgx/9xcuctsg038.html#wp1083227

QUESTION 80

Which of the following interfaces enables database synchronization between UCM and a CUPS server? (Select the best answer.)

- A. AXL/SOAP
- B. LDAP
- C. SIP
- D. XMPP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Cisco Administrative Extensible Markup Language (AXL)/Simple Object Access Protocol (SOAP) interface enables database synchronization tasks from Cisco Unified Communications Manager (UCM) to a Cisco Unified Presence (CUPS) server database. UCM and CUPS together are the primary components of a Cisco Presence deployment. For synchronization to start, the Sync Agent service must be started on the CUPS server.

The Extensible Messaging and Presence Protocol (XMPP) interface does not enable database synchronization between UCM and a CUPS server. However, the XMPP interface is used to handle the exchange of availability information between UCM and XMPP clients, such as instant messaging (IM) clients that are developed by third parties.

The Session Initiation Protocol (SIP) interface does not enable database synchronization between UCM and a CUPS server. However, a SIP trunk interface does handle the exchange of availability information between UCM and a CUPS server. A UCM SIP trunk interface must point to the CUPS server in order for availability

information to be exchanged between the two systems. CUPS is also capable of sending SIP subscribe messages to UCM over the SIP trunk if UCM is configured as a Presence gateway.

The Lightweight Directory Access Protocol (LDAP) interface does not enable database synchronization between UCM and a CUPS server. However, the LDAP interface is used to synchronize user information between UCM and CUPS in order to create a single signon (SSO) user experience or to search for contacts. For example, a Cisco Unified Personal Communicator user can be authenticated to both the CUPS server and UCM by connecting directly to the CUPS server. LDAP listens on Transmission Control Protocol (TCP) port 389 unencrypted or on port 636 over Secure Sockets Layer (SSL). Thirdparty XMPP clients can also use LDAP to search the database and add users as contacts.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cups/8_6/english/configAdmin/CUPdeploy/dgfeaturesandfunctions.html#pgfId-1160393

QUESTION 81

You issue the following commands on a CME router:

```
Dial-peer voice 1 pots Destination-  
pattern 9911  
prefix 9  
port 1/0/0
```

Which of the following digits will be forwarded to the PSTN when a caller dials 9911? (Select the best answer.)

- A. 9
- B. 911
- C. 9911
- D. No digits will be forwarded.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The following command set will forward the digit 9 to the public switched telephone network (PSTN) when a caller dials 9911:

```
Dial-peer voice 1 pots Destination-  
pattern 9911  
prefix 9  
port 1/0/0
```

The dialpeer voice command is used to define how calls are routed to destination endpoints on either the PSTN or a Voice over IP (VoIP) network. To define call routing for the PSTN, you should issue the dialpeer voice command with the pots keyword.

The `destinationpattern` command is used to match both inbound and outbound dial peers. The sequence of dialed digits that will be matched for a dial peer can contain the digits 0 through 9, the asterisk (*), and the pound sign (#). In addition, you can use a period (.) as a wildcard symbol to refine the dialing pattern or to match multiple dial strings for a single dial peer. The command set in this scenario configures a dial peer on a Cisco Unified Communications Manager Express (CME) router to match the destination pattern 9911. By default, CME only forwards digits matched by wildcards in a destination pattern, not digits that are explicitly defined in the destination pattern. In the `destinationpattern 9911` command, all the destination pattern digits are explicitly defined. Therefore, CME will not forward any of the digits in the destination pattern when a user dials 9911.

The `prefix` command is used to add one or more digits to the front of the dial string before the dial string is forwarded to the destination network. Issuing the `prefix 9` command in this scenario ensures that the digit 9 will be forwarded to the PSTN, even though CME will automatically strip every digit in the destination pattern. Therefore, only the digit 9 will be forwarded to the PSTN when a caller dials 9911.

If the intent of the configuration in this scenario is to forward the emergency service code 911 to the PSTN, the configuration is incomplete. To configure the dial peer to forward the 911 emergency service code to the PSTN without forwarding the internal access code 9, you could do one of the following:

- A. Issue the `prefix 911` command instead of the `prefix 9` command.
- B. Issue the `forwarddigits 3` command instead of the `prefix 9` command.

The `port` command is used to configure a plain old telephone service (POTS) dial peer to send outgoing traffic destined for the PSTN through a specific port on a CME router. In addition, the `port` command is used to match incoming calls from the PSTN to POTS dial peers. In this scenario, the `port 1/0/0` command configures CME to forward outgoing calls made to 9911 through port 1/0/0 to the PSTN.

The `forwarddigits` command configures a dial peer to forward the rightmost number of digits matched by the destination pattern, even if the digits are explicitly matched. The number of digits forwarded by CME depends on the value configured in the `forwarddigits` command. For example, if you were to issue the `forwarddigits 4` command instead of the `prefix 9` command in this scenario, CME would forward the digits 9911 to the PSTN when a caller dials 9911. If you were to issue the `forwarddigits 4` command in addition to the `prefix 9` command, CME would forward the digits 99911 to the PSTN when a caller dials 9911.

Issuing the `forwarddigits implicit` command or the `no forwarddigits` command configures a dial peer to its default behavior of stripping digits that are explicitly matched in the destination pattern. Issuing the `forward-digits all` command configures a dial peer to forward every digit that matches the destination pattern, even if the digits are explicitly matched.

Reference:

<https://www.cisco.com/c/en/us/support/docs/voice/call-routing-dial-plans/14074-in-dial-peer-match.html>

QUESTION 82

Which of the following Cisco Unified Personal Communicator features require XMPP to communicate with CUPS? (Select 2 choices.)

- A. availability status
- B. contact searches
- C. instant messaging
- D. media streaming
- E. softphone mode signaling
- F. voice mail downloads

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Availability status and instant messaging (IM) require Extensible Messaging and Presence Protocol (XMPP) to communicate with Cisco Unified Presence (CUPS). XMPP is an open Extensible Markup Language (XML) IM and presence protocol. Cisco Unified Personal Communicator is software that enables a user to connect to several different communication services from a single application. CUPS is server software that integrates network traffic from several different communications services so that it can be transmitted over a Cisco Voice over IP (VoIP) network. CUPS also uses XMPP to communicate with thirdparty IM clients. In addition, CUPS uses Session Initiation Protocol (SIP) and SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) to integrate with thirdparty clients and applications. SIP is a call signaling protocol that is used by Cisco Unified Communications Manager (UCM) to communicate with collaboration endpoints, such as Unified Personal Communicator and Jabber.

Cisco Jabber, which also uses SIP and XMPP, is an application that is intended to integrate CUPS server services, such as user availability, with Microsoft Office. Cisco Jabber is also an IM client, a voice and video call client, and a desktop sharing client.

Unified Personal Communicator uses Lightweight Directory Access Protocol (LDAP) or LDAP Secure (LDAPS), not XMPP, to perform contact searches on an LDAP directory. LDAP is a directory protocol that is used by other servers, such as CUPS to perform contact lookups. LDAP listens on Transmission Control Protocol (TCP) port 389 unencrypted or on port 636 over Secure Sockets Layer (SSL) . In addition, Cisco Unified Communications Manager (UCM), Cisco Unity Connection, and CUPS can all synchronize user accounts and contacts from an LDAP directory, such as Microsoft Active Directory.

Unified Personal Communicator uses Realtime Transport Protocol (RTP), not XMPP, for media streaming. RTP is used to transport audio or video packets between devices on a VoIP network after a connection has been established. A twoway audio session, such as a telephone conversation, requires two RTP streams: one stream originating from each device. RTP sessions are established on evennumbered User Datagram Protocol (UDP) ports ranging from 16384 through 32767. Once an RTP stream is established on a UDP port, it remains on that port for the duration of the session.

Unified Personal Communicator uses SIP, not XMPP, for softphone mode signaling. SIP is an Internet Engineering Task Force (IETF)standard call signaling protocol. Although SIP is typically used as a peerto-peer call signaling protocol, it can also operate in client/server mode. A softphone is software that behaves like a phone, enabling a user to have voice conversations over a typical workstation network connection. Softphone mode is an operational mode that Unified Personal Communicator uses to act as a softphone.

Unified Personal Communicator uses Internet Message Access Protocol (IMAP), IMAP over SSL, or IMAP over Transport Layer Security (TLS), not XMPP, for voice mail downloads. Unified Personal Communicator uses IMAP over TLS to specifically communicate with Cisco Unity Connection. For other voice mail servers, either IMAP or IMAP over SSL can be used.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cupc/8_0/english/release/notes/cupc80.html#wp39407

QUESTION 83

You assign a UCM user to the Standard CAR Admin Users group in UCM. However, the user reports that CAR cannot be accessed from the Tools menu in Cisco Unified Serviceability.

Which of the following is most likely the cause of the problem? (Select the best answer.)

- A. The Cisco CAR Web Service is not running.
- B. The UCM system is generating CDR files too slowly.
- C. The user does not have the privileges to access CAR.
- D. The CDR Enabled flag is set to FALSE.
- E. The disk space where reports are stored is full.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most likely, the Cisco CAR Web Service is not running if Cisco Call Detail Records (CDR) Analysis and Reporting (CAR) cannot be accessed from the Tools menu in Cisco Unified Serviceability. If the CAR Web Service is not running, CAR will not be available from the Tools menu. To activate the CAR Web Service, click Tools > Service Activation in Cisco Unified Serviceability, select the call processing server from the Servers dropdown menu, and then select the check boxes next to the appropriate CDR services.

It is not likely that the CDR Enabled flag is the cause of the problem. The CDR Enabled flag determines whether a given Cisco Unified Communications Manager (UCM) server will generate CDR reports. If the CDR Enabled flag is not set to TRUE on a UCM server, CAR reports will not be generated for that server. In a UCM cluster, the CDR Enabled flag should be set to TRUE on the Publisher server and on all Subscriber servers in the cluster. In addition, you should verify that the Call Diagnostics are enabled and that the Cisco CAR Scheduler service is running on the Publisher server.

It is not likely that the rate at which the UCM system is generating CDR files is the cause of the problem. By default, every UCM server can generate one CDR file and one Call Management Records (CMR) file every minute for up to one hour. However, the rate at which UCM generates CDR files has nothing to do with whether the service is available from the Tools menu in Cisco Unified Serviceability. In addition, it is not likely that the amount of available disk space where reports are stored is the cause of the problem. The oldest CDR files are deleted on an hourly basis by the CDR Repository Manager's File Manager process if disk usage reaches a maximum threshold.

The user does have the privileges to access CAR. In this scenario, you have assigned the UCM user to the Standard CAR Admin Users group. By default, any UCM user can be configured as a CAR administrator by adding the user to the Standard CAR Admin Users group in UCM. This includes application users and end users. However, application users cannot access the Individual Bill report even though they might have read and write access to the CAR database.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/8_0_2/car/CAR/caranrpt.html#wp1050468

QUESTION 84

Your company synchronizes Microsoft Active Directory enduser accounts with UCM.

Which of the following tasks cannot be performed by using the UCM administrative GUI? (Select 2 choices.)

- A. assigning users to groups
- B. assigning an IP phone to a user
- C. assigning roles to user groups

- D. changing user PINs
- E. creating end-user accounts
- F. deleting end-user accounts

Correct Answer: EF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Because your company synchronizes Microsoft Active Directory end-user accounts with Cisco Unified Communications Manager (UCM), you cannot create enduser accounts by using the UCM administrative graphical user interface (GUI). In addition, you cannot delete end-user accounts by using the UCM administrative GUI.

When UCM is configured to synchronize with a Lightweight Directory Access Protocol (LDAP) directory, such as OpenLDAP or Microsoft Active Directory, the user ID and all user personal and organizational data that is stored in the LDAP directory, except for passwords, are replicated to the UCM database. It is important to note that the Cisco Directory Synchronization (DirSync) service must be activated before LDAP synchronization can take place.

When LDAP synchronization is configured, UCM configures the synchronized data as readonly data and acknowledges the LDAP directory as the central authority for creating and deleting user accounts. Therefore, UCM prevents administrators from using the UCM GUI to add and delete users. None of the data that was replicated to the UCM database can be modified by using the GUI. However, UCM user data that is not managed by the LDAP directory, such as the user's password and personal identification number (PIN), can be modified in the UCM administrative GUI.

You can assign roles to user groups in the UCM administrative GUI, even if your company synchronizes Microsoft Active Directory enduser accounts with UCM. UCM roles are configured with privileges that are specific to UCM, such as the ability to log in to the administrative GUI and the ability to modify specific configuration settings. Therefore, an administrator must be able to assign UCM roles to user groups in the UCM administrative GUI so that the end users in those groups can perform tasks in the GUI. However, UCM synchronization with LDAP overrides any role's privilege to add or delete UCM end users.

You can assign users to groups in the UCM administrative GUI, even if your company synchronizes Microsoft Active Directory enduser accounts with UCM. Because the user groups and user roles that control user privileges in UCM are unique to UCM, administrators must be able to assign those groups and roles to end users by using the UCM administrative GUI.

You can assign an IP phone to a user in the UCM administrative GUI, even if your company synchronizes Microsoft Active Directory enduser accounts with UCM. Because the enduser IP phone assignments are not stored in Active Directory, administrators must be able to assign those devices to end users by using the UCM administrative GUI.

You can change user PINs in the UCM administrative GUI, even if your company synchronizes Microsoft Active Directory enduser accounts with UCM. Because the enduser PIN assignments are not stored in Active Directory, administrators must be able to assign PINs to end users by using the UCM administrative GUI.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/8x/uc8x/directry.html#wp1067953

QUESTION 85

Which of the following fields is not available in the Cisco Unity Connection VoiceMailUser Template? (Select the best answer.)

- A. Alias
- B. Display Name
- C. Extension
- D. Alternate Extension
- E. Employee ID

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Alternate Extension field is not available in the VoiceMailUser Template. The Alternate Extension field is typically used in Cisco Unity Connection Administration to enable a single voice mailbox to serve more than one directory number (dn). For example, up to nine administrator configured alternate extensions, or lines, can be assigned to a single voice mailbox. These alternate extensions can be individual dns from the voice virtual LAN (VLAN) or the numbers of external devices. As a result, it is possible to enable a user to conveniently access Unity Connection from a mobile phone or from another IP phone. Similarly, an Alternate Extension can be used to access a single voice mailbox from multiple line appearances on a single IP phone. However, you can only add alternate extensions by editing a single user's account or by editing users in Bulk Edit mode.

The Alias field and the Extension field are mandatory fields in the VoiceMailUser Template when you manually create a new user with a voice mailbox in Cisco Unity Connection Administration. Cisco Unity Connection can integrate with various phone systems, including Cisco Unified Communications Manager (UCM). The Alias field holds the key that the Unity Connection database uses to identify a user; therefore, the Alias value must always be unique. The Extension field is used to link a UCM user to a Unity Connection mailbox; therefore, it is important that the Unity Connection user have an extension that matches the extension defined for the corresponding user in UCM. If the extension does not match, some of the Unity Connection integration features will not work correctly. For example, if you changed the extension for a user in UCM and did not make the corresponding change for the user in Unity Connection, the user could receive new voice mail in his or her mailbox but might not receive new voice message notifications to his or her IP phone.

Both the Display Name field and the Employee ID field are available in the VoiceMailUser Template. However, neither the Display Name field nor the Employee ID field is mandatory in the VoiceMailUser Template when you manually create a new user with a voice mailbox in Cisco Unity Connection Administration.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx/8xcucmac080.html#pgfId-1055920

QUESTION 86

Which of the following does not provide access to realtime reporting? (Select the best answer.)

- A. CAR
- B. RTMT
- C. Unified Serviceability
- D. Unified Reporting

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Cisco Unified Call Detail Records (CDR) Analysis and Reporting Tool (CAR) does not provide access to realtime reporting. CAR generates CDR reports, Quality of Service (QoS) reports, traffic reports, and billing reports from data that is stored in the CDR database. The reports can be automatically generated at scheduled intervals or generated manually. You can access CAR by clicking Tools > CDR Analysis and Reporting in Unified Serviceability if you are a system administrator or by using the Secure Hypertext Transfer Protocol (HTTPS) address <https://ipaddress:8443/car/Logon.jsp>, where ipaddress is the IP address of the Cisco Unified Communications Manager (UCM) server or cluster, if you are a CAR administrator or user.

Cisco Unified RealTime Monitoring Tool (RTMT) provides access to realtime reporting. RTMT is a clientside application that enables an administrator to monitor devices on a Cisco Voice over IP (VoIP) network in real time. RTMT uses HTTPS to connect to VoIP devices and gather information, such as device status and performance statistics, in real time. The data that is gathered by RTMT can then be used to pinpoint problems on the VoIP network or to monitor performance thresholds.

To access RTMT, you should first ensure that the Cisco RTMT Reporter Servlet and Cisco Serviceability Reporter services are running in the UCM environment. Next, install the RTMT plugin on a workstation by clicking Application > Plugins in the UCM administrative graphical user interface (GUI). After you have installed the plugin, you should launch the RealTime Monitoring Tool application on the workstation, type the appropriate IP address and credential information for accessing the UCM server or cluster, select the Secure Connection check box, and then click OK.

Cisco Unified Serviceability uses RTMT to provide access to realtime reporting. Unified Serviceability is a browserbased troubleshooting tool that uses HTTPS to access information that is provided by other reporting tools, such as RTMT and CAR. In addition, Unified Serviceability provides access to several feature services that can be activated by using the Service Activation window, including database services, CDR services, and security services. You can access Unified Serviceability by clicking Navigation > Cisco Unified Serviceability from within the UCM administrative GUI or by using the HTTPS address <https://ip-address:8443/ccmservice/>, where ipaddress is the IP address of the UCM server or cluster.

Cisco Unified Reporting uses RTMT to provide access to realtime reporting. Similar to Unified Serviceability, Unified Reporting is a browserbased troubleshooting tool that uses HTTPS to access information that is provided by other reporting tools, such as RTMT and CAR. However, Unified Reporting does not provide access to feature activation tools and network service activation tools. You can access Unified Reporting by clicking Navigation > Cisco Unified Reporting from within the UCM administrative GUI or by using the HTTPS address <https://ipaddress:8443/cucreports/>, where ipaddress is the IP address of the UCM server or cluster. For example, after you have navigated to Cisco Unified Reporting, you could navigate to System Reports > Unified CM Data Summary > Generate Report to monitor system activities.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/8_0_2/car/CAR/carovrvw.html#wp1101768

QUESTION 87

You are the administrator for your company's UCM network. Your company is running the UCM 8.6(1).

Examine the exhibit below, and answer the associated question:



You have verified that the softphone named Jabberwocky has been created and associated with the correct end user in UCM Administration.

Which of the following is least likely to have caused the Cisco Jabber error message? (Select the best answer.)

- A. The TFTP server is down.
- B. The IM and Presence server is down.
- C. Servers have not been configured by using host names.
- D. Cisco Jabber requires a fully qualified user name.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Although Cisco Jabber does require a fully qualified user name, such as joecambers@example.com, to register with Cisco Unified Communications Manager (UCM) and to configure a new Jabber user for the first time, typing an incorrectly formatted user name in an unconfigured or manually configured Cisco Jabber client will produce the following error message:





After Cisco Jabber has been correctly configured and registered with UCM for the first time, it is possible to log in to Jabber with only a shortened form of the user name in the user name field, as shown in the following exhibit:





However, if you mistype the user name or type a different, valid user name into the login field, Jabber will prompt you to verify that you want to completely reset the client configuration, as shown in the following exhibit:



Clicking Reset would cause Jabber to delete the current configuration and attempt to replace it with a new one for a different user name. Clicking Cancel returns the user to the login screen.

If Jabber had not been previously configured for a given user, Jabber would produce the following if provided with a short invalid user name:



Cisco Jabber uses Session Initiation Protocol (SIP) to connect to UCM in softphone mode. SIP is an Internet Engineering Task Force (IETF) standard call signaling protocol. Although SIP is typically used as a peer-to-peer call signaling protocol, it can also operate in client/server mode. A softphone is software that behaves like a phone, enabling a user to participate in voice sessions over a typical workstation network connection.

The Cisco Jabber client can be configured automatically by the UCM server or manually by clicking Advanced Settings from the login screen. Regardless of the configuration method, the Trivial File Transfer Protocol (TFTP) server and the Cisco Unified Communications Manager IP Phone (CCMCIP) server must be reachable by the client on which Jabber is installed. If the TFTP server is not available or is misconfigured, the Jabber client will not be able to download configuration files. If the CCMCIP server is not available or is misconfigured, Jabber cannot participate in instant messaging (IM) and Presence.

Cisco does not recommend configuring endpoints, whether they are desk phones or softphones like Cisco Jabber, by using host names. Configuring the Jabber client with server information by using host names instead of IP addresses could cause the error message in this scenario. When using host names or fully qualified domain names (FQDNs), the Domain Name System (DNS) server or local hosts file must be present and working. In addition, the Cisco Unified Presence (CUPS) server or IM and Presence server must be up and working. Otherwise, the user might receive a Cannot communicate with the server error message when attempting to log in, even if the login servers are correctly configured.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/10_5/CJAB_BK_D6497E98_00_deployment-installation-guide-ciscojabber/CJAB_BK_D6497E98_00_deployment-installation-guide-ciscojabber_chapter_01001.html

QUESTION 88

You issue the show running-config command on a CME router and receive the following partial output:



```
ip dhcp excluded-address 192.168.14.1 192.168.14.9
ip dhcp pool IPPhones
  network 192.168.14.0 255.255.255.240
  default-router 192.168.14.1
!
<output omitted>
!
interface FastEthernet 0/0
  ip address 192.168.14.1 255.255.255.0
  no shutdown
!
<output omitted>
!
dial-peer voice 2147483647 voip
  destination-pattern .T
  session target dns:192.168.14.11
  dtmf-relay sip-notify
  no vad
!
<output omitted>
!
ephone-dn 50
  number 5000
!
ephone-dn 51
  number 5001
!
ephone 20
  button 1:50
!
ephone 21
  button 1:51
  button 2:50
```



Examine the output, and use the information you gather to answer the question.

Which of the following statements about the dial peer configuration is true? (Select the best answer.)

A. The dial peer number is invalid.

- B. The destination pattern is invalid.
- C. The wrong keyword has been used to define the session target.
- D. The session target is the same as the default router.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The wrong keyword has been used to define the session target. Dial peer session targets can be specified by IP address or by host name. To specify a session target by IP address, you should configure the session target ipv4:ipaddress command, where ip address is the IP address of the router to which an outbound call matching the dial peer should be forwarded. To specify a session target by host name, you should configure the session target dns: hostname command, where hostname is the alphanumeric host name that is mapped to an IP address by a Domain Name System (DNS) server. The dns keyword also supports some wildcard options.

A voice gateway router will perform the following evaluations when it must send an outbound call:

1. The router will attempt to match the destination Dialed Number Identification Service (DNIS) to a destinationpattern string command on a digitbydigit basis, comparing the digit string to the destination pattern as the user dials the digits.
2. If the dial peer is a plain old telephone service (POTS) dial peer, the router will forward the call to the port indicated by the corresponding portport command.
3. If the dial peer is a Voice over IP (VoIP) dial peer, the router will forward the call to the IP address indicated by the corresponding session target ipv4: ipaddress command.
4. If no match is found, the call will be dropped.

The dial peer number is not invalid. A VoIP dial peer can be configured with any number in the range from 1 through 2145483647.

The destination pattern is not invalid. The dial peer command destination-pattern .T is used to indicate any string of up to 32 digits. The T character is used at the end of a string to instruct the router to wait for the complete dial string to be entered before matching a call to a dial peer.

The session target is not the same as the default router in this configuration. The default router is defined by the Dynamic Host Configuration Protocol (DHCP) defaultrouter 192.168.14.1 command. The session target is misconfigured and is therefore unlikely to map a host name of 192.168.14.11 to the default router's IP address of 192.168.14.1.

Reference:

https://www.cisco.com/c/en/us/td/docs/ios/12_2/voice/configuration/guide/fvfax_c/vvfpeers.html#wp1287795

QUESTION 89

Which of the following does Cisco recommend as the maximum amount of packet loss on a VoIP network? (Select the best answer.)

- A. 1 percent
- B. 3 percent
- C. 20 percent
- D. 50 percent

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cisco recommends a maximum packet loss of 1 percent for Voice over IP (VoIP) traffic. Packet loss is often caused when networks become congested and packets are dropped. Dropped packets can cause clips, or breaks, in the audio stream. However, voice traffic is more tolerant of dropped packets than of delayed packets because a small amount of packet loss is not noticeable to the human ear. Some codecs can correct small amounts of packet loss. On networks with limited bandwidth, a lowbitrate codec can mitigate packet loss. However, the overall quality of the audio will be reduced. Packet loss can also be mitigated by implementing Quality of Service (QoS) mechanisms.

Short delays and low packet loss on a VoIP network help protect the rate at which bits flow over the network. In addition to the packet loss recommendations, Cisco recommends a maximum jitter of 30 ms for VoIP traffic. Jitter is a variation in delay, which can cause voice traffic to arrive at different times, thereby causing breaks, or choppiness, in the audio stream. Jitter can be mitigated by implementing QoS mechanisms.

Cisco also recommends a maximum endtoend delay of 200 ms. The International Telecommunication Union (ITU) considers an endtoend delay of 150 ms or less to be acceptable for high voice quality. Delay, which is also called latency, can introduce interruptions in conversation flow, causing the speakers at each end of the circuit to interrupt each other. Endtoend delay can be mitigated by implementing QoS mechanisms.

Reference:

https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.pdf

QUESTION 90

You are the administrator for a small VoIP network connected to an ITSP in the United States. Your supervisor informs you that he is hearing a fast busy signal when he picks up the handset of his IP phone. You have verified that no other users are experiencing this problem.

In which of the following fault domains should you begin troubleshooting? (Select the best answer.)

- A. the IP phone
- B. the cable connecting the IP phone to the switch
- C. the network switch that is connected to the IP phone
- D. the voice network's router

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Because only one user is experiencing the problem, you should begin troubleshooting the IP phone fault domain. Fast busy signals can be caused by a codec mismatch between an IP phone and a Cisco voice gateway. You can determine what codec your supervisor's phone is using by pressing settings > Status > Call

Statistics on the IP phone keypad. The default audio codec on a Cisco voice gateway is the G.729 codec, which is a high-complexity compressed codec that consumes bandwidth at a rate of 8 Kbps.

You would not begin the troubleshooting process by examining the cable connecting the IP phone to the switch. You might check the cable connecting the IP phone to the switch or the switch port to which the cable is connected if the IP phone were a Power over Ethernet (PoE) device that was not receiving power from the switch or if Cisco Unified Communications Manager (UCM) reported that the device is of an unknown type. You might also check the network cable and switch port if the device were powered by a power supply but unable to register and download a configuration.

It is not likely that you would begin troubleshooting the network switch or the voice network's router in this scenario, because only one user is affected by the problem. You might begin troubleshooting the problem at the network switch if an entire department within an organization were reporting a problem. You might begin troubleshooting at the voice router if more than one department or the entire organization were experiencing a problem.

Reference:

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-maintenance-guides-list.html>

QUESTION 91

Which of the following is not true of both CUPS persistent chat rooms and CUPS ad-hoc chat rooms? (Select the best answer.)

- A. Neither room can be created or managed by users.
- B. Users cannot invite other users to a persistent room.
- C. The presence status of users cannot be viewed in an ad-hoc room.
- D. Both rooms are deleted when the last user logs out.
- E. Ad-hoc chat rooms allow the recording of transcripts.



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Both Cisco Unified Presence (CUPS) adhoc chat rooms and persistent chat rooms can be created or managed by users. There are two types of CUPS chat rooms: adhoc and persistent. Adhoc chat rooms are temporary. Persistent chat rooms, on the other hand, are always available in CUPS, even after all users have logged out. Support for persistent chat rooms must be specifically enabled when configuring CUPS.

Persistent chat rooms, not adhoc chat rooms, enable the recording of transcripts of the discussions that occur within the room. Persistent chat rooms therefore enable users to collaborate on and store information about longterm collaborative projects by using CUPS instant messaging (IM) and Presence. CUPS maintains no records or transcripts related to the adhoc chat room.

Both adhoc chat rooms and persistent chat rooms allow users to invite other users to the room. In addition, users can view the presence status of other users in a CUPS chat room regardless of the type of chat room. However, only an adhoc chat room is deleted when the last user logs out.

Reference:

<https://www.cisco.com/c/en/us/obsolete/unified-communications/cisco-unified-presence-version-8.5.html#pgfId-1091246>

QUESTION 92

You are deploying Cisco Jabber in a UCM 10.0 environment with full integration. You have already configured all of the following:

1. A `_cisco-uds` Service DNS SRV record for UCM on the DNS server
2. An IM and Presence Service Profile in UCM Service Profiles
3. End users with the IM and Presence Service Profile in UCM User Management You click the Advanced settings link in Cisco Jabber.

Which of the following radio buttons should most likely be selected for the Select your account type group in order to complete the Cisco Jabber configuration?
(Select the best answer.)

- A. Automatic
- B. Cisco IM & Presence
- C. WebEx Messenger
- D. Cisco Communications Manager 8.x
- E. Cisco Communications Manager 9 or later

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most likely, the Automatic radio button should be selected for the Select your account type group in Cisco Jabber's Advanced settings dialog box because, in this scenario, you have correctly configured all the requirements for enabling the automatic configuration of Cisco Jabber clients from Cisco Unified Communications Manager (UCM). Cisco Jabber's Advanced settings dialog box features an Automatic option that allows Cisco Jabber to automatically configure itself as long as all of the following are true:

1. UCM is operating at release 9 or later.
2. A correct `_cisco-uds` Service (SRV) record has been configured on the Domain Name System (DNS) server.
3. Automatic is selected in Advanced settings.
4. An instant message (IM) and Presence Service profile has been configured in UCM.
5. The IM and Presence Service Profile has been correctly applied to end users in UCM User Management.

The following exhibit displays the Cisco Jabber Advanced settings dialog box with the Automatic radio button selected:



Advanced settings

Select your account type:

- Automatic
- Cisco IM & Presence
- WebEx Messenger
- Cisco Communications Manager 8.x
- Cisco Communications Manager 9 or later

Login server:

- Use the default servers
- Use the following servers

TFTP server:

CTI server:

CCMCIP server:

Save Cancel



You would not select the Cisco Communications Manager 9 or later radio button unless you were configuring Cisco Jabber so that it could not be automatically configured by UCM. You might select the Cisco Communications Manager 9 or later radio button if you had not configured the _cisco-uds SRV record on the DNS server. Cisco Jabber relies on that SRV record to automatically connect to the appropriate UCM 9.0 or later services.

You would not select the Cisco Communications Manager 8.x radio button, because you have deployed UCM 10.0. In addition, you would not select either the Cisco IM & Presence radio button or the WebEx Messenger radio button, because those options do not allow Cisco Jabber to fully integrate with UCM.

Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/10_6/CJAB_BK_C56DE1AB_00_cisco-jabber-106-deployment-and-installation-guide/CJAB_BK_C56DE1AB_00_cisco-jabber-106-deployment-and_chapter_01010.html#CJAB_CN_CA735D5D_00

QUESTION 93

Which of the following can managers display by clicking Device Reports > Gateway in the CAR GUI? (Select the best answer.)

- A. the Gateway Detail report
- B. the Gateway Summary report
- C. the Gateway Utilization report
- D. none of the gateway reports

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

Explanation:

Only administrators can display reports by clicking Device Reports > Gateway in the Cisco Unified Communications Manager (UCM) Call Detail Records (CDR) Analysis and Reporting (CAR) graphical user interface (GUI)? managers cannot display reports by using this path. CAR provides three privilege levels for reporting: administrators, managers, and individual users. However, only administrators are permitted to view Gateway device reports.

The Gateway Detail report can be used to examine issues with a specific gateway. The Gateway Summary report can be used to examine a summary of every call that was transmitted through the gateways. Therefore, the Gateway Summary report can be used to monitor traffic and Quality of Service (QoS). The Gateway Utilization report can be used to determine whether a given gateway or gateways are over utilized. Therefore, you can use the Gateway Utilization report to determine whether new gateways need to be added to the network.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/7_1_2/car/CAR/cardvgat.html#wp1045126

QUESTION 94

Which of the following Unity Connection features cannot be modified from a user account's Phone Menu screen? (Select the best answer.)

- A. touchtone conversation style
- B. touchtone conversation live reply
- C. touchtone conversation menu style
- D. touchtone conversation speed

- E. touchtone conversation volume
- F. message locator sort order

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You cannot modify the Cisco Unity Connection touchtone conversation live reply feature from a user account's Phone Menu screen in the Unity Connection graphical user interface (GUI). Live reply is a Unity Connection Class of Service (CoS) feature that enables voice mail users to reply to a voice mail message by pressing a key on the IP phone keypad or by using the Unity Connection voice recognition feature. CoS feature settings can be modified only from the CoS screen, by using Bulk Edit Mode, or by using the Phone section of a Unity Connection user template. You can implement multiple CoS configurations in a single Unity Connection environment. Therefore, you can modify an individual CoS configuration or use Bulk Edit Mode to edit multiple CoS configurations. Until user templates and CoS have been configured, user accounts cannot be added to Unity Connection by using the Bulk Administration Tool (BAT).

The touchtone conversation style feature can be modified from a user account's Phone Menu screen in the Unity Connection GUI. A touchtone conversation is a series of voice prompts that users can answer by pressing keys on the IP phone keypad. The Touchtone Conversation dropdown field in the Touchtone Conversation Style area of the Phone Menu enables an administrator to choose from a list of available conversation styles. By default, the Touchtone Conversation dropdown field is set to Classic Conversation. The Touchtone Conversation field can be configured by editing individual user accounts, editing user templates, or editing user accounts in Bulk Edit Mode.

The touchtone conversation menu style feature can be modified from a user account's Phone Menu screen in the Unity Connection GUI. The Touchtone Conversation Menu Style field determines whether a user will hear a full set of instructions or a brief set of instructions after dialing into the voice mail system. Cisco recommends configuring the touchtone conversation style to Full for inexperienced users and Brief for experienced users. By default, the Touchtone Conversation Menu Style field is configured to Full for all users. The Touchtone Conversation Menu Style field can be configured by editing individual user accounts, editing user templates, or editing user accounts in Bulk Edit Mode.

The touchtone conversation speed feature can be modified from a user account's Phone Menu screen in the Unity Connection GUI. The Conversation Speed field determines the rate at which the touchtone conversation is played back to the user; it can be configured as Slow, Normal, Fast, or Fastest. The Conversation Speed field can be configured by editing individual user accounts, editing user templates, or editing user accounts in Bulk Edit Mode.

The touchtone conversation volume feature can be modified from a user account's Phone Menu screen in the Unity Connection GUI. The Conversation Volume field determines the decibel rate at which the touchtone conversation is played back to the user; it can be configured as Low, Medium, or High. The Conversation Volume field can be configured by editing individual user accounts, editing user templates, or editing user accounts in Bulk Edit Mode.

The message locator sort order feature can be modified from a user account's Phone Menu screen in the Unity Connection GUI. The Message Locator Sort Order field determines the order that voice mail messages are listed in when a voice mail user uses Message Locator to search for voice mail messages from other users. In order to use the Message Locator feature, you must select the Enable check box of the Finding Messages with Message Locator area of the Phone Menu. The Message Locator Sort Order drop-down field can be configured as Last In, First Out or First In, Last Out. The Message Locator Sort Order field can be configured by editing individual user accounts, editing user templates, or editing user accounts in Bulk Edit Mode.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx/8xcucmac050.html#pgfId-1056117

QUESTION 95

Which of the following is a Cisco voice messaging product that is typically installed in a router module slot? (Select the best answer.)

- A. CME
- B. UCM
- C. Unity
- D. CUE
- E. Unity Connection

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cisco Unity Express (CUE) is a voice messaging product that is typically installed in a router module slot on a Cisco Unified Communications Manager Express (CME) router. CUE provides voice mail messaging, automated attendant services, and interactive voice response (IVR) services. CUE can support a maximum of 250 voice mailboxes, depending on the license that is installed. Both CUE and CME can be administered by using either a commandline interface (CLI) or the browserbased graphical user interface (GUI).

CME is not a voice messaging product that is typically installed in a router module slot. CME is a call processing platform that is based on IOS and is contained within a Cisco Integrated Services Router (ISR). CME supports a maximum of 350 IP phones.

Cisco Unified Communications Manager (UCM) is not a voice messaging product that is typically installed in a router module slot. UCM is a call processing platform that can be installed on Cisco Media Convergence Servers, on a Cisco Unified Computing System, or on one of a specific list of thirdparty server platforms. UCM supports a maximum of 30,000 IP phones per cluster. UCM and its components can be administered by using Cisco Unified Operating System Administration. You can use the URL <http://ipaddress/ccmadmin>, where ip address is the IP address of a UCM server, to access Cisco Unified Operating System Administration.

Cisco Unity Connection is not a voice messaging product that is typically installed in a router module slot. Unity Connection is a voice messaging product that is typically installed as an appliance. Unity Connection supports a maximum of 250 voice messaging ports and 20,000 voice mailboxes. Unity Connection supports voiceenabled features, such as voice navigation and voice dialing; it can also be used to listen to audio translations of email messages.

Cisco Unity is not a voice messaging product that is typically installed in a router module slot. Unity is typically installed on Windows servers. Unity supports a maximum of 15,000 voice mailboxes.

Reference:

<https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unity-express/91195-chg-ipaddr-cue-module.html#intro>

QUESTION 96

Which of the following statements are true? (Select 2 choices.)

- A. A reset is faster than a restart.
- B. A reset restores the IP phone to the factory default settings.
- C. You can reset an IP phone by pressing **##*##** on the phone's keypad.
- D. You can restart an IP phone by pressing **##*##** on the phone's keypad.
- E. An IP phone reset contacts the TFTP server.
- F. An IP phone restart contacts the TFTP server.

Correct Answer: EF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Both an IP phone reset and an IP phone restart will contact the Trivial File Transfer Protocol (TFTP) server to check for and download phone configuration updates. A Cisco IP phone can be reset by issuing the reset command in ephone configuration mode on a Cisco Unified Communications Manager Express (CME) router or by pressing the ****#**** key sequence at the Settings menu of an IP phone. You can access the Settings menu of an IP phone by pressing the settings button on the phone's keypad.

A Cisco IP phone can be restarted by issuing the restart command in ephone configuration mode on a CME router. When you restart an IP phone, the phone will unregister and reregister with the Cisco call processing platform in addition to contacting the TFTP server. In the Cisco Unified Communications Manager (UCM) graphical user interface (GUI), you can restart a phone by clicking Device > Phone > Restart.

You must reset a phone after performing the following tasks:

- Updating the phone's firmware
- Modifying the Dynamic Host Configuration Protocol (DHCP) scope
- Changing the IP address of the TFTP server
- Changing Uniform Resource Locators (URLs)
- Changing the date and time settings
- Changing the language displayed on the phone
- Changing the call progress tones for the phone
- Changing the voice mail access number

You can either reset or restart a phone after performing the following tasks:

- Adding or deleting a phone button
- Associating a button with a new ephone-dn
- Modifying an extension on an ephone-dn
- Modifying speed-dial numbers on an ephone
- Enabling call park

Both the reset command on a CME router and the ****#**** key sequence on an IP phone perform a hard reset of the phone, similar to powering down the device and powering it back up again. In the UCM GUI, you can reset a phone by clicking Device > Phone > Reset. When you reset the IP phone, the phone contacts the

DHCP server to obtain IP configuration information, including the IP address of the TFTP server. The phone then contacts the TFTP server and downloads the most recent phone configuration information. The phone will also unregister and reregister with the Cisco call platform.

A reset is not faster than a restart. A restart is a soft reboot of the phone, which causes the phone to boot much quicker than a reset. When you restart an IP phone, the phone does not contact the DHCP server to obtain new IP configuration information. However, it does contact the TFTP server to download the most recent phone configuration information.

A reset does not restore the IP phone to the factory default settings. When an IP phone is restored to the factory default settings, any configuration changes that might be stored on the IP phone itself are lost. The method you use to restore a Cisco IP phone to factory default settings varies by phone model.

You can neither reset nor restart an IP phone by pressing `###` on the phone's keypad. The proper keypad sequence for resetting an IP phone is `**#**`. There is no similar keypad sequence for restarting an IP phone.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/admin/configuration/manual/cmeadm/cmreset.html#pgfId-1009231

QUESTION 97

Your company uses DRS to back up UCM data on a tape drive. You want to add a network directory as a DRS backup device.

Which of the following is required to complete your task? (Select the best answer.)

- A. IPSec
- B. SFTP
- C. SSL
- D. a cluster security password

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Secure File Transfer Protocol (SFTP) is required in order to add a network directory as a Cisco Unified Communications Manager (UCM) Disaster Recovery System (DRS) backup device. DRS is a Cisco application that can be used to back up data from UCM, Cisco Unity Connection, and Cisco Unified Presence (CUPS) server. SFTP is a file transport protocol that uses the secure transport protocol Secure Shell (SSH) to perform operations on remote file systems. Because SFTP is protected by a secure transport protocol, the transmission of data over an SFTP link is encrypted. DRS supports only tape devices and SFTP network directories as backup devices.

It is important to note that a backup device cannot be deleted from DRS if that backup device is part of an existing backup schedule. In order to remove an existing backup device from a DRS configuration, you must first ensure that the device has been removed from any backup schedules in which it might be configured.

Although DRS requires the cluster security password to encrypt backup data for storage, SFTP is specifically required to add a network directory. DRS uses the existing cluster security password when performing encryption on a backup. If the cluster security password is modified by using the commandline interface (CLI)

or by a fresh UCM installation, you might not be able to decrypt and restore that backup. Workarounds to this issue include remembering the old cluster security password that was used to encrypt the data or immediately performing a fresh backup when the cluster security password changes.

Although DRS requires Secure Sockets Layer (SSL) for authentication and encryption between Master Agents and Local Agents, SFTP is specifically required to add a network directory. Although DRS requires IP Security (IPSec) for public key infrastructure (PKI) encryption, IPSec is not required to add a network directory as a DRS backup device. Master Agents store component registrations, maintain scheduled tasks, and store backup data on a locally attached device. Local Agents, which are installed and activated by default on each cluster node, are responsible for running backup and restore scripts on the local server. The deletion of the IPSec trust store from UCM's security configuration can cause DRS to function improperly.

Reference:

https://www.cisco.com/en/US/docs/voice_ip_comm/cups/6_0_1/disaster_recovery/administration/guide/drsag601_2.pdf

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cu/cm/8_5_1/drsag851.html#wp42275

QUESTION 98

You have a Cisco CME router with CUE installed. You want to configure the router so that the MWI light will turn on when a user receives a voice mail message. All of the users have four-digit extensions.

You issue the following commands on the router:

```
ephone-dn 1  
mwi on
```



Which of the following commands could you issue to complete the configuration? (Select the best answer.)

- A. number *1
- B. number
- C. number 601
- D. number 6001....
- E. number 6001
- F. number *1

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You could issue the number 6001....command to complete the configuration so that the message waiting indicator (MWI) light will turn on when a user receives a voice mail message. The number command is used to create the code that Cisco Unity Express (CUE) sends to Cisco Unified Communications Manager Express (CME) whenever a user receives a voice mail message.

To configure MWI, you must create two ephonedns: one ephonedn to turn the MWI light on when the user receives a message, and one ephonedn to turn the MWI light off when the user retrieves all of his or her messages. When CUE receives a voice mail message for a user, CUE will send a code to the CME router to

indicate that the user's MWI light should be turned on. When the user retrieves the message, CUE will send another code to CME to indicate that the user's MWI light should be turned off.

The MWI codes can be any number of any length, as long as they are not the same as any existing extension numbers. To configure the MWI code that CUE will send to CME, you should issue the number command with the MWI code plus a number of periods equal to the number of digits in the users' extensions. For example, if you want to create MWI code 6001 and your system is configured to use four-digit extensions, you should issue the number 6001.... command in ephonedn configuration mode.

Finally, the ephonedn that is configured with the MWI code must also be configured with the mwi on or the mwi off command, depending on whether the ephonedn should be responsible for turning the MWI light on or off, respectively. For example, the following command set configures ephonedn 1 to turn on the MWI light for any fourdigit extension that is prefaced by the MWI code 6001: ephonedn 1 number 6001.... mwi on

Similarly, the following command set configures ephonedn 2 to turn off the MWI light for any fourdigit extension that is prefaced by the MWI code 6002:
ephonedn 2
number 6002....
mwi off

After CME receives a dialed string from CUE that contains the MWI code, CME will match the dialed digits to the ephonedn number pattern, strip off the explicitly matched MWI code, and change the state of the MWI light for the extension that matches the remaining forwarded digits. For example, in this scenario, CUE will send the digit string 60017777 to CME when the user at extension 7777 receives a voice mail message? CME will then strip off MWI code 6001 and turn on the MWI light for extension 7777.

You should not issue the number *1 command to complete the configuration. Although the number *1 command would configure ephonedn 1 to use the digits *1 to turn on the MWI light for an IP phone, the command does not define an extension number pattern. Therefore, the MWI light would not turn on for any phone extension.

You should not issue the number 601 command to complete the configuration. Although the number 601 command would configure ephonedn 1 to use the digits 601 to turn on the MWI light for an IP phone, the command does not define an extension number pattern. Therefore, the MWI light would not turn on for any phone extension.

You should not issue the number command to complete the configuration. Although the numbercommand would configure ephonedn 1 with a fourdigit extension number pattern, no MWI code would be explicitly defined. Therefore, dialing any fourdigit extension would cause CUE to simply dial the user's extension? it would not turn on the MWI light on a user's phone.

You should issue neither the number *1 nor the number 6001 command to complete the configuration. Unless you separate the extension numbers by using the secondary keyword, you cannot issue the number command with more than one extension number parameter? the MWI code and the extension number pattern should be typed together without a space between them.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/command/reference/cme_cr/cme_m1ht.html#wp1990978567

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/command/reference/cme_cr/cme_n1ht.html#wp1742630717

QUESTION 99

Which of the following can a user template automatically configure for a new user in Unity Connection? (Select 2 choices.)

A. a user alias

- B. an extension number
- C. an administrator role
- D. the message volume
- E. an SMTP address

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A user template can automatically configure an administrator role and the message volume for a new user in Cisco Unity Connection. Unity Connection user templates enable an administrator to automatically populate certain settings of a new user account based on the settings of a user template. The template settings are divided into two parts: basic settings and additional parameters. Administrator roles and the volume of message playback can be configured as additional parameters.

Templates are created in Unity Connection by clicking Templates > User Templates and then clicking Add New. Next, you should choose an existing template to use as the base for the new template. The template you choose as the base template can be one of the Unity Connection default templates, such as the Voice-mail User Template or the Administrator Template, or a custom template that you have previously configured. The new template will inherit all the settings of the base template except for settings that are unique to each template, such as the template alias and display name.

To configure a Unity Connection user template with an administrator role, you should select the administrator role you want to add from the list of options available on the Edit > Roles page of the template creation window. The following are the eight unique administrator levels that can be applied to a user template:

- Audio Text Administrator
- Greeting Administrator
- Help Desk Administrator
- Remote Administrator
- Mailbox Access Delegate Account
- Systems Administrator
- Technician
- User Administrator

The administrative abilities of the user accounts that are created from the new user template depend on the role you select in the template's configuration. If you do not select an administrator role when creating a new template, the user accounts that are created from the template will inherit the same abilities as those granted by the base template. For example, if you base the new template on Unity Connection's predefined Administrator Template, the template you create will inherit the Systems Administrator role from the predefined template. If the base template does not have an administrator role, new users created from the template will be created as regular, nonadministrator end users.

You can edit the message playback settings of the user template by clicking Edit > Playback Message Settings in the template creation window. In the Playback Settings area of the window, you can change the Message Volume dropdown field to Low, Medium, or High. The configuration of the Message Volume field determines the volume of voice mails and recorded instructions for faxing when the user plays those messages over the phone. You can also configure several

other message playback settings in the Playback Message Settings window, such as the number of recorded messages a user is allowed to save, the speed at which the messages play, and what information about a new message is announced to the user when that message is played for the first time.

A user template cannot automatically configure a user alias, an extension number, and a Simple Message Transfer Protocol (SMTP) address. The Alias field stores a user name, or alias, for the new user. The Extension field stores the telephone extension number that callers must dial to call the new user. The Alias field and the Extension field are required fields when you manually create a new user, even if the rest of that user's information is based on a user template. In addition, the Unity Connection administrative graphical user interface (GUI), not a user template, can automatically configure the SMTP Addressfield. The SMTP addresses that are created by the GUI are based on the user alias you assign in the Alias field, unless the Alias field contains characters that are not ASCII characters.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx/8xcucmac070.html#pgfId-1056275

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx/8xcucmac020.html#wp1049464

QUESTION 100

Two VoIP users and a mobile phone caller are participating in an active UCM call. No analog gateway is present on the network. During the call, one of the UCM subscriber servers fails.

Which of the following will occur? (Select the best answer.)

- A. The mobile phone caller will be disconnected.
- B. All three users will be disconnected.
- C. All three users will remain active on the call.
- D. The two VoIP users will be disconnected.



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The mobile phone caller will be disconnected because mobile phones, which place calls through the public switched telephone network (PSTN), are not supported by the Cisco Unified Communications Manager (UCM) call preservation feature. The call preservation feature enables some Voice over IP (VoIP) devices to continue active sessions even if UCM fails or communication between UCM and the device is interrupted.

When a UCM server fails, other UCM servers and supported devices in a cluster can detect the failure. UCM is then able to ensure that active calls remain active until either the users hang up or media stops streaming between the devices. Similarly, if UCM does not fail but loses connectivity to a device that is involved in an active call, both UCM servers and connected devices will detect the failure. The active call will remain active until the users end the call or media stops streaming between the devices.

When a supported device other than UCM fails, that device will no longer stream media. Thus the device is no longer able to participate in its active call. However, UCM will detect this failure and any other devices that might have been active on the same call will remain connected and active.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/8_0_1/ccmsys/accm-801-cm/a02dvsup.html#wp1020706

QUESTION 101

A user wants to ensure that callers from the voice VLAN and callers from the PSTN are directed to a voice mailbox if the line associated with the user's dn is in use.

Which of the following settings in the Call Forward and Pickup Settings section of the UCM Administration Directory Number Configuration page would enable this behavior? (Select 2 choices.)

- A. Forward All
- B. Forward Busy External
- C. Forward Busy Internal
- D. Forward No Answer External
- E. Forward No Answer Internal
- F. Forward Unregistered External

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, the Forward Busy External setting would forward public switched telephone network (PSTN) callers to a voice mailbox if the line associated with the user's directory number (dn) is in use. Similarly, the Forward Busy Internal setting would forward callers from the voice virtual LAN (VLAN) to a voice mailbox if the line associated with the user's dn is in use. The Cisco Unified Communications Manager (UCM) Administration Directory Number Configuration page enables a UCM administrator to configure several settings related to dns, including the following: call forwarding, call pickup, call waiting, line display text, ring settings, and voice mailboxes.

The Forward Unregistered External setting in the Call Forward and Pickup Settings section of the UCM Administration Directory Number Configuration page would direct a caller from the PSTN to voice mail if that caller attempted to connect to an extension that does not exist on your company's Voice over IP (VoIP) network. In contrast to the Forward Unregistered External setting, the Forward Unregistered Internal setting would forward internal callers to a specific voice mailbox if the internal caller dialed a nonexistent dn.

The Forward All setting forwards all callers, internal or external, to a specific voice mailbox. This is the same behavior as the CFwdAll softkey that appears on a Cisco IP phone. However, an administrator can configure this behavior for a user by accessing the Directory Number Configuration page if the user for some reason does not have access to the CFwdAll softkey.

The Forward No Answer External setting forwards any calls from the PSTN that go unanswered by the user. Similarly, the Forward No Answer Internal setting forwards any internal calls that go unanswered by the user.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/8_0_2/ccmcfg/bccm-802-cm/b03dn.html#wp1337027

QUESTION 102

Which of the following can you display by clicking System Reports > Traffic > Summary by Phone Number in the UCM 8.0 CAR GUI? (Select the best answer.)

- A. the current number of billing errors
- B. the call volume for a given period of time
- C. the QoS rating information for inbound calls
- D. the top number of users by maximum length of calls

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can display information about call volume for a given period of time by using the System Reports > Traffic > Summary by Phone Number report in the Cisco Unified Communications Manager (UCM) Call Detail Records (CDR) Analysis and Reporting (CAR) graphical user interface (GUI). This report enables a CAR administrator to choose a range of time and IP phone extension numbers from which to view call volume information, thereby enabling an administrator to view what extensions were in use at a specific time.

You can view information about the top number of users by maximum length of calls by using the User Reports menu. The By Duration report can be accessed by clicking User Reports > Top N in the UCM CAR GUI. This report enables a CAR administrator to view users who have made the longest calls over a given period of time, starting with the user who placed the longest call.

You can view information about the current number of billing errors by using the System Reports > CDR Error report in the UCM CAR GUI. This report enables a CAR administrator to view the number of errors that occurred when CDR data was loaded into the reporting system.

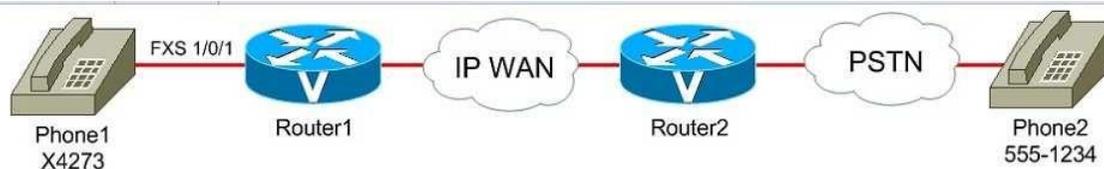
You can view Quality of Service (QoS) rating information for inbound calls by using the System Reports > QoS > Detail report in the UCM CAR GUI. The Detail report enables a CAR administrator to choose a UCM network and a period of time for which to view QoS ratings for both inbound and outbound calls. The Detail report can be used to monitor QoS at a user level.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/8_0_2/car/CAR/carsyrpu.html#wp1141383

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/8_0_2/car/CAR/carsytra.html#wp1037599

QUESTION 103



You issue the show running-config command on Router1 and Router2 and receive the following partial output on both routers: Dial-peer voice 7 voip destinationpattern session target ipv4:10.11.12.13

How will VoIP dial peer 7 be used when Phone1 calls Phone2? (Select the best answer.)

- A. Router1 will use it as an inbound dial peer.
- B. Router1 will use it as an outbound dial peer.
- C. Router2 will use it as an inbound dial peer.
- D. Router2 will use it as an outbound dial peer.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Router1 will use Voice over IP (VoIP) dial peer 7 as an outbound dial peer. A dial peer defines a logical route to a telephony endpoint. A voice gateway will match the call information with a dial peer configured on the router and create a corresponding call leg. A call leg is a logical inbound or outbound connection for a voice gateway. Dial peers that match inbound calls create inbound call legs, and dial peers that match outbound calls create outbound call legs.

A dial peer is a plain old telephone service (POTS) dial peer if the call comes from, or is destined to, an analog phone, the public switched telephone network (PSTN), or an analog public branch exchange (PBX). A dial peer is a VoIP dial peer if the call comes from, or is destined to, an IP phone or another voice gateway across an IP WAN.

In this scenario, Router1 is the originating voice gateway and Router2 is the terminating voice gateway. When Router 1 receives a call from Phone1, Router1 attempts to match the inbound call information to a POTS dial peer because Phone1 is an analog phone connected to a foreign exchange station (FXS) port on Router1. If no matching dial peer is found, Router1 will use the default dial peer. Dial peer 7 does not match, because it is a VoIP dial peer, not a POTS dial peer. Therefore, Router1 will not use dial peer 7 as an inbound dial peer.

Router1 must then send the call over an IP WAN network; therefore, Router1 attempts to match the outbound call information to a VoIP dial peer. If no matching dial peer is found, Router1 will drop the call. Dial peer 7 is a VoIP dial peer, and the destinationpattern command matches the destination number 5551234. Therefore, Router1 will use dial peer 7 as an outbound dial peer.

Router2 receives the inbound call from Router1 and attempts to match the inbound call information to a VoIP dial peer. If no matching dial peer is found, Router2 will use the default dial peer. Dial peer 7 does not match, because the destinationpatterncommand does not match the originating extension 4273. Therefore, Router2 will not use dial peer 7 as an inbound dial peer.

Finally, Router2 must send the call over the PSTN? therefore, Router2 attempts to match the outbound call information to a POTS dial peer and sends the call to Phone2 over the PSTN. If no matching dial peer is found, Router2 will drop the call. Dial peer 7 does not match, because it is a VoIP dial peer, not a POTS dial peer. Therefore, Router2 will not use dial peer 7 as an outbound dial peer.

A voice gateway router will perform the following evaluations when it receives an inbound call:

1. The router will attempt to match the destination Dialed Number Identification Service (DNIS) to an incoming called-number DNIS command.
2. The router will attempt to match the source Automatic Number Identification (ANI) to an answer-address ANI command.
3. The router will attempt to match the source ANI to a destination-pattern string command.
4. The router will attempt to match the incoming call's voice port to a port command.
5. If no match is found, the router will use the default dial peer.

Once a dial peer match is found, the router will immediately create an inbound call leg without proceeding to the next step. If multiple matches are found for a step, the router will select the longest explicit match. The default dial peer will only be used if no match is found. You cannot configure any of the settings for the default dial peer.

To create an outbound call leg, a voice gateway router will perform the following evaluations:

1. The router will attempt to match the destination DNIS to a destination-pattern string command.
2. If the dial peer is a POTS dial peer, the router will forward the call to the port indicated by the corresponding port port command.
3. If the dial peer is a VoIP dial peer, the router will forward the call to the IP address indicated by the corresponding session target ipv4: ip-address command.
4. If no match is found, the call will be dropped.

As with the inbound call leg, the router will immediately create an outbound call leg as soon as a match is found. If multiple matches are found for a step, the router will select the longest explicit match. The call will be dropped only if no match is found.

Reference:

<https://www.cisco.com/c/en/us/support/docs/voice/call-routing-dial-plans/12164-dialpeer-call-leg.html>

QUESTION 104

Users report that voice mail recordings are not loud enough.

Which of the following is least likely to aid in troubleshooting the problem? (Select the best answer.)

- A. adjusting AGC decibels
- B. disabling AGC
- C. obtaining a sniffer capture at the closest point to Unity Connection
- D. verifying the advertised codec settings

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, obtaining a sniffer capture at the closest point to Cisco Unity Connection is least likely to aid in troubleshooting the problem. However, you might obtain a sniffer capture of an audio stream before Unity Connection receives it as a step in troubleshooting garbled voice mail recordings.

Disabling Automatic Gain Control (AGC) or adjusting AGC decibels might aid in troubleshooting the problem. AGC enables Unity Connection to automatically adjust the audio volume of calls. You can adjust or disable AGC if users report that the audio volume of voice mail recordings is always too loud or always too soft.

Verifying the advertised codec settings might aid in troubleshooting the problem, especially if users are reporting no sound at all. An IP phone's codec must match the voice gateway's codec to enable a user to successfully place a call. In Unity Connection Administration, you can verify the codec's settings by examining the list of codecs in Telephony Integrations> Port Group.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/troubleshooting/guide/8xcuctsgx/8xcuctsg060.html#wp1052958

QUESTION 105

You are upgrading the firmware on all Cisco IP Phone 7961s that are connected to your company's network. All IP phones are configured to their default upgrade settings.

Which of the following upgrade methods will require the most administrative overhead? (Select 2 choices.)

- A. individual IP phone upgrades
- B. load server download
- C. peer firmware sharing
- D. traditional TFTP server download

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, individual IP phone upgrades and peer firmware sharing will require the most administrative overhead if the IP phones are configured to their default upgrade settings. By default, Cisco IP phones are configured to use the traditional Trivial File Transfer Protocol (TFTP) upgrade method. In order to enable peer firmware sharing, the administrator must enable it on each IP phone. Similarly, individual IP phone upgrades require the administrator to address each IP phone's upgrade individually.

When using the traditional TFTP server download method, each IP phone independently downloads the new image from the TFTP server in an "every man for himself" style strategy. When firmware images were small, this strategy was acceptable even when the IP phones were on a network at a separate location from Cisco Unified Communications Manager (UCM). Over time, IP phone firmware sizes have increased, which could cause slow upgrades over WAN links. In addition, the traditional TFTP download method could create high CPU usage on the UCM TFTP server.

You can also update the firmware on an individual IP phone by using the traditional TFTP method. First, you should make a note of the existing Phone Load Name value for the phone model that you want to upgrade by navigating to Device > Device Settings > Device Defaults in UCM Administrator. This is important because installing the new firmware image will automatically overwrite the value of the Phone Load Name field in Device > Device Settings > Device Defaults. You should then upload the new firmware to UCM by navigating to Software Upgrades > Install/Upgrade.

After you upload the new firmware, specify the name of the new firmware in the Phone Load Name field for the specific IP phone you want to upgrade by using UCM Administration's Device > Phone menu. Next, navigate to Device > Device Settings > Device Defaults and replace the new value of the Phone Load Name field with its original value. This will prevent other IP phones from downloading the new firmware after you restart the TFTP service.

Finally, you should restart the TFTP service in Cisco Unified Serviceability. After the service restarts, the IP phone you edited in UCM Administration should download the new firmware, upgrade the firmware, and restart. Other IP phones might restart as well. However, those IP phones will not be upgraded.

In contrast to the traditional TFTP server method, the load server download method enables the administrator of the LAN on which the IP phone operates to provide his or her own local TFTP server for firmware upgrades instead of relying on a remotely located default UCM TFTP server. This means that IP phones on remote networks will be able to download firmware updates in approximately the same amount of time it would take for an IP phone that is local to UCM. In addition, the TFTP load can be balanced among multiple TFTP servers at multiple sites. One disadvantage to the load server download method is that the local administrator is responsible for copying the firmware update to the TFTP server. Therefore, the TFTP upload and server configuration is subject to human error.

When peer firmware sharing is implemented, only one Cisco IP phone at a location is responsible for downloading the new firmware. The firmware is then distributed to the other IP phones on the LAN in a parent-child hierarchy. The downloading phone distributes the firmware to its children. Those children then distribute the firmware to their children, and so on. No one parent in the hierarchy can have more than two children. Some disadvantages to the peer firmware sharing method are that the hierarchies are limited to their own subnets and are specific to phone model. In addition, peer firmware sharing must be enabled on each IP phone.

Reference: https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-ip-phones-9900-series/white_paper_c11-583891.html <https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-ip-phone-7900-series/108090-upgrade-ip-firmware.html>

QUESTION 106

You are the administrator of a VoIP network. Your supervisor reports that calls to both internal and external users are connecting; however, users are unable to hear any audio. No recent configuration changes have been made to the VoIP network.

Which of the following is most likely the cause of the problem? (Select the best answer.)

- A. CUE network module failure
- B. Ethernet cable failure
- C. router WIC failure
- D. digital signal processor failure

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A digital signal processor (DSP) failure is most likely the cause of the problem. A DSP failure is likely if you are experiencing any of the following problems:

- Callers are unable to hear audio in one or both directions.
- Call setup is failing.
- Channels become stuck in the PARK state. -
- Error messages report DSP timeouts.

When analog audio is received by a DSP, the DSP samples and quantizes the analog audio data, encodes the data into binary format, and optionally, compresses it to conserve bandwidth. For example, Cisco Integrated Services Routers (ISRs) with DSP resources are used to process calls between Cisco Unified Communications Manager (UCM) and the public switched telephone network (PSTN).

A Cisco Unity Express (CUE) network module failure is not the cause of the problem. CUE is a voice mail and automated attendant hardware platform for small to medium-sized offices. It provides up to 250 mailboxes and up to 24 simultaneous voice sessions, depending on the CUE hardware platform. A CUE network module failure could result in a loss of voice mail and automated attendant features.

An Ethernet cable failure is not the cause of the problem. An Ethernet cable failure could result in a failure to connect to the voice router or voice gateway, thereby resulting in disconnected or intermittently disconnected calls.

A router WAN interface card (WIC) failure is not the cause of the problem. A router WIC failure could result in a loss of connectivity to an IP WAN, thereby resulting in disconnected calls or an inability to connect calls over the IP WAN.

Reference:

http://docwiki.cisco.com/wiki/Cisco_IOS_Voice_Troubleshooting_and_Monitoring_--_Digital_Signal_Processor_Troubleshooting#DSP_Symptoms

QUESTION 107

Your company has implemented Cisco Unity Connection. A user reports that outside callers are hearing a tone after recording 30 seconds of a voice mail message.

Which of the following is most likely true? (Select the best answer.)

- A. The user's Message Settings > Maximum Message Length field is configured to the default value.
- B. The user's Message Settings > Maximum Message Length field is configured to 30 seconds.
- C. The user's Message Settings > Maximum Message Length field is configured to more than 30 seconds.
- D. The user's Message Settings > Maximum Message Length field is configured to less than 30 seconds.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The user's Message Settings > Maximum Message Length field in the Cisco Unity Connection administrative graphical user interface (GUI) is most likely configured to more than 30 seconds. There are three typical ways to create users in Unity Connection: local manual creation, import from Cisco Unified Communications Manager (UCM), or synchronization by using Lightweight Directory Access Protocol (LDAP). When you edit users manually in the GUI, the Message Settings > Maximum Message Length field limits the length of voice mail messages that are left by outside callers. When the Maximum Message Length field is enabled, a caller will hear a tone as a warning that the maximum message length has almost been reached.

To modify the Maximum Message Length field value for a single user, you should edit the field on the Message Settings page of the user's account. You can also modify the setting for a number of users at once by editing the Maximum Message Length field in Bulk Edit Mode. In addition, you can configure the Maximum Message Length field on the Message Settings page of a voice mail user template to apply a nondefault maximum message length to any new user accounts that are based on the template.

It is not likely that the user's Message Settings > Maximum Message Length field is configured to the default value. By default, the Maximum Message Length field is configured to 300 seconds, or five minutes. If the user's Message Settings > Maximum Message Length field were configured to the default value, callers would not hear a warning tone until nearly 300 seconds of a message had been recorded.

It is not likely that the user's Message Settings > Maximum Message Length field is configured to 30 seconds. If the user's Message Settings > Maximum Message Length field were configured to 30 seconds, callers would not hear a warning tone until nearly 30 seconds of a message had been recorded. In this scenario, callers are hearing a warning tone after 30 seconds of the message has been recorded.

It is not likely that the user's Message Settings > Maximum Message Length field is configured to less than 30 seconds. If the user's Message Settings > Maximum Message Length field were configured to less than 30 seconds, callers would hear a warning tone before 30 seconds of a message had been recorded.

In this scenario, callers are hearing a warning tone after 30 seconds of the message has been recorded. Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/gui_reference/guide/8xcucgrgx/8xcucgrg010.html#pgfId-1051385

QUESTION 108

All of your department's IP phones are connected to a switch that does not support PoE. A DHCP server has been configured for the voice VLAN on the switch. Another administrator power cycles the switch without warning. No calls are in progress.

Which of the following is most likely to occur? (Select the best answer.)

- A. The IP phones will power down until the switch restarts.
- B. The IP phones will not be affected by the power cycle.
- C. The IP phones will disappear from the UCM configuration.
- D. The IP phones will reset and lose IP configuration information.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most likely, the IP phones will reset and lose IP configuration information when the administrator power cycles the switch because, in this scenario, the IP addressing information is automatically assigned to each IP phone by a Dynamic Host Configuration Protocol (DHCP) server. When an IP phone is disconnected from Cisco Unified Communications Manager (UCM), the phone will automatically reset in an attempt to re-establish communication. Therefore, if an IP phone suddenly resets or is continuously attempting to register with UCM, it is important to first verify the phone's connectivity to the network switch.

IP phones can be manually configured with IP addressing information. In that case, the IP phones would reset. Similarly, the IP phones will not be able to download configuration files from the Trivial File Transfer Protocol (TFTP) server until connectivity to the switch is restored.

The IP phones will not disappear from the UCM configuration. You can verify that an IP phone exists in the UCM by clicking Device > Phone > Find in UCM Administration and searching for the particular IP phone's Media Access Control (MAC) address. The IP phone will no longer be registered with UCM when it loses connectivity. However, the IP phone's record in the UCM configuration will remain there.

The IP phones will not power down until the switch restarts, because the switch in this scenario does not support Power over Ethernet (PoE). Therefore, the IP phones in this scenario must be connected to individual power supplies in order to obtain power. In addition to registration problems, IP configuration problems, and TFTP configuration problems, IP phones that are powered directly from a switch by using PoE will not be able to receive power until the switch has restarted. The IP phones will be affected by the power cycle. In addition to registration problems, IP configuration problems, and TFTP configuration problems, IP phones that are powered directly from a switch by using PoE will not be able to receive power until the switch has restarted. Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/7905g_7912g/5_0/sip/english/administration/guide/5_0/LowPtrb.html#wp1092158

QUESTION 109

Which of the following command sets presents the dial peer commands in the order that they are evaluated by a voice gateway for an inbound dial peer? (Select the best answer.)

- A. destination-pattern port
session target
- B. incoming called-
number answer-

- address destination-pattern port
- C. incoming called-number port session target destination-pattern
- D. portincoming called-number destination-pattern answer-address
- E. portincoming called-number answer-address

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The following command set presents the dial peer commands in the order that they are evaluated by a voice gateway for an inbound dial peer: incoming called-number answer-address destination-pattern port

A dial peer defines a logical route to a telephony endpoint. A voice router will perform the following evaluations when it receives an inbound call:

1. The router will attempt to match the destination Dialed Number Identification Service (DNIS) to an incoming called-number DNIS command.
2. The router will attempt to match the source Automatic Number Identification (ANI) to an answer-address ANI command.
3. The router will attempt to match the source ANI to a destination-pattern string command.
4. The router will attempt to match the incoming call's voice port to a port port command.
5. If no match is found, the router will use the default dial peer.

Once a dial peer match is found, the router will immediately route the call without proceeding to the next step. If multiple matches are found for a step, the router will select the longest explicit match. The default dial peer will only be used if no match is found. You cannot configure any of the settings for the default dial peer.

The dial peer evaluation process will occur for every call leg along the path from the source endpoint to the destination endpoint. A call leg is a logical inbound or outbound connection for a voice gateway. The originating voice gateway and the terminating voice gateway between two telephony endpoints have one call leg in the inbound direction and one call leg in the outbound direction. Therefore, there will be exactly two call legs for each voice gateway.

The session target command is not evaluated by a voice gateway router for an incoming dial peer; it is used by a voice gateway router to determine where to route an outgoing Voice over IP (VoIP) dial peer. A voice router will perform the following evaluations when it must send an outbound call:

1. The router will attempt to match the destination DNIS to a destination-pattern string command.
2. If the dial peer is a POTS dial peer, the router will forward the call to the port indicated by the corresponding port port command.

3. If the dial peer is a VoIP dial peer, the router will forward the call to the IP address indicated by the corresponding session target ipv4: ip-address command.
4. If no match is found, the call will be dropped.

The destination-pattern command is used for both inbound and outbound dial peer matching. However, the string variable must match the source ANI for inbound dial peer matching and must match the destination DNIS for outbound dial peer matching. The port-command is used for inbound POTS dial peer matching and to determine where to route an outgoing POTS dial peer.

Reference:

<https://www.cisco.com/c/en/us/support/docs/voice/call-routing-dial-plans/14074-in-dial-peer-match.html> <https://www.cisco.com/c/en/us/support/docs/voice/call-routing-dial-plans/12164-dialpeer-call-leg.html#peers>

QUESTION 110

With which of the following control components do UCM media resources interact when UCM needs to locate resources to establish transcoding? (Select the best answer.)

- A. call control
- B. media control
- C. MTP control
- D. MOH control

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cisco Unified Communications Manager (UCM) media resources interact with UCM's media control component in order to locate resources to establish transcoding, or to establish a media termination point (MTP). The UCM media control component is responsible for managing the creation and teardown of media streams for a given endpoint. The UCM Media Resource Manager is responsible for connecting the media streams that comprise conferencing features, among others. When troubleshooting media resource problems, such as conference call failures, it is important to first investigate the UCM media resources configuration. UCM media resources are available directly from the UCM server on which the services are enabled. In addition, the UCM Media Resource Manager enables UCM to provide those services to other UCM servers in a cluster.

UCM media resources do not interact with UCM's call control component when UCM needs to locate resources to establish transcoding. However, UCM media resources do interact with UCM's call control component when locating resources to establish a conference call or music on hold (MOH).

UCM media resources do not interact with UCM's MTP control component when UCM needs to locate resources to establish transcoding. UCM media resources interact with UCM's MTP control component in order to reserve transcoders within a UCM cluster.

UCM media resources do not interact with UCM's MOH control component when UCM needs to locate resources to establish transcoding. UCM media resources interact with UCM's call control component in order to locate resources to establish an MOH session. Because the MOH control enables UCM to redirect a caller to an audio server, UCM media resources also interface with the MOH control when establishing such a session.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/8_6_1/ccmsys/accm-861-cm/a05media.html#pgfId-1020235

QUESTION 111

Which of the following is a Cisco Unity Connection feature that you can modify in the Location section of the User Templates Basics page? (Select the best answer.)

- A. CoS
- B. partition
- C. search space
- D. time zone

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, only the Cisco Unity Connection time zone feature can be modified in the Location section of the User Templates Basics page. If your company's Cisco Unity Connection implementation must support users in different time zones, you can create a unique user template for each time zone. You can also adjust the system default language in this section of a user template.

You can modify the Class of Service (CoS) settings, the partition, and the search space in the Phone section of the Cisco Unity Connection User Templates Basics page.

CoS settings enable an administrator to apply a specific set of privileges to Cisco Unity Connection users. A partition is a logical grouping of Voice over IP (VoIP) route patterns and directory numbers (dns). A search space is an ordered list of partitions that a device is allowed to search for patterns that match a dialed number.

Reference:

<https://www.cisco.com/c/en/us/obsolete/unified-communications/cisco-unified-communications-manager-version-7.1.html#uc-bulk>

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/9x/user_mac/guide/9xcucmacx/9xcucmac020.html#pgfId-1049464 **QUESTION 112**

You want to view information about called numbers that have cost the most over a given period of time in Cisco Unified Serviceability's System Overview report.

Which of the following sections of the report should you examine? (Select the best answer.)

- A. Top 5 Users based on Charge
- B. Top 5 Destinations based on Charge
- C. Top 5 Calls based on Charge
- D. Traffic Summary Report -Hour of Day
- E. Gateway Summary Report

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To view information about called numbers that have cost the most over a given period of time, you should examine the Top 5 Destinations based on Charge section of the System Overview report in Cisco Unified Serviceability. Cisco Unified Communications Manager (UCM) Call Detail Records (CDR) Analysis and Reporting (CAR) administrators can display the System Overview report by clicking Tools > System Reports > System Overview in Cisco Unified Serviceability.

The System Overview report contains all of the following sections:

- Top 5 Users based on Charge: lists the five users whose calls have cost the most over a given period of time
- Top 5 Destinations based on Charge: lists the five called numbers that have cost the most over a given period of time
- Top 5 Calls based on Charge: lists the five calls that have cost the most over a given period of time
- Top 5 Users based on Duration: lists the five users who have spent the most time on calls over a given period of time
- Top 5 Destinations based on Duration: lists the five called numbers on which users have spent the most time over a given period of time
- Top 5 Calls based on Duration: lists the five longest calls over a given period of time
- Traffic Summary Report -Hour of Day: displays the volume of calls for a given hour- of the day
- Traffic Summary Report -Day of Week: displays the volume of calls for a given day of the week
- Traffic Summary Report -Day of Month: displays the volume of calls for a given day of the month
- Quality of Service Report -Summary: displays the number of calls that fell within Quality of Service (QoS) parameters over a given period of time - Gateway Summary Report: displays the call classification, QoS, duration, and number of calls for each voice gateway over a given period of time

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/7_1_2/car/CAR/carsyovw.pdf

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/8_0_2/car/CAR/carsysrr.html#wpxref43862

QUESTION 113

Which of the following can you display by clicking System Reports > Traffic > Summary by Phone Number in the UCM 8.0 CAR GUI? (Select the best answer.)

- A. the current number of billing errors
- B. the call volume for a given period of time
- C. the QoS rating information for inbound calls
- D. the top number of users by maximum length of calls

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can display information about call volume for a given period of time by using the System Reports > Traffic > Summary by Phone Number report in the Cisco Unified Communications Manager (UCM) Call Detail Records (CDR) Analysis and Reporting (CAR) graphical user interface (GUI). This report enables a CAR

administrator to choose a range of time and IP phone extension numbers from which to view call volume information, thereby enabling an administrator to view what extensions were in use at a specific time.

You can view information about the top number of users by maximum length of calls by using the User Reports menu. The By Duration report can be accessed by clicking User Reports > Top N in the UCM CAR GUI. This report enables a CAR administrator to view users who have made the longest calls over a given period of time, starting with the user who placed the longest call.

You can view information about the current number of billing errors by using the System Reports > CDR Error report in the UCM CAR GUI. This report enables a CAR administrator to view the number of errors that occurred when CDR data was loaded into the reporting system.

You can view Quality of Service (QoS) rating information for inbound calls by using the System Reports > QoS > Detail report in the UCM CAR GUI. The Detail report enables a CAR administrator to choose a UCM network and a period of time for which to view QoS ratings for both inbound and outbound calls. The Detail report can be used to monitor QoS at a user level. Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/8_0_2/car/CAR/carsyrpu.html#wp1141383

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/8_0_2/car/CAR/carsytra.html#wp1037599

QUESTION 114

You have enabled SIP Early Offers.

Which of the following is most likely the reason? (Select the best answer.)

- A. A service provider requires it.
- B. Analog audio must be compressed in the stream.
- C. Codec conversion is required.
- D. H.323 trunks are in use.



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, you are most likely to enable Session Initiation Protocol (SIP) Early Offers if a public switched telephone network (PSTN) service provider requires it. By default, Cisco Unified Communications Manager (UCM) uses SIP Delayed Offers. UCM uses the SIP Offer/Answer model to establish SIP sessions. SIP Offers, which are messages sent in the Session Description Protocol (SDP) fields of a SIP message, contain information about the streams, codecs, IP addresses, and ports supported by the device. The remote device receives the SIP Offer and sends a SIP Answer in the SDP fields of its response. SIP Early Offers are sent by the session initiator in the SIP Invite, before the session is established. SIP Delayed Offers are sent by the session initiator after the receiver sends its capabilities.

Delivering SIP Early Offers over SIP trunks is a function of Media Termination Points (MTPs). There are two ways to enable Early Offers on SIP trunks in Cisco Unified Communications Manager (UCM): select the MTP Required check box on the SIP trunk or select the Early Offer support for voice and video calls (insert MTP if needed) check box on the SIP profile that is connected to the SIP trunk. If MTP is required, all outbound calls will use MTP, as will calls operating on the same codec. If MTP is enabled as needed, it is inserted if the trunk is incapable of sending complete information about its media capabilities in the SIP Invite message.

Converting digital audio from one codec to another is a function of a transcoder. Transcoders enable communication between devices that support dissimilar audio codecs. For example, a transcoder can translate a G.729 encoded packet to a G.711 encoded packet and vice versa. Transcoders translate the data stream in real time between two devices so that no audio delay is experienced by either endpoint.

Sampling, encoding, and compression of analog audio is a function of a digital signal processor (DSP). DSPs execute the steps required to convert an analog voice signal to digital packets, which allow voice data to traverse a Voice over IP (VoIP) network. There are four steps involved in converting analog audio data to digital audio data: sampling, quantization, encoding, and compression.

Providing connectivity for SIP devices and H.323 devices is a function of a UCM's SIP trunks and H.323 trunks, respectively, not of MTPs. UCM supports both SIP trunks and H.323 trunks. Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/9x/uc9x/trunks.html#wp1126439

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/7x/uc7_0/trunks.html#wp1045957

QUESTION 115

A user informs you that CAR queries are failing consistently for recent dates. However, older dates are still accessible. Which of the following is most likely the problem? (Select the best answer.)

- A. The Cisco CAR Web Service is not running.
- B. The UCM system is generating CDR files too slowly.
- C. The user does not have the privileges to log on to CAR.
- D. The CDR Enabled flag is set to FALSE.
- E. The disk space where reports are stored is full.



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the choices provided, the problem is mostly likely that the CDR Enabled flag is set to FALSE if Cisco Call Detail Records (CDR) Analysis and Reporting (CAR) queries are failing consistently for recent dates but older dates are still accessible. If the CDR Enabled flag is not set to TRUE on a Cisco Unified Communications Manager (UCM) server, CAR reports will not be generated for that server. In a UCM cluster, the CDR Enabled flag should be set to TRUE on the Publisher server and on all Subscriber servers in the cluster. If the CDR Enabled flag is already set to TRUE, you should verify that only the Publisher server has the Cisco CDR Insert service activated. In addition, you should verify that the Call Diagnostics are enabled and that the Cisco CAR Scheduler service is running on the Publisher server.

It is likely that the Cisco CAR Web Service is running if older dates are still accessible, even though CAR queries are failing consistently for recent dates. CAR is typically accessed by using the Tools menu in Cisco Unified Serviceability. If the CAR Web Service were not running, CAR would not be available from the Tools menu. Thus the user would have no way of knowing whether recent queries were failing or whether older dates were still accessible. To activate the CAR Web Service, click Tools > Service Activation in Cisco Unified Serviceability, select the call processing server from the Servers dropdown menu, and then select the check boxes next to the appropriate CDR services.

It is not likely that the UCM system is generating CDR files too slowly. By default, every UCM server can generate one CDR file and one Call Management Records (CMR) file every minute for up to one hour. In addition, it is not likely that the disk space where reports are stored is full. The oldest CDR files are deleted on an hourly basis by the CDR Repository Manager's File Manager process if disk usage reaches a maximum threshold. Therefore, if the disk were full, older dates would be affected by the issue, not recent ones.

It is not likely that the user does not have the privileges to log on to CAR, because the user can see the results of older queries. By default, any UCM user can be configured as a CAR administrator by adding the user to the Standard CAR Admin Users group in UCM. This includes application users and end users. However, application users cannot access the Individual Bill report even though they might have read and write access to the CAR database.

Reference:

<https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/68010-carfailure.html#solution>

QUESTION 116

A user has asked you to configure an IP phone PIN so that the user can circumvent afterhours call blocking restrictions. Which of the following PINs will the CME router not accept? (Select 2 choices.)

- A. 123
- B. 4312
- C. 5670192
- D. 12943560112
- E. 34872345

Correct Answer: AD

Section: (none)

Explanation



Explanation/Reference:

Explanation:

The Cisco Unified Communications Manager Express (CME) router will not accept a personal identification number (PIN) of 123, because that PIN is too short. In addition, the CME router will not accept a PIN of 12943560112, because that PIN is too long. CME administrations can issue the pin number command in ephone configuration mode to configure a specific IP phone with a PIN. The number parameter accepts a numeric string with a length in the range from four digits through eight digits. Therefore, you cannot configure a PIN of less than four digits nor can you configure a PIN of more than eight digits.

When an ephone is configured with a PIN, that PIN can be used to circumvent any afterhours calling restrictions that have been placed on the ephone. Afterhours calling restrictions are typically used to prevent certain types of calls from taking place during a specifically defined time period. For example, you could configure a calling restriction that prevents calls to longdistance numbers from the time your company closes for the day until the time it reopens for the next business day.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/command/reference/cme_cr/cme_p1ht.html#wp1592178732

QUESTION 117

Which of the following tools can be used to export data from both Cisco Unity and Cisco Unity Connection? (Select the best answer.)

- A. the BAT
- B. COBRAS
- C. Cisco Unity to Connection Migration Export Tool
- D. DiRT for Unity
- E. DiRT for Connection

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the choices provided, only the Cisco Object Backup and Restore Application Suite (COBRAS) can be used to export data from both Cisco Unity and Cisco Unity Connection. COBRAS is a suite of applications that can be used to import and export data for Unity or Unity Connection. In addition, you can import a Unity export from COBRAS into Unity Connection. For example, you can use COBRAS Export for Unity to extract information from Unity 4.0(5) and later and then use COBRAS Import for Connection to import the Unity data into Unity Connection 7.0 or later.

Cisco Unity is a voice mail server that runs on Microsoft Windows? it can integrate with Cisco Unified Communications Manager (UCM), Microsoft Exchange Server, and Lotus Domino. Cisco Unity supports a subscriberbased model instead of a userbased model, meaning that Unity subscribers are stored in a database that is separate from Unity, such as UCM, Microsoft Exchange Server, or Lotus Domino.

Cisco Unity Connection, on the other hand, is a voice mail server that runs on Linux? it can use Internet Message Access Protocol (IMAP) to retrieve email and collaboration information from Microsoft Exchange Server and Lotus Domino. Unity Connection supports a userbased model, meaning that users can be imported to Unity Connection from UCM, Microsoft Exchange Server, or Lotus Domino. Unity Connection stores its own users.

You cannot use the Bulk Administration Tool (BAT) to export data from both Cisco Unity and Cisco Unity Connection. Instead, you can use the BAT to export data from Unity Connection into commaseparated values (CSV) format. In addition, the BAT enables administrators to import users, update user settings, and delete users by importing CSV files.

You cannot use Disaster Recovery Tools (DiRT) for Connection to export data from both Cisco Unity and Cisco Unity Connection. In addition, you cannot use DiRT for Unity to export data from both Cisco Unity and Cisco Unity Connection. DiRT is a set of two applications: Disaster Recover Backup and Disaster Recover Restore. Furthermore, there are two different versions of DiRT. You can use DiRT for Connection to back up and restore data in only Unity Connection. You can use DiRT for Unity to back up and restore data in only Unity.

You cannot use the Cisco Unity to Connection Migration Export Tool to export data from both Cisco Unity and Cisco Unity Connection. Instead, you can use the Cisco Unity to Connection Migration Export Tool to export data from Unity into CSV format. You can then use the BAT to import the CSV file into Unity Connection.

Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/upgrade/guide/8xcucrugx/8xcucrug020.html

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/upgrade/guide/8xcucrugx/8xcucrug022.html

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/upgrade/guide/8xcucrugx/8xcucrug024.html#wp1063157

QUESTION 118

You issue the show running-config command on a CME router and receive the following partial output:

```
ip dhcp excluded-address 192.168.14.1 192.168.14.9
ip dhcp pool IPPhones
  network 192.168.14.0 255.255.255.0
  default-router 192.168.14.1
!
<output omitted>
!
interface FastEthernet 0/0
  ip address 192.168.14.1 255.255.255.0
  no shutdown
!
<output omitted>
!
dial-peer voice 1 pots
  destination-pattern .T
  direct-inward-dial
  port 1/0/0
!
<output omitted>
!
ephone-dn 50
  number 5000
!
ephone-dn 51
  number 5001
!
ephone 20
  button 1:50
!
ephone 21
  button 1:51
  button 2:50
```



Examine the output, and use the information you gather to answer the question.
Which of the following statements is true? (Select the best answer.)

- A. There will be no delay after the phone number is dialed.
- B. IP phones will not be able to download their configurations.

- C. IP phones will require manual IP address configuration.
- D. No dialed digit can be matched.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

IP phones will not be able to download their configurations from a Trivial File Transfer Protocol (TFTP) server, because the option 150 ip ipaddress command is missing from the Dynamic Host Configuration Protocol (DHCP) configuration in the output above. To automatically assign a TFTP server to IP phones, you should issue the option 150 ip ipaddress command, where ipaddress is the address of the TFTP server. A TFTP server is required so that IP phones can download their startup configuration files. In this scenario, the option 150 ip 192.168.14.1 command would configure the DHCP server on the Cisco Unified Communications Manager Express (CME) router to assign the TFTP server address of 192.168.14.1 to IP phones that are configured by using DHCP.

There will be a delay after the called number is dialed, and up to 32 digits will be matched by the destination pattern. The dial peer command destinationpattern .T is used to indicate any string of up to 32 digits. The T character is used at the end of a string to instruct the router to wait for the complete dial string to be entered before matching a call to a dial peer. Cisco recommends that you use the destinationpattern .T command rather than the destinationpattern T command because the destinationpattern .T command requires that the caller dial a digit.

IP phones will not require manual IP address configuration. The ip address 192.168.14.1 255.255.255.0 command configures the FastEthernet 0/0 interface on the CME router with the IP address 192.168.14.1. In addition, the ip dhcp excludedaddress 192.168.14.1 192.168.14.9 command prevents the CME router from assigning the IP address 192.168.14.1 to an IP phone. Reference:

https://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfdhcp.html#wp1010670

https://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fc002.html#wp1020232

<https://www.cisco.com/c/en/us/support/docs/voice/h323/22372-no-dialtone.html#solution5>

https://www.cisco.com/en/US/docs/ios/12_3/vvf_r/vrg_d1_ps1839_TSD_Products_Command_Reference_Chapter.html#wp1289151

QUESTION 119

```
ip dhcp excluded-address 192.168.14.1 192.168.14.9
ip dhcp pool IPPhones
  network 192.168.14.0 255.255.255.0
  default-router 192.168.14.1
!
<output omitted>
!
interface FastEthernet 0/0
  ip address 192.168.14.1 255.255.255.0
  no shutdown
!
<output omitted>
!
dial-peer voice 1 pots
  destination-pattern .T
  direct-inward-dial
  port 1/0/0
!
<output omitted>
!
ephone-dn 50
  number 5000
!
ephone-dn 51
  number 5001
!
ephone 20
  button 1:50
!
ephone 21
  button 1:51
  button 2:50
```



Examine the output, and use the information you gather to answer the question.
How many phones will ring if a user dials extension 5001? (Select the best answer.)

A. none

- B. one
- C. two
- D. three

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

One phone will ring if a user dials extension 5001 because only one IP phone has a line button that is configured to use extension 5001. By contrast, both the phone associated with ephonedn 50 and the phone associated with ephonedn 51 will ring when a user dials extension 5000 because both phones have buttons that are configured to use that extension. The following command set configures two phones to ring simultaneously when a call is received on extension 5000:

```
ephonedn 50  
number 5000  
!
```

```
ephonedn 51  
number 5001  
!
```

```
ephone 20  
button 1:50  
!
```

```
ephone 21  
button 1:51  
button 2:50
```



You can configure which ephonedn is given preference by issuing the preference command in ephonedn configuration mode. When multiple ephonedns are configured with the same extension number, the ephonedn with the lowest preference value will receive the call. The preference can be set to a value from 0 to 10; an ephonedn is set to a preference of 0 by default. An ephonedn with a preference of 0 is preferred over an ephonedn with a preference of 1. Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/command/reference/cme_cr/cme_p1ht.html#wp1403322580

QUESTION 120

You issue the show running-config command on a CME router and receive the following partial output:

```
ip dhcp excluded-address 192.168.14.1 192.168.14.9
ip dhcp pool IPPhones
  network 192.168.14.0 255.255.255.0
  default-router 192.168.14.1
!
<output omitted>
!
interface FastEthernet 0/0
  ip address 192.168.14.1 255.255.255.0
  no shutdown
!
<output omitted>
!
dial-peer voice 1 pots
  destination-pattern .T
  direct-inward-dial
  port 1/0/0
!
<output omitted>
!
ephone-dn 50
  number 5000
!
ephone-dn 51
  number 5001
!
ephone 20
  button 1:50
!
ephone 21
  button 1:51
  button 2:50
```



Examine the output, and use the information you gather to answer the question.

Which of the following statements is true? (Select the best answer.)

A. There will be no delay after the phone number is dialed.

- B. There will be no dial tone on the voice port.
- C. There will be an IP conflict between the CME router and an IP phone.
- D. Only the first dialed digit will be matched.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

There will be no dial tone on the voice port, because the dial peer has been configured with the `direct-inward-dial` command. The `direct-inward-dial` command and the `shutdown` command can both disable dial tones on a voice port. You should issue the `direct-inward-dial` command on a plain old telephone service (POTS) dial peer to enable direct inward dialing (DID) for an incoming number. DID uses the incoming dialed number to match an outgoing dial peer. For example, you can use DID to map a POTS telephone number to a four-digit extension on a Voice over IP (VoIP) network so that callers from POTS numbers can bypass the automated attendant or menu system and reach the internal VoIP extension directly. When DID is enabled on a POTS dial peer, the caller will not hear a dial tone on the voice port that is associated with that dial peer.

If you issue the `shutdown` command on a voice port, the port enters the shutdown state, meaning that no voice or data packets can traverse the port and, therefore, no dial tone can be heard by a caller who is attempting to place a call on the port. You can reenable a voice port by issuing the `no shutdown` command in interface configuration mode.

If you do not hear a dial tone on an IP phone even though `direct-inward-dial` has not been configured on the dial peer and the `no shutdown` command has been issued on the voice port, it is probable that you have not assigned an `ephone-dn` to the line that is associated with the IP phone. You can assign a directory number (`dn`) to an IP phone in Cisco Unified Communications Manager Express (CME) by issuing the `button-number:dntag` command in `ephone` configuration mode, where `dntag` is the number that has been assigned to the `ephone-dn` and `button-number` is the number of the line button on the IP phone to which you want to associate the `dn`. In this scenario, the `ephone-dn 50` has been assigned to button 1 on ephone 20.

There will be a delay after the phone number is dialed. In addition, up to 32 digits will be matched by the destination pattern, not just the first digit. The dial peer command `destination-pattern .T` is used to indicate any string of up to 32 digits. The `T` character is used at the end of a string to instruct the router to wait for the complete dial string to be entered before matching a call to a dial peer. Cisco recommends that you use the `destination-pattern .T` command rather than the `destination-pattern T` command because the `destination-pattern T` command requires that the caller dial a digit. A dial peer with the `destination-pattern T` command will be matched if an outbound caller takes the phone offhook for 10 seconds. Destination patterns that do not use the `T` wildcard do not experience a delay between the completion of the dialed string and the connection of the call; the dialed string is matched on a digit-by-digit basis, and the call is connected as soon as a match is found.

There will not be a conflict between the CME router and an IP phone. The following commands configure the router with a Dynamic Host Configuration Protocol (DHCP) pool that will be used to assign IP addresses to an IP phone:

```
ip dhcp pool IPPhones
network 192.168.14.0 255.255.255.0
default-router 192.168.14.1
```

In addition, the `ip address 192.168.14.1 255.255.255.0` command configures the FastEthernet 0/0 interface on the CME router with the IP address 192.168.14.1. In addition, the `ip dhcp excluded-address 192.168.14.1 192.168.14.9` command prevents the CME router from assigning the IP address 192.168.14.1 to an IP phone.

Reference:

https://www.cisco.com/en/US/docs/ios/12_3/vvf_r/vrg_d1_ps1839_TSD_Products_Command_Reference_Chapter.html#wp1289151

<https://www.cisco.com/c/en/us/support/docs/voice/h323/22372-no-dialtone.html#solution5>

QUESTION 121

You issue the show running-config command on a CME router and receive the following partial output:



```
ip dhcp excluded-address 192.168.14.1 192.168.14.9
ip dhcp pool IPPhones
  network 192.168.14.0 255.255.255.0
  default-router 192.168.14.1
!
<output omitted>
!
interface FastEthernet 0/0
  ip address 192.168.14.1 255.255.255.0
  no shutdown
!
<output omitted>
!
dial-peer voice 1 pots
  destination-pattern .T
  direct-inward-dial
  port 1/0/0
!
<output omitted>
!
ephone-dn 50
  number 5000
!
ephone-dn 51
  number 5001
!
ephone 20
  button 1:50
!
ephone 21
  button 1:51
  button 2:50
```



Examine the output, and use the information you gather to answer the question.
Which of the following best describes port 1/0/0 in this configuration? (Select the best answer.)

- A. an analog FXO port
- B. an analog FXS port

- C. a SIP trunk port
- D. a VoIP port

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Port 1/0/0 is an analog foreign exchange office (FXO) port. An FXO interface is typically used to connect an analog device to the public switched telephone network (PSTN). In addition, if a public branch exchange (PBX) is configured with a foreign exchange station (FXS) port, the FXO interface on an analog device can terminate an analog trunk line from a PBX. FXO interfaces are commonly found on standard telephones, fax machines, and analog modems.

The port command is used by a voice router to match inbound plain old telephone service (POTS) dial peers and to determine where to route outgoing POTS dial peers. The dial peer voice command is used to define how calls are routed to destination endpoints on either the PSTN or a Voice over IP (VoIP) network. To define call routing for the PSTN, you should issue the dialpeer voice command with the pots keyword. To define call routing for a VoIP network, you should issue the dialpeer voice command with the voip keyword. In this scenario, dial peer 1 is configured as a pots dial peer. Therefore, the Cisco Unified Communications Manager Express (CME) router port that is connected to the PSTN is FXO port 1/0/0.

Port 1/0/0 is not an analog FXS port. An analog trunk line from the central office (CO) typically originates from an FXS interface on a phone switch. The switch provides dial tone, ring voltage, and line voltage for the customer site. Because the FXS interface on the phone switch provides power, it cannot be connected to another FXS interface; instead, the FXS interface must be connected to a device with an FXO interface, such as an analog telephone or a legacy voice mail system. Port 1/0/0 is neither a Session Initiation Protocol (SIP) trunk port nor a VoIP port. SIP is the signaling method that is most commonly used by Internet telephony service providers (ITSPs). ITSPs enable customers to use VoIP to make phone calls over the Internet. SIP is an Internet Engineering Task Force (IETF) standard call signaling protocol that is supported by a wide variety of IP telephony vendors. The configuration methods for SIP trunking among ITSPs vary. To configure a CME dial peer for SIP trunking in Cisco IOS, you should issue the session protocol sipv2 command in dial peer configuration mode. For example, the following configuration creates dial peer 5012 to handle an outgoing call to a SIP trunk connected to the PSTN:

```
dialpeer voice 5012 voip
session protocol sipv2 session
target ipv4:10.11.12.13
dtmfrelay sipnotify no vad
```

The configuration above sets the trunking protocol for the dial peer to SIP version 2, identifies the SIP trunk as having the IP address 10.11.12.13, specifies that dualtone multifrequency (DTMF) dialed digits should be relayed through SIP's NOTIFY messages, and disables voice activity detection (VAD) for the dial peer. Because no codec configuration command is issued, the default G.729 codec will be used for the dial peer.

Reference:

https://www.cisco.com/en/US/docs/ios/12_3t/voice/command/reference/vrht_d1_ps5207_TSD_Products_Command_Reference_Chapter.html#wp1458170

https://www.cisco.com/en/US/docs/ios/12_3t/voice/command/reference/vrht_p2_ps5207_TSD_Products_Command_Reference_Chapter.html#wp1107545

QUESTION 122

Which of the following Cisco UCM Mobility features is user configurable? (Select the best answer.)

- A. Application Dial Rules
- B. Remote Destination Profile

- C. Remote Destination
- D. SNR assignment schedule

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, only the Cisco Unified Communications Manager (UCM) Single Number Reach (SNR) assignment schedule is user configurable. SNR allows a user to specify an alternate number that will be automatically called when the user receives a call through UCM. SNR assignment schedules enable users to configure specific days and spans of time during which a given SNR configuration will be enabled. For example, if a user wanted to ensure that a given SNR was operational Monday through Friday from 8 a.m. until 6 p.m., the user could configure an SNR assignment schedule for those days and times.

End users are not capable of configuring a Remote Destination Profile or a Remote Destination in UCM.

However, before a user can enable SNR, an administrator must perform the following actions:

- Create a Remote Destination Profile
- Create a Remote Destination
- Enable Mobility on the end user's phone



End users are not capable of configuring Application Dial Rules. Application Dial Rules are used within UCM to add or remove digits from numbers that users dial.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/8_5_1/ccmfeat/fsgd-851-cm/fsmobmgr.html#wp1125072

QUESTION 123

You issue the no auto-reg-ephone command on a CME

router. Which of the following is true? (Select the best

answer.) A. No phones can automatically register with CME.

B. Phones explicitly listed in the configuration can automatically register with CME.

C. Phones can be registered in CME only by using the webbased GUI.

D. The MAC addresses of phones that cannot automatically register will not be recorded.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Only phones that are explicitly listed in the Cisco Unified Communications Manager Express (CME) configuration can automatically register with CME if you issue the no autoregephone command on a CME router. When the no autoregephone command is issued in telephony-service configuration mode, phones that do not have a Media Access Control (MAC) address explicitly listed in the configuration will be blocked and not able to automatically register with CME. However, phones with MAC addresses that are explicitly listed in the configuration will still be able to automatically register.

The autoregephone command, which is issued by default on a CME router, configures a router to automatically assign an ephone to an IP phone even if the phone's MAC address is not explicitly listed in the configuration. When an IP phone registers with a router that is configured with the autoregephone command, the router will associate the MAC address of the IP phone with the first unassigned ephone on the router. If all the ephones on the router are associated with IP phones, the router will create a new ephone, provided that the number of configured ephones does not exceed the value of the max-ephonecommand.

On a Cisco 1700 router that is running IOS 12.4(4)XC, the CME graphical user interface (GUI) will display a dialog box that includes the words "no new phone to add" and a button labeled OK if you attempt to add a phone when autoregistration has been disabled on the router. Autoregistration can be disabled by issuing the no autoregephone command in telephony-service configuration mode in the router's commandline interface (CLI). However, you can register phones in ways other than the CME webbased GUI if auto-registration is disabled. For example, you can issue the macaddressmacaddresscommand in ephone configuration mode in the CLI to manually register an IP phone with CME. The only workaround for the CME GUI error is to enable autoregistration by issuing the autoregephone command in telephony-service configuration mode in the CLI.

The MAC addresses of phones that cannot automatically register will be recorded by the CME router if the no autoregephone command has been issued on the CME router. In this scenario, IP phones that are not explicitly listed in the configuration are blocked by CME when they attempt to automatically register. CME records the MAC address of each blocked IP phone. You can display a list of blocked IP phones by issuing the show ephone attemptedregistrations command in privileged EXEC mode. You can erase the record of blocked IP phone registration attempts by issuing the clear telephony-service ephoneattemptedregistrations command in privileged EXEC mode.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/command/reference/cme_cr/cme_a1ht.html#wp3432972036

https://www.cisco.com/c/en/us/td/docs/ios/12_4/12_4x/release/notes/rn1700xc.html#wp281798

QUESTION 124

How many Publisher servers can be added to a UCM cluster? (Select the best answer.)

- A. one
- B. two
- C. six
- D. eight

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A Cisco Unified Communications Manager (UCM) cluster supports one Publisher server. The Publisher server in a UCM cluster has two roles. It holds the master writable copy of the IBM Informix database for the cluster, and it acts as a Trivial File Transfer Protocol (TFTP) server for IP phone configuration downloads. The Publisher server is the only server that contains a writable copy of the IBM Informix database that stores directory numbers (dns), calling permissions, route plans, and other information. The Publisher server replicates the data that is stored in the master database to the Subscriber servers, all of which then store their own readonly copies of the database.

A UCM cluster can support up to eight Subscriber servers. Subscriber servers typically handle call routing, dial tone, receiving digits, and the streaming of onhold music in a UCM cluster. In medium to large environments, the Subscriber servers perform most of the work in connecting and maintaining calls so that the performance of the Publisher server is not hindered. A UCM cluster is an environment that contains a Publisher server and up to eight Subscriber servers. Each server in the UCM cluster has a unique configuration.

A Cisco Unified Presence (CUPS) server cluster can support up to six servers. CUPS is server software that centralizes network traffic from several different communications services so that it can all be transmitted over the same Cisco Voice over IP (VoIP) network. CUPS uses industrystandard Jabber XCP for communication between different instant messaging (IM) clients? Extensible Message and Presence Protocol (XMPP) is the protocol that establishes the IM sessions. In addition, Jabber XCP facilitates other features such as file and application sharing and video conferencing.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/8x/uc8x/callpros.html#wp1146802

QUESTION 125

Which of the following dial peer commands will match dial strings 1777 and 3777? (Select 3 choices.)

- A. destinationpattern .777
- B. destinationpattern *777
- C. destinationpattern (13)777
- D. destinationpattern [13]777
- E. destinationpattern [13]777



Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The following dial peer commands will match dial strings 1777 and 3777:

- destinationpattern .777
- destinationpattern [13]777
- destinationpattern [13]777

The destination-npattern command is used to match both inbound and outbound dial peers; a dial peer defines a logical route to a telephony endpoint. Outbound dial peers are matched to destination patterns on a digit-by-digit basis as the caller dials the destination number. If multiple dial peers explicitly match the destination pattern, the most specific match for the pattern will be used. The sequence of dialed digits that will be matched for a dial peer can contain the digits 0 through 9, the asterisk (*), and the pound sign (#). In addition, you can use the following symbols to refine the dialing pattern or to match multiple dial strings for a single dial peer:

.	The period matches any dialed digit.
,	The comma inserts a one-second pause.
%	The percent sign indicates that the preceding digit occurs zero or more times.
+	The plus sign indicates that the preceding digit occurs one or more times. When placed at the start of the string, the plus sign indicates an E.164 standard number.
?	The question mark indicates that the preceding digit occurs zero or one time.
[]	Square brackets indicate a range or a set of characters.
^	The caret can be used within square brackets to indicate characters that should not match.
()	Parentheses indicate a sequence of characters, often used with repeating patterns.
T	The T character is placed at the end of a string to indicate any string of zero or more digits.

The dial peer command destinationpattern .777 matches any fourdigit dial string that ends with 777. The period is used as a wildcard character that matches any digit. Not only will the destinationpattern .777 command match 1777 and 3777, it will also match 0777, 2777, 4777, 5777, and so on.

The dial peer command destinationpattern [13]777 matches only the dial strings 1777 and 3777. When square brackets contain a set of digits without a dash, the pattern will match any of the bracketed digits for that digit position. For example, the destinationpattern [135]777 command matches the dial strings 1777, 3777, and 5777. The caret (^) can be used within the brackets to indicate characters that should not match. For example, the destinationpattern [^01479]777 command matches the dial strings 2777, 3777, 5777, 6777, and 8777, but the command does not match the dial strings 0777, 1777, 4777, 7777, and 9777.

The dial peer command destinationpattern [13]777 matches the dial strings 1777, 2777, and 3777. The dash indicates a range of characters. You can also use the dash along with a set of characters. For example, the destinationpattern [135]777 command matches the dial strings 1777, 3777, 4777, and 5777.

The dial peer command destinationpattern *777 does not match the dial strings 1777 and 3777. The * character is not used as a wildcard character? it is used to indicate the asterisk on the telephone keypad. Therefore, the destinationpattern *777 command matches only the dial string *777.

The dial peer command destinationpattern (13)777 does not match the dial strings 1777 and 3777. Parentheses are used to indicate a specific sequence of characters. Therefore, the destinationpattern (13) 777 command matches only the dial string 13777. Parentheses are often used with the %, +, and ? characters to indicate a repeating pattern. For example, the destinationpattern (13)+777 command matches 13777, 1313777, 131313777, and so on.

Reference:

https://www.cisco.com/en/US/docs/ios/12_3t/voice/command/reference/vrht_d1_ps5207_TSD_Products_Command_Reference_Chapter.html#wp1459870

QUESTION 126

Your company has segregated UCM users into four partitions by region. You are configuring Cisco Unity Connection user templates.

Which of the following are you most likely to configure? (Select the best answer.)

- A. a single template for all regions
- B. a unique template for each search space
- C. a unique template for each region
- D. a unique template for each user

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most likely, you will configure a unique Cisco Unity Connection user template for each region if your company has segregated Cisco Unified Communications Manager (UCM) users into four partitions by region. A partition is a logical grouping of Voice over IP (VoIP) route patterns and directory numbers (dns). A Cisco Unity Connection user template is a collection of settings that are applied to each user who is created based on the given template.

When users are separated into partitions, it is likely that certain settings, such as time zones, might be the same for the users within the partition but different for users in another partition. Therefore, you should consider creating separate Cisco Unity Connection user templates for users who exist in different partitions so that such settings can be applied to all users within a given partition with minimal administrative overhead. Other reasons you might create a separate user template include the use of a different call handler by some users or the use of a different phone system by some users.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/administration/guide/10xcucsagx/10xcucsag030.html#31622

QUESTION 127

Which of the following is not a function of Cisco Unified Attendant Console Business Edition? (Select the best answer.)

- A. determining user availability by using presence status
- B. sending CDR reports to administrators or management
- C. reverting transferred calls back to the operator if the call is unanswered
- D. support for conferencing a single third party into an existing call

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Sending Call Detail Records (CDR) reports to administrators or management is not a function of Cisco Unified Attendant Console Business Edition. Cisco Unified Attendant Console is a software application that enables human operators to streamline the process of routing incoming calls across a Cisco IP phone network. There are several versions of Cisco Unified Attendant Console, including Compact Edition, Business Edition, Department Edition, Enterprise Edition, and Premium Edition.

Some features of Cisco Unified Attendant Console are common to all versions. Others require a specific version in order to use the feature set. For example, in Cisco Unified Attendant Console Enterprise Edition, it is possible to configure the Night Service feature, which enables the definition of operator working hours. If incoming calls arrive outside of the operator's working hours, those calls can be automatically redirected to an answering service or a voice mail system.

Determining user availability by using presence status is a function of Cisco Unified Attendant Console Business Edition. Operators can determine the presence of a given contact by selecting the contact from the corporate directory and then pressing the F2 key on the keyboard. The IP phone user's presence and line status are indicated by various phone icons.

Reverting transferred calls back to the operator if the call is unanswered is a function of Cisco Unified Attendant Console Business Edition. Cisco Unified Attendant Console will return a call to the application's Call Progress area if the call is not answered by the user at the destination. From there it will move to Active Calls, at which point the operator can rightclick on the call and choose from one of several options for handling the call.

Support for conferencing a single third party into an existing call is a function of Cisco Unified Attendant Console Business Edition. You can add a third party to an existing call by clicking the party's extension in the application and then clicking Start Conference. If the third party you attempt to add does not want to participate in the conference or does not answer, the call automatically reverts back to the original two participants.

Reference:

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucmac/arc/CUACBE_91110OUG.pdf https://www.cisco.com/c/en/us/products/collateral/unified-communications/unified-mobile-communicator/product_data_sheet0900aecd805e6a5f.html

QUESTION 128

A caller presses an IP phone softkey labeled QRT. The caller is not logged in to the IP phone. Which of the following will not be sent to an administrator? (Select the best answer.)

- A. the time stamp
- B. the category
- C. the reason
- D. the source user name
- E. the destination user name
- F. the source IP address
- G. the destination IP address

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, the source user name will not be sent to an administrator if a user presses an IP phone softkey labeled QRT and is not logged in to the IP phone. The Cisco Quality Report Tool (QRT) can be configured as an extended function to enable users to send QRT information to Cisco Unified Communications administrators directly from the user's IP phone. The report can then be displayed from the Tools menu within Cisco Unified Serviceability. However, if the user is not logged in to the IP phone at the time the data is sent, the user name, or source device owner field, will be null.

The QRT tool collects a variety of available source device information, destination device information, Real-time Information Server (RIS) information, Cisco CallManager service and CTIManager service information, CallManager database information, and enduser information when a user presses the QRT softkey. An administrator can then analyze that information to troubleshoot quality issues or other issues that occurred during a given call.

There is not enough information to determine whether the destination user name will be sent to the administrator. If the call's recipient is logged in to the destination IP phone, the destination user name will be sent to the administrator. However, if the recipient is not logged in to the IP phone, the destination user name will be null.

Enduser information, such as the time stamp, the category, and the reason, will be sent to the administrator. In addition, the source IP address and the destination IP address will be sent to the administrator.

Reference:

https://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/3_3_3/ccmsrvs/ssqrt.html#wp1033729

QUESTION 129

A caller from the voice VLAN attempts to connect to an extension that does not exist on your company's VoIP network.

Which of the following settings in the Call Forward and Pickup Settings section of the UCM Administration Directory Number Configuration page would direct such callers to voice mail? (Select the best answer.)

- A. Forward All
- B. Forward Busy External
- C. Forward Busy Internal
- D. Forward No Answer External
- E. Forward Unregistered External
- F. Forward Unregistered Internal

Correct Answer: F

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Of the available choices, the Forward Unregistered Internal setting would forward internal callers to a specific voice mailbox if the internal caller dialed a nonexistent directory number (dn). The Forward Unregistered Internal setting in the Call Forward and Pickup Settings section of the Cisco Unified Communications Manager (UCM) Administration Directory Number Configuration page would direct a caller from the internal network, or voice virtual LAN (VLAN), to voice mail if that caller attempted to connect to an extension that does not exist on your company's Voice over IP (VoIP) network. The Directory Number Configuration page enables a UCM administrator to configure several settings related to dns, including the following: call forwarding, call pickup, call waiting, line display text, ring settings, and voice mailboxes. In contrast to the Forward Unregistered Internal setting, the Forward Unregistered External setting forwards callers from the public switched telephone network (PSTN) to a specific voice mailbox if the internal caller dialed a nonexistent dn.

The Forward All setting forwards all callers, internal or external, to a specific voice mailbox. This is the same behavior as the CFwdAll softkey that appears on a Cisco IP phone. However, an administrator can configure this behavior for a user by accessing the Directory Number Configuration page if the user for some reason does not have access to the CFwdAll softkey.

The Forward Busy External setting forwards any calls from the PSTN that arrive while the given dn is already in use. Similarly, the Forward Busy Internal setting forwards any internal calls that arrive while the given dn is already in use.

The Forward No Answer External setting forwards any calls from the PSTN that go unanswered by the user. Similarly, the Forward No Answer Internal setting forwards any internal calls that go unanswered by the user. Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/8_0_2/ccmcfg/bccm-802-cm/b03dn.html#wp1337027

QUESTION 130

You want to add a user to a CME router. The router has been assigned the IP address of 192.168.51.50. Which of the following interfaces cannot be used to accomplish your task? (Select the best answer.)

- A. CCP
- B. CLI
- C. http://192.168.51.50/ccme.html
- D. TUI



<https://vceplus.com/>

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You cannot use the telephone user interface (TUI) to add a user to the Cisco Unified Communications Manager Express (CME) router. The TUI is a voice-prompted interface that enables users to perform actions by pressing a number or a specific sequence of numbers on a telephone keypad. A typical function for a TUI on a Voice over IP (VoIP) system is to enable voice mail users to authenticate to the voice mail system and check messages. You can also use a telephone's keypad to perform some configuration tasks, such as modifying network settings or restarting an IP phone.

You can use Cisco Configuration Professional (CCP) to add a user to the CME router. You should click Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users in the graphical user interface (GUI) to add a user or to add a phone if you are using CCP. CCP is a graphical device management tool that is installed as an application on a Windows computer. CCP can be used to configure voice systems, such as CME routers, and other Cisco networking products. When properly installed and configured, CCP enables you to make configuration changes to phones or users by modifying the options on the Phones and Users summary page. You can create, edit, delete, restart, and reset one or more phones from the Phones and Users summary page in CCP. In addition, you can create, edit, and delete one or more phone system users from the Phones and Users summary page in CCP.

You can use the CME commandline interface (CLI) to add a user to the CME router. To create a phone user by using the CLI, issue the username usernamepassword password command in ephone configuration mode, where username is the user name that you want to assign to the user and password is the password that you want to assign to the user. You should issue the username usernamepassword password command only in ephone configuration mode of the device that you want to assign to the user you are creating. For example, if you want user John to be able to manage the device settings of ephone 5 by using the CME GUI, you should issue the following commands on the CME router:

```
CME1(config)#ephone 5
```

```
CME1(configephone)#username john password b0s0n
```

The ephone 5 command places the router into ephone configuration mode for ephone 5. The username john password b0s0n command creates a new user name of john for ephone 5 and assigns that user name the password b0s0n.

You can use the web address of <http://192.168.51.50/ccme.html> to add a user to the CME router in this scenario. CME routers support the configuration of phones and users by using a webbased GUI. After the GUI is enabled, you can access it by typing the CME router's IP address followed by /ccme.html into a browser's location bar. To create a phone user account in the CME GUI, you should click Configure Phones Add Phone, which opens the Add Phone window. In the Login Account area of the Add Phone window, assign the phone user a user name and password and then associate the phone user with either an existing device or a new device? you can create a new device by filling out the devicerelated fields in the Add Phone window. Reference:

https://www.cisco.com/c/dam/en/us/td/docs/net_mgmt/cisco_configuration_professional/v2_5/olh/ccp.pdf#page=1236

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucme/gui/user/guide/cmegui_user.pdf#page=6

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/command/reference/cme_cr/cme_u1ht.html#wp1020821455

QUESTION 131

Your company policy indicates that voice mail messages from internal users can be no longer than 120 seconds. Your company policy also indicates that voice mail messages from outside callers can be no longer than 300 seconds.

All UCM voice mail message length options are currently set to the defaults.

Which of the following options should you modify in Cisco Unity Connection? (Select the best answer.)

- A. Message Settings > Maximum Message Length
- B. Class of Service > Recorded Name-Maximum Length
- C. Class of Service > Message Length-Maximum Length
- D. Advanced > Conversations > System Broadcast Message: Maximum Recording Length in Milliseconds

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You should modify the Class of Service > Message LengthMaximum Length field in Cisco Unity Connection to configure a 120second voice mail recording limit for internal users. The Class of Service > Message LengthMaximum Length field sets a maximum length in seconds for users who are assigned to the specific Class of Service (CoS) that is being modified. Cisco Unity Connection enables an administrator to limit voice mail recording lengths for internal users separately from outside callers. Therefore, you can configure Unity Connection so that outside callers can leave longer messages than internal users. By default, both outside callers and internal users are limited to 300second voice mail messages. Therefore, you only need to configure the Class of Service > Message LengthMaximum Length field to 120 to meet your company's requirements. CoS settings can be modified for multiple users by using the Phone section of a Unity Connection user template or by using Bulk Edit Mode.

You should not modify the Message Settings > Maximum Message Length field, because this field limits the length of voice mail messages that are left by outside callers. By default, the Maximum Message Length field is configured to 300 seconds, which is your company's requirement; therefore, you need not modify this field. However, if you were to modify the Maximum Message Length field value for a single user, you would edit the field on the Message Settings page of the user's account. There are three typical ways to create users in Unity Connection: local manual creation, import from Cisco Unified Communications Manager (UCM), or synchronization by using Lightweight Directory Access Protocol (LDAP).

You can also modify the setting for a number of users at once by editing the Maximum Message Length field in Bulk Edit Mode. In addition, you can configure the Maximum Message Length field on the Message Settings page of a voice mail user template to apply a nondefault maximum message length to any new user accounts that are based on the template.

You should not modify the Class of Service > Recorded NameMaximum Length field. This field applies to users who have been assigned to the CoS and limits the length of time allotted to a user for recording the voice mailbox name that will be announced to callers who reach that user's voice mail. By default, the Recorded NameMaximum Length field is set to 30 seconds; the field's configurable range is from one through 100 seconds. You should not modify the Advanced > Conversations > System Broadcast



Message: Maximum Recording Length in Milliseconds field, because this field limits the length of system broadcast messages that are played for all voice mail users. System broadcast messages are typically used for announcements and can be scheduled to start and end on specific dates and times. By default, the maximum length of a broadcast message is configured to 300,000 milliseconds, which is 300 seconds or five minutes. Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/gui_reference/guide/8xcucgrg/8xcucgrg020.html#76980

QUESTION 132

You issue the following commands on a CME router:

```
CME1#configure terminal
CME1(config)#ephone 6
CME1(config-ephone)#username john password b0s0n
CME1(config-ephone)#end
```

Which of the following best describes the type of CME user you just configured? (Select the best answer.)

- A. a customer administrator
- B. an LDAP user
- C. a phone user
- D. a system administrator

Correct Answer: C

Section: (none)

Explanation



Explanation/Reference:

Explanation:

You have configured a phone user if you issued the commands in this scenario on a Cisco Unified Communications Manager Express (CME) router. A CME environment supports three types of users: system administrator, customer administrator, and phone user. Phone users can manage IP phone settings either by using the telephone keypad or by logging on to the CME browserbased graphical user interface (GUI). In order for a phone user to log on to the GUI, a system administrator must create a phone user account for that user and associate that account with a device. The phone user can then access the GUI by using the Uniform Resource Locator (URL) <http://ipaddress/ccme.html>, where ipaddress is the IP address of the CME router.

To create a phone user by using the commandline interface (CLI), you should issue the `username user - namepassword password` command in ephone configuration mode, where username is the user name you want to assign to the user and password is the password you want to assign to the user. You should issue the `username usernamepassword password` command only in ephone configuration mode of the device that you want to assign to the user you are creating. For example, if you want user John to be able to manage the device settings of ephone 6 by using the CME GUI, you should issue the following commands on the CME router:

```
ephone 6
username john password b0s0n
```

To create a phone user account in the CME GUI, you should click **Configure > Phones > Add Phone** in the GUI, which opens the **Add Phone** window. In the **Login Account** area of the **Add Phone** window, you should assign the phone user a user name and password and then associate the phone user with either an existing device or a new device. Finally, click the **Change** button to create the user. You can also change an existing user's password by clicking **Configure > Phones** in the GUI. Scroll through the list of Media Access Control (MAC) addresses in the **Phone Physical ID (MAC Address)** column until you find the phone you want to modify.

Click the phone you want to modify, change the password, and then click the **Change** button.

You have not created a customer administrator. Customer administrator accounts are configured in the CLI by issuing the web admin customer name user namepassword string command in telephony-service configuration mode, where username is the user name you want to assign to the customer administrator and string is the password you want to associate with the user name. In addition, you can configure a customer administrator in the GUI by clicking Administrator's Login Account in the Configure System Parameters menu. After you have entered values in the Admin User Name (username) field, the Admin User Type (Customer) field, and both password fields, click the Change button to create the user.

You have not created a system administrator. The system administrator account must be configured from the CLI before the system administrator account can access the GUI. You can enable GUI access for a system administrator by issuing the web admin system name admin password string command in telephony-service configuration mode.

You have not created a Lightweight Directory Access Protocol (LDAP) user account. You cannot directly synchronize users in an LDAP directory, such as Microsoft

Active Directory, with CME. However, you can synchronize users in an LDAP directory with other Cisco Unified Communications products, such as Cisco Unity Connection.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/admin/configuration/manual/cmeadm/cmegui.html#pgfId-1056755

QUESTION 133

Which of the following devices are not found in the endpoints layer in the Cisco Unified Communications Architecture? (Select 2 choices.)

- A. VoIP gateways
- B. analog gateways
- C. analog phones
- D. wireless phones
- E. IP phones
- F. IM clients



Correct Answer: AC

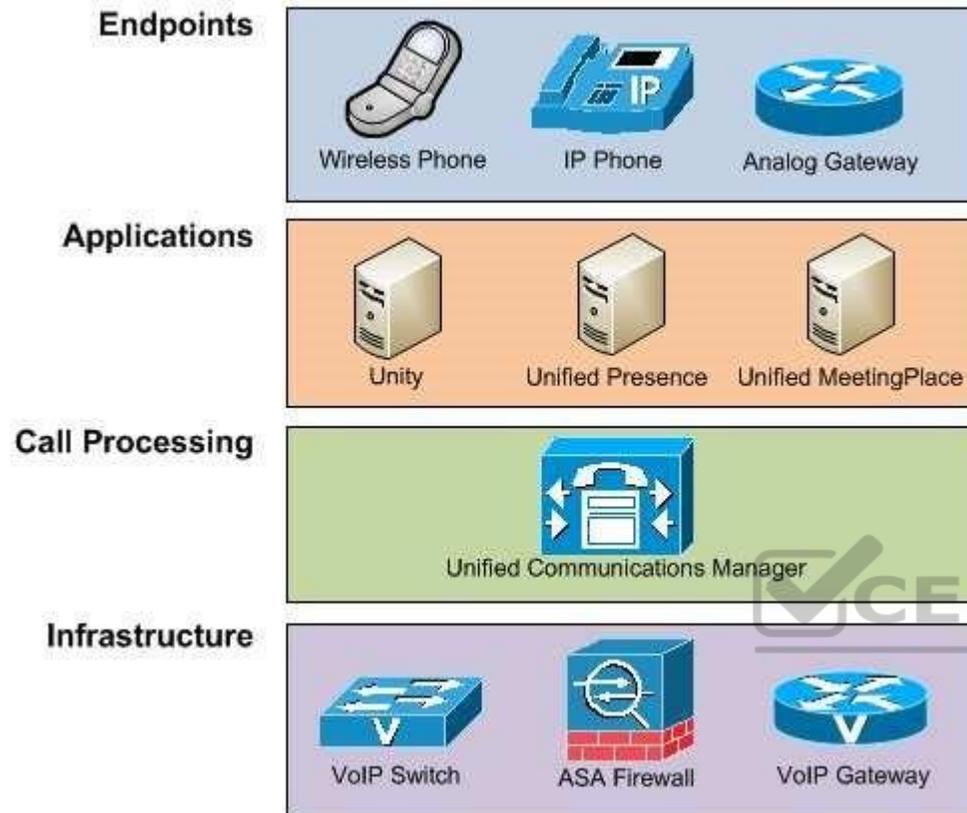
Section: (none)

Explanation

Explanation/Reference:

Explanation:

Voice over IP (VoIP) gateways and analog phones are not found in the endpoints layer in the Cisco Unified Communications Architecture. The Cisco Unified Communications Architecture divides the components of a VoIP solution into the following four layers:



The endpoints layer generally contains devices that an end user is most likely to recognize and use. End users do not typically interface with VoIP gateways, which are found in the infrastructure layer. Analog phones are not capable of directly interfacing with a VoIP network; therefore, analog phones are not part of the Cisco Unified Communications Architecture.

Wireless phones, IP phones, and instant messaging (IM) clients are all found in the endpoints layer because end users commonly interface with these devices. An analog gateway is responsible for translating voice packets between VoIP networks and analog phones. The VoIP network does not extend beyond the analog gateway to the analog phone; therefore, the analog gateway is also considered an endpoint in the Cisco Unified Communications Architecture.

The applications layer of the Cisco Unified Communications Architecture contains devices and systems responsible for enhancing a Cisco VoIP solution with additional features, such as voice mail, fax delivery, and email integration. Systems that are found in the applications layer include Cisco Unity and Cisco Unified Presence (CUPS). Cisco Unity is a scalable messaging server that integrates with thirdparty collaboration servers, such as Microsoft Exchange and Novell GroupWise. CUPS is an application that can assist a user in determining whether another user is currently on a call or available for a meeting.

The call processing layer of the Cisco Unified Communications Architecture contains devices that are responsible for determining what functions or signals must be generated for specific actions. Systems that are found in the call processing layer include Cisco Unified Communications Manager (UCM), Cisco Unified Communications Manager Express (CME), and Unified Communications 500 (UC500). Each of these systems supports a different number of end users. The infrastructure layer is the foundation of the Cisco Unified Communications Architecture. This layer contains devices that are responsible for routing and

switching voice packets across a network. Systems that are found in the infrastructure layer include VoIP gateways, VoIP switches, and Cisco Adaptive Security Appliance (ASA) firewalls.

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/UC8-6-1/system_description/SD861.pdf#page=78

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/7x/uc7_0/endpnts.html

QUESTION 134

Which of the following support XMPP? (Select 3 choices.)

- A. a Cisco IP phone
- B. Cisco Unity Connection
- C. Cisco Unified MeetingPlace
- D. Cisco Unified Personal Communicator
- E. Cisco Jabber
- F. CUPS

Correct Answer: DEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cisco Unified Personal Communicator, Cisco Jabber, and Cisco Unified Presence (CUPS) all support Extensible Message and Presence Protocol (XMPP). Unified Personal Communicator is software that enables a user to connect to several different communication services from a single application. For example, you can use Unified Personal Communicator to place phone calls, download voice mails, and instant message (IM) another user.

Cisco Jabber is an application that is intended to integrate CUPS server services, such as user availability, with Microsoft Office. Cisco Jabber is also an IM client, a voice and video call client, and a desktop sharing client.

CUPS is server software that centralizes network traffic from several different communications services so that it can all be transmitted over the same Cisco Voice over IP (VoIP) network. CUPS uses XMPP to communicate with IM clients. However, CUPS uses Session Initiation Protocol (SIP) to communicate with collaboration endpoints.

Cisco IP phones support SIP and Skinny Client Control Protocol (SCCP), not XMPP. SCCP is a Cisco-proprietary, client/server call signaling protocol. SCCP must be used with a Cisco call processing platform, such as Unified Communications Manager (UCM), because SCCP is proprietary to Cisco. The firmware on Cisco IP phones is configured to use SCCP by default. SCCP must be used on Cisco IP phones to enable the phones to use Cisco's full VoIP feature set. SIP is supported on Cisco IP phones with a firmware replacement.

Cisco Unity Connection uses Internet Message Access Protocol (IMAP), not XMPP. IMAP can be used to retrieve email messages from a remote server. Many email clients support the use of either Post Office Protocol 3 (POP3) or IMAP to retrieve email messages. Unity Connection uses IMAP to enable Unified Personal Communicator to download voice mails.

Cisco Unified MeetingPlace uses Hypertext Transfer Protocol (HTTP) or Secure HTTP (HTTPS), not XMPP. Unified MeetingPlace is a collaboration tool that enables users to share information in the same manner that a conference room would? however, this solution comes together remotely with the use of a phone and browserbased workstation desktop sharing.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/9x/uc9x/presence.html#wp1083881

QUESTION 135

You administer a small VoIP network. You have registered one Cisco IP phone with UCM. Every other IP phone on the network is a thirdparty IP phone. Which of the following statements is most likely true? (Select the best answer.)

- A. Only one H.323 endpoint is registered with UCM.
- B. Only one SCCP endpoint is registered with UCM.
- C. Only one SIP endpoint is registered with UCM.
- D. Only one MGCP endpoint is registered with UCM.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Most likely, only one Skinny Client Control Protocol (SCCP) endpoint is registered with Cisco Unified Communications Manager (UCM) if you have registered one Cisco IP phone with UCM and every other IP phone on the network is a thirdparty IP phone. By default, Cisco IP phones use SCCP, which is a Cisco-proprietary client/server call signaling protocol intended to be an alternative to H.323. A call signaling protocol is responsible for the setup, maintenance, and teardown of a voice call. For example, call signaling protocols can detect and report when a phone is offhook.

Although a few thirdparty IP phones support SCCP, Session Initiation Protocol (SIP) is more widely supported on nonCisco IP phones. SIP is an Internet Engineering Task Force (IETF)standard call signaling protocol that is supported by a wide variety of IP telephony vendors. SIP can be supported by Cisco IP phones with a firmware replacement.

SIP uses a textbased signaling method, which is easier to understand and troubleshoot than the binary method used by other protocols, such as SCCP and H.323. For example, SIP uses textbased INVITE requests and ACK requests to invite a user to participate in a call and to acknowledge that user's response to the INVITE, respectively. Although SIP is typically used as a peertopeer call signaling protocol, it can also operate in client/server mode. SIP is most commonly used by Internet telephony service providers (ITSPs). Therefore, many nonCisco IP phones and video phones are SIP phones.

Neither Cisco IP phones nor thirdparty IP phones typically use H.323. H.323 is an International Telecommunication Union (ITU)standard, peertopeer call signaling protocol. Peertopeer call signaling protocols do not require a call processing platform, because the voice gateways provide their own call signaling and call routing. Therefore, you would be more likely to register a nonCisco SIP IP phone than an H.323 IP phone with UCM. Although UCM supports H.323, Cisco IP phones do not, because H.323 consumes a large amount of processor and memory resources.

Neither Cisco IP phones nor thirdparty IP phones typically use Media Gateway Control Protocol (MGCP). MGCP is a client/server call signaling protocol. MGCP is an IETFstandard protocol that can be used on some Cisco IP phones with a firmware replacement. Reference:

https://www.cisco.com/en/US/tech/tk652/tk701/technologies_configuration_guide_chapter09186a00800eadfa.html#xtocid2

QUESTION 136

Which of the following best describes Connection Reports Data Harvester? (Select the best answer.)

- A. It synchronizes existing users with LDAP directory services.
- B. It enables administrators to import or modify users by using CSV files.
- C. It is the service required for Unity Connection report generation.
- D. It is the feature that an administrator can use to automatically populate certain settings of a new user account in Unity Connection.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Connection Reports Data Harvester is the service required for Cisco Unity Connection report generation. Unity Connection reports can be accessed in Cisco Unified Serviceability, which enables an administrator to view reports and manage other Cisco Unified Communications Manager (UCM) features. Unity Connection is a voice messaging product that is typically installed as an appliance. Cisco Unified Serviceability is a browserbased troubleshooting tool that uses Secure Hypertext Transfer Protocol (HTTPS) to access information that is provided by other reporting tools, such as Cisco Unified RealTime Monitoring Tool (RTMT) and Call Detail Records (CDR) Analysis and Reporting (CAR) tool.

The Connection Reports Data Harvester service allows data to be collected from log files and entered into the Cisco Unified Serviceability Reports Archive, which holds information from which reports can be generated. You can verify that the Connection Reports Data Harvester service is running by clicking Navigation > Cisco Unified Serviceability from within the UCM graphical user interface (GUI) and then clicking Service Management from the Tools menu. The Connection Reports Data Harvester service can be found under Optional Services. If the service is deactivated, you can click Activate to turn it on.

The Bulk Administration Tool (BAT), not the Connection Reports Data Harvester, enables administrators to import or modify users by using commaseparated values (CSV) files. For example, to use the BAT to modify the voice mail message length limit, you could export the voice mail users to a CSV file, change the message length limit value for each user in the CSV file, and then import the CSV file again. You can access the BAT by clicking Tools> Bulk Administration Tool in the Unity Connection GUI.

The Cisco Directory Synchronization (DirSync) service, not the Connection Reports Data Harvester, synchronizes existing Unity Connection users with Lightweight Directory Access Protocol (LDAP) directory services, such as Microsoft Active Directory. To enable Unity Connection to synchronize with an LDAP directory, you must select the Cisco DirSync check box in the Directory Services area of the Unity Connection GUI. In addition, you can import new users from LDAP by either using the BAT to import a CSV file or by using the Users > Import Users tool to import into Unity Connection LDAP information that was previously imported into UCM. Because Unity Connection stores users locally, a user that is synchronized with Unity Connection from LDAP will continue to be stored locally even if that user is later deleted from the LDAP database.

A user template, not the Connection Reports Data Harvester, is the feature that an administrator can use to automatically populate certain settings of a new user account in Unity Connection. Templates are created in Unity Connection by clicking Templates > User Templates and then clicking Add New. Next, you should choose an existing template to use as the base for the new template. The template you choose as the base template can be one of the Unity Connection default templates, such as the Voicemail User Template or the Administrator Template, or a custom template that you have previously configured. The new template will inherit all the settings of the base template except for settings that are unique to each template, such as the template alias and display name.

Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/7x/troubleshooting/guide/7xcuctsgx.pdf

QUESTION 137

Which of the following best describes jitter? (Select the best answer.)

- A. serialization delay
- B. variation in delay
- C. end-to-end delay
- D. dropped packets
- E. flapping links

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Jitter is a variation in delay, which can cause packets to arrive out of sequence or at a different rate than they were sent. Voice over IP (VoIP) traffic is heavily affected by jitter because voice traffic is timesensitive and requires that the destination host receive the voice traffic in the order, and at the same rate, it was sent. When jitter is present, the end user might experience choppiness in the audio connection. A dejitter buffer at the destination is used to collect packets, sort them into the proper sequence based on Realtime Transport Protocol (RTP) time stamps, and release them to the voice application. Although a dejitter buffer can decrease jitter, it can increase delay as packets sit in the buffer. Jitter can be mitigated by increasing bandwidth, using Quality of Service (QoS) mechanisms to prioritize timesensitive traffic, using Compressed RTP (cRTP) to compress headers, and using Stacker and Predictor to compress payloads.

Jitter is not dropped packets, nor is it caused by dropped packets. Congested networks often cause dropped packets. Dropped packets can cause clips, or breaks, in the audio stream. However, voice traffic is more tolerant of dropped packets than of delayed packets, because a small amount of packet loss is not noticeable to the human ear. Packet loss can be mitigated by implementing QoS and congestion avoidance mechanisms, increasing bandwidth, and increasing buffer space. In addition, some codecs can correct small amounts of packet loss.

Jitter is not serialization delay. Serialization delay is the time required to place a packet onto a medium, such as a copper or fiberoptic cable. Serialization delay is directly related to the clocking method and the bandwidth of the line.

Jitter is not endtoend delay. Endtoend delay is the sum of the processing, queuing, serialization, and propagation delays in the traffic path between the source of the packet and the destination of the packet. Therefore, the total network delay between the source of the packet and its destination is considered endto-end delay. Endtoend delay can be mitigated by QoS mechanisms.

Jitter is not flapping links, although jitter can be caused by a flapping link. A flapping link is an interface that alternates between enabled and disabled, often because of a faulty cable or network card. Flapping links can cause packets to take different routes through a network, which can introduce jitter and packet loss.

Reference:

<https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/18902-jitter-packet-voice.html>

QUESTION 138

You want to configure a shared line configuration whereby two phones will ring simultaneously when a caller dials extension 301.

Which of the following command sets should you issue? (Select the best answer.)

- A. CME(config)#ephonedn 21
CME(config)#ephonedn#number 301
CME(config)#ephonedn#ephonedn 22
CME(config)#ephonedn#number 301
CME(config)#ephone 1
CME(config)#button 1:21 2:22
- B. CME(config)#ephonedn 21
CME(config)#ephonedn#number 301
CME(config)#ephonedn#ephonedn 22
CME(config)#ephonedn#number 301
CME(config)#ephone 1
CME(config)#button 1:21
CME(config)#ephone 2

- ```
CME(configephone)#button 1:22
```
- C. CME(config)#ephonedn 21  
CME(configephonedn)#number 301  
CME(configephonedn)#preference 1  
CME(configephonedn)#ephone 1  
CME(configephone)#button 1:21  
CME(configephone)#ephone 2  
CME(configephone)#button 2:21
- D. CME(config)#ephonedn 21 dualline  
CME(configephonedn)#number 301  
CME(configephonedn)#ephone 2  
CME(configephone)#button 1:21

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation

You should issue the following command set to configure a shared line configuration whereby two phones will ring simultaneously when a caller dials extension 301:

```
CME(config)#ephonedn 21
CME(configephonedn)#number 301
CME(configephonedn)#preference 1
CME(configephonedn)#ephone 1
CME(configephone)#button 1:21
CME(configephone)#ephone 2 CME(configephone)#button
2:21
```

The ephonedn 21 command creates ephonedn 21. The number 301 command associates extension 301 with ephonedn 21. The ephone 1 command creates ephone 1, and the ephone 2 command creates ephone 2. The button 1:21 command associates button 1 on ephone 1 with ephonedn 21; similarly, the button 2:21 command associates button 2 on ephone 2 with ephonedn 21.

When multiple ephones are configured with the same extension number, as they are in this scenario, they are configured as shared lines. When a caller dials extension 301, ephonedn 21 will be matched and all of the ephones that are associated with ephonedn 21 will ring.

The preference 1 command is irrelevant to this configuration. The preference command is used to indicate the order in which ephonedns are selected when multiple ephonedns are configured with the same extension number. However, in this scenario, there is only one ephonedn.

It is also possible to configure phones with a shared line when those phones are registered with Cisco Unified Communications Manager (UCM) instead of Cisco Unified Communications Manager Express (CME). To configure a shared line in UCM Administration, navigate to the phones on which you want to share the line and add the directory number (dn) for the shared line. For example, if User 1 has a primary dn of 2401 and User 2 has a primary dn of 2402, you can configure 2401 as a shared line by adding it as another dn on the User 2 phone.

You should not issue the following command set to configure a shared line configuration whereby two phones will ring simultaneously when a caller dials extension 301:

```
CME(config)#ephonedn 21
CME(configephonedn)#number 301
CME(configephonedn)#ephonedn 22
CME(configephonedn)#number 301
CME(configephonedn)#ephone 1
CME(configephone)#button 1:21 2:22
```

This configuration has one ephone with two ephonedns. The button 1:21 2:22 command associates button 1 with ephonedn 21 and button 2 with ephonedn 22. Because the ephonedns are not configured with the preference command, they will use the default preference value of 0. Both preference values are the same, so when a call is placed to extension 301, either ephonedn 21 or ephonedn 22 will be selected randomly. Therefore, either button 1 or button 2 on ephone 1 will ring. You should not issue the following command set to configure a shared line configuration whereby two phones will ring simultaneously when a caller dials extension 301:

```
CME(config)#ephonedn 21
CME(configephonedn)#number 301
CME(configephonedn)#ephonedn 22
CME(configephonedn)#number 301
CME(configephonedn)#ephone 1
CME(configephone)#button 1:21
CME(configephone)#ephone 2
CME(configephone)#button 1:22
```

This configuration has two ephones, each with its own ephonedn. Button 1 of ephone 1 is associated with ephonedn 21, and button 1 of ephone 2 is associated with ephonedn 22. The ephonedns are not configured with the preference command, so they will use the default preference value of 0. As a result, either ephonedn 21 or ephonedn 22 will be selected at random when a call is placed to extension 301, and only one phone will ring.

You should not issue the following command set to configure a shared line configuration whereby two phones will ring simultaneously when a caller dials extension 301:

```
CME(config)#ephonedn 21 dualline
CME(configephonedn)#number 301
CME(configephonedn)#ephone 2
CME(configephone)#button 1:21
```

This is a dualline configuration with one ephone associated with one ephonedn. An ephonedn configured with the dualline keyword is capable of handling two calls simultaneously, thereby enabling the ephonedn to support call waiting, call conferencing, and consult transfers. The button 1:21 command associates button 1 of ephone 2 with ephonedn 21. When a call is placed to extension 301 while ephonedn 21 is in use, the receiver will hear a call waiting beep.

Reference:

[https://www.cisco.com/en/US/docs/ios/12\\_3/vvf\\_r/vrg\\_p1\\_ps1839\\_TSD\\_Products\\_Command\\_Reference\\_Chapter.html#wp1014099](https://www.cisco.com/en/US/docs/ios/12_3/vvf_r/vrg_p1_ps1839_TSD_Products_Command_Reference_Chapter.html#wp1014099)

### QUESTION 139

Which of the following is not a valid device name for a Cisco Unified Client Services Framework softphone device in UCM? (Select the best answer.)

A. UPCJPUBLIC

- B. UPCJoanPublic
- C. JOANPUBLICUPC
- D. UPCJPSOFTPHONE
- E. JPUBLICSOFTPHONE

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

JPUBLICSOFTPHONE is not a valid device name for a Cisco Unified Client Services Framework softphone device in Cisco Unified Communications Manager (UCM), because JPUBLICSOFTPHONE contains more than 15 characters. Neither the Cisco Unified Personal Communicator device type name nor the Cisco Unified Client Services Framework device type name can contain more than 15 characters. The Cisco Unified Personal Communicator device type name can contain uppercase letters and numbers. By contrast, Cisco Unified Client Services Framework device type names can contain uppercase letters, lowercase letters, and numbers.

There are five steps to configuring an end user for Cisco Unified Personal Communicator:

1. Assign the user a license in UCM.
2. Create the end user in UCM.
3. Create the Client Services Framework device.
4. Associate the Client Services Framework device to the end user.
5. Associate a directory number (dn) to the end user.

The Cisco Unified Personal Communicator device type naming convention requires that the name begin with the letters UPC and be derived from the UCM user name. For example, if you were to configure the user Joan Public with a UCM user name of jpublic, the softphone device name associated with the Cisco Unified Personal Communicator device type would be UPCJPUBLIC. Similarly, the user name of j\_public or j.public would have an associated softphone device name of UPCJPUBLIC. If two UCM user names are similar enough to result in identical softphone device names, softphone registration problems can occur in UCM.

Therefore, it is important to be aware of the Cisco Unified Personal Communicator naming convention when you are assigning user names and configuring softphone devices. The Cisco Unified Client Services Framework device type name has no such naming convention.

A softphone is software that behaves like a phone, enabling a user to have voice conversations over a typical workstation network connection. Softphone mode is an operational mode that Unified Personal Communicator uses to act as a softphone. In order to use Unified Personal Communicator as a softphone with UCM, you must add a device to UCM that enables the registration of Unified Personal Communicator in softphone mode. You can configure a softphone device in UCM by clicking Device > Phone > Add New in the UCM administrative graphical user interface (GUI) and selecting either Cisco Unified Personal Communicator or Cisco Unified Client Services Framework from the Phone Type dropdown field. You must configure the Phone Type field with Cisco Unified Personal Communicator if the user is using Unified Personal Communicator version 7.0. You must configure the Phone Type field with Cisco Unified Client Services Framework if the user is using Unified Personal Communicator version 8.0 or later.

UPCJPUBLIC is a valid device name for both Cisco Unified Client Services Framework softphone devices and Cisco Unified Personal Communicator softphone devices in UCM. The UPCJPUBLIC device name conforms to all the naming convention requirements of Cisco Unified Personal Communicator device types. Similarly, UPCJPSOFTPHONE is a valid device name for both softphone device types, provided that the UCM user name associated with the Cisco Unified Personal Communicator device type is jsoftphone or something similar.

UPCJoanPublic is a valid device name for Cisco Unified Client Services Framework softphone devices in UCM because that device type allows lowercase letters. However, UPCJoanPublic is not a valid device name for Cisco Unified Personal Communicator devices, because that device type requires uppercase letters. JOANPUBLICUPC is a valid device name for Cisco Unified Client Services Framework softphone devices in UCM because that device type has no

naming convention that requires UPC to be at the front of the device name. However, JOANPUBLICUPC is not a valid device name for Cisco Unified Personal Communicator devices, because that device type has a naming convention that requires that device names begin with UPC. .Reference: <https://www.cisco.com/c/en/us/obsolete/unified-communications/cisco-unified-presence-version-8.5.html#98570>

#### QUESTION 140

Which of the following protocols typically listens on TCP port 389? (Select the best answer.)

- A. LDAP
- B. SCCP
- C. SIP
- D. XMPP

**Correct Answer:** A

**Section:** (none)

**Explanation**

#### Explanation/Reference:

Explanation:

Lightweight Directory Access Protocol (LDAP) listens on Transmission Control Protocol (TCP) port 389 unencrypted. LDAP Secure (LDAPS) listens on TCP port 636 over Secure Sockets Layer (SSL). LDAP is a directory protocol that is used by other servers, such as Cisco Unified Presence (CUPS) to perform contact lookups.

Session Initiation Protocol (SIP) is an Internet Engineering Task Force (IETF) standard call signaling protocol. Although SIP is typically used as a peertopeer call signaling protocol, it can also operate in client/ server mode. SIP is used for call signaling between Cisco Unified Communications Manager (UCM) and thirdparty IP phones, or between UCM and Cisco SIPenabled IP phones. SIP is supported on Cisco IP phones with a firmware replacement.

Skinny Client Control Protocol (SCCP) is a Cisco proprietary, client/server call signaling protocol. SCCP must be used with a Cisco call processing platform, such as UCM, because SCCP is proprietary to Cisco. The firmware on Cisco IP phones is configured to use SCCP by default. SCCP must be used on Cisco IP phones to enable the phones to use Cisco's full Voice over IP (VoIP) feature set.

Extensible Messaging and Presence Protocol (XMPP) is an open Extensible Markup Language (XML) instant messaging (IM) and presence protocol. CUPS uses XMPP to communicate with thirdparty IM clients

Reference:

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/im\\_presence/configAdminGuide/10\\_0\\_1/CUP0\\_BK\\_C318987B\\_00\\_config-admin-guide-imp-100/CUP0\\_BK\\_C318987B\\_00\\_config-admin-solutions-imp-100\\_chapter\\_0110.html#CUP0\\_RF\\_L39030A6\\_00](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/10_0_1/CUP0_BK_C318987B_00_config-admin-guide-imp-100/CUP0_BK_C318987B_00_config-admin-solutions-imp-100_chapter_0110.html#CUP0_RF_L39030A6_00)

#### QUESTION 141

Which of the following can administrators display by clicking Device Reports > Gateway in the CAR GUI? (Select the best answer.)

- A. the Gateway Detail report
- B. the Gateway Summary report
- C. the Gateway Utilization report
- D. any of the Gateway device reports

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Administrators can display any of the gateway reports by clicking Device Reports > Gateway in the Cisco Unified Communications Manager (UCM) Call Detail Records (CDR) Analysis and Reporting (CAR) graphical user interface (GUI). CAR provides three privilege levels for reporting: administrators, managers, and individual users. Only administrators are permitted to view Gateway device reports.

The Gateway Detail report can be used to examine issues with a specific gateway. The Gateway Summary report can be used to examine a summary of every call that was transmitted through the gateways. Therefore, the Gateway Summary report can be used to monitor traffic and Quality of Service (QoS). The Gateway Utilization report can be used to determine whether a given gateway or gateways are over utilized. Therefore, you can use the Gateway Utilization report to determine whether new gateways need to be added to the network. Reference:

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/service/7\\_1\\_2/car/CAR/cardvgat.html#wp1045126](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/7_1_2/car/CAR/cardvgat.html#wp1045126)

**QUESTION 142**

You issue the following commands on a Cisco voice router:

```
voice translation-rule 1
rule 1 /^615/ //
voice translation-profile VCE
translate called 1 dia-lpeer
voice 101 pots translation-
profile incoming VCE direct-
inward-dial port 1/0:21
```



Which of the following will occur when you issue the test voice translation-rule 1 6155550121 command from privileged EXEC mode? (Select the best answer.)

- A. The number will not change, because 615 is at the beginning of the string.
- B. The digits 615 will be stripped from the beginning of the string.
- C. An error will occur because the command syntax is not correct.
- D. The digits 615 will be added to the beginning of the string.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

The digits 615 will be stripped from the beginning of the string when you issue the test voice translationrule 1 6155550121 command in this scenario. The command set in this scenario creates a voice translation rule with an ID of 1 that is then attached to a voice translation profile named VCE. The translation profile is then associated with plain old telephone service (POTS) dial peer 101 in the inbound direction.

The voice translationrule 1 command creates a voice translation rule with an ID of 1. The rule 1 /^615/ // command creates the first rule within voice translation rule 1. The first two slash marks in a translation rule contain the regular expression pattern that is to be matched within the string. In this scenario, the ^615 within the first set of slashes creates a pattern that matches the digits 615 as long as those digits are anchored at the beginning of the string.

The second set of slashes in the rule 1 command represents the values with which the rule should replace the matched digits. In this scenario, no value has been placed between the second set of slashes in the command. Therefore, the rule is designed to simply remove the digits 615 from the beginning of the string. However, a voice translation rule alone will not automatically strip the digits. Voice translation rules must be applied to voice translation profiles. In this scenario, the following set of commands creates a voice translation profile named VCE and applies voice translation rule 1 to the profile:

```
voice translation-profile VCE
translate called 1
```

After the voice translation profile has been created, the profile must be associated with a dial peer and applied in the appropriate direction. The following set of commands performs these actions:

```
dialpeer voice 101 pots
translationprofile incoming
VCE directinwarddial port
1/0:21
```

By using voice translation rules and voice translation profiles, a company that wants the local area code stripped from any incoming local calls can create a voice translation rule that matches the digits of the area code within the incoming Automatic Number Identification (ANI) string and replaces those digits with nothing. Performing this operation thus reduces the size of the string from 10 digits to seven.

Reference:

<https://www.cisco.com/c/en/us/support/docs/voice/call-routing-dial-plans/64020-number-voice-translation-profiles.html#con16>

### QUESTION 143

Which of the following statements best describes DiffServ? (Select the best answer.)

- A. It prioritizes packets by traffic class.
- B. It is not a QoS model that is recommended by Cisco for voice traffic.
- C. It requires applications to reserve their endtoend bandwidth requirements.
- D. It is a traffic policing mechanism for when traffic exceeds minimum bandwidth limits.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Differentiated Services (DiffServ) is a Quality of Service (QoS) model that prioritizes packets by traffic class. QoS enables a network to treat a specific type of traffic with a different priority than other types of traffic. For example, QoS can ensure that voice traffic gets higher priority on a network than data traffic. QoS models include the besteffort model, the Integrated Services (IntServ) model, and the DiffServ model. Each QoS model handles packet flows in a different manner.

IntServ, not DiffServ, requires that applications reserve their endtoend bandwidth requirements. In addition, IntServ is not the QoS model that is recommended by Cisco. Cisco recommends using DiffServ instead of other QoS models when configuring QoS for voice traffic.

Committed Access Rate (CAR) is a traffic policing mechanism that you can use when traffic exceeds the configured bandwidth limitations. When CAR is used, packets that exceed the bandwidth limits are re-marked with a lower priority and forwarded instead of being dropped. Reference:

[https://www.cisco.com/en/US/technologies/tk543/tk766/technologies\\_white\\_paper09186a00800a3e2f.html](https://www.cisco.com/en/US/technologies/tk543/tk766/technologies_white_paper09186a00800a3e2f.html)

#### QUESTION 144

All of your department's IP phones are connected to a switch that does not support PoE. The IP phones have all been manually configured with IP addressing information. Another administrator power cycles the switch without warning. No calls are in progress. Which of the following is most likely to occur? (Select the best answer.)

- A. The IP phones will power down until the switch restarts.
- B. The IP phones will not be affected by the power cycle.
- C. The IP phones will disappear from the UCM configuration.
- D. The IP phones will reset but retain IP configuration information.

**Correct Answer:** D

**Section:** (none)

**Explanation**

#### Explanation/Reference:

Explanation:

Most likely, the IP phones will reset but retain IP configuration information when the administrator power cycles the switch because, in this scenario, the IP addressing information has been manually configured on each IP phone. When an IP phone is disconnected from Cisco Unified Communications Manager (UCM), the phone will automatically reset in an attempt to reestablish communication. Therefore, if an IP phone suddenly resets or is continuously attempting to register with UCM, it is important to first verify the phone's connectivity to the network switch.

The IP phones will not disappear from the UCM configuration. You can verify that an IP phone exists in the UCM by clicking Device > Phone > Find in UCM Administration and searching for the particular IP phone's Media Access Control (MAC) address. The IP phone will no longer be registered with UCM when it loses connectivity. However, the IP phone's record in the UCM configuration will remain there.

The IP phones will not power down until the switch restarts, because the switch in this scenario does not support Power over Ethernet (PoE). Therefore, the IP phones in this scenario must be connected to individual power supplies in order to obtain power.

The IP phones will be affected by the power cycle. In addition to registration problems, IP configuration problems, and Trivial File Transfer Protocol (TFTP) configuration problems, IP phones that are powered directly from a switch by using PoE will not be able to receive power until the switch has restarted.

Reference:

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cuipph/7905g\\_7912g/5\\_0/sip/english/administration/guide/5\\_0/LowPtrb.html#wp1092158](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/7905g_7912g/5_0/sip/english/administration/guide/5_0/LowPtrb.html#wp1092158)

#### QUESTION 145

You want to test a new dial plan before you deploy the plan in a UCM environment. Which of the following tools should you use? (Select the best answer.)

- A. CAR
- B. DNA
- C. RIS
- D. RTMT

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

You should use the Cisco Unified Communications Manager (UCM) Dialed Number Analyzer (DNA) to test a new dial plan before you deploy the plan in a UCM environment. You can also use DNA to test a dial plan after deployment. DNA initially displays results in a new browser window. However, you can export data from DNA in the form of an Extensible Markup Language (XML) file.

A dial plan is a set of rules, or route plan, that determines how calls reach their destinations. A Voice over IP (VoIP) dial plan enables a company to route calls between geographically dispersed sites while keeping the calls onnetwork. Onnetwork calls are calls routed over a single network, such as an IP data network. By contrast, offnetwork calls are calls that are routed through multiple telephony networks, such as those routed over the public switched telephone network (PSTN). DNA and verification of the calling search space are both ways to troubleshoot error recordings when attempting to make offnetwork calls.

You should not use Cisco Unified RealTime Monitoring Tool (RTMT). RTMT is a clientside application that enables an administrator to monitor devices on a Cisco VoIP network in real time by using Secure Hypertext Transfer Protocol (HTTPS). RTMT uses HTTPS to connect to VoIP devices and gather information, such as device status and performance statistics, in real time. The data that is gathered by RTMT can then be used to pinpoint problems on the VoIP network or to monitor performance thresholds.

You should not use the Cisco Realtime Information Server (RIS). The RIS maintains device registration statuses, performance counter information, and information about critical alarms in real time. Similar to DNA, the Cisco RIS Data Collector, which transmits data to the RIS, runs as a UCM service. If you notice that UCMregistered devices are not showing up in the UCM Administration pages, you should try restarting the Cisco RIS Data Collector service.

You should not use the Cisco Call Detail Records (CDR) Reporting and Analysis (CAR) tool. CAR is used to generate CDR reports, Quality of Service (QoS) reports, traffic reports, and billing reports. Reference:

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/dna/9\\_0\\_1/CUCM\\_BK\\_C7C05BE8\\_00\\_cucm-dialed-number-analyzer-90/CUCM\\_BK\\_C7C05BE8\\_00\\_cucm-dialed-number-analyzer-guide\\_chapter\\_01.html#CUCM\\_TP\\_D4E3DA13\\_00](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/dna/9_0_1/CUCM_BK_C7C05BE8_00_cucm-dialed-number-analyzer-90/CUCM_BK_C7C05BE8_00_cucm-dialed-number-analyzer-guide_chapter_01.html#CUCM_TP_D4E3DA13_00)

#### **QUESTION 146**

You issue the no ip source-address 172.16.0.1 command in telephony service configuration mode on a CME router. Which of the following is true? (Select the best answer.)

- A. The CME router will no longer receive credential services messages.
- B. The CME router will receive IP phone messages through an alternate port.
- C. The CME router will no longer receive messages from IP phones.
- D. The CME router will receive messages from IP phones by using IPv6.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

The Cisco Unified Communications Manager Express (CME) router will no longer receive messages from IP phones if you issue the no ip sourceaddress 172.16.0.1 command in telephony service configuration mode. The syntax of the ip sourceaddress command is ip sourceaddress {ipv4address | ipv6address},

where ipv4address is the IP version 4 (IPv4) address on which you want the router to receive IP phone messages. Issuing the no form of this command disables the CME router's ability to receive messages from IP phones.

The CME router will not receive IP phone messages through an alternate port. To configure the CME router to receive IP phones through an alternate port, you should issue the ip sourceaddress command with the port keyword. However, the port keyword applies only to Skinny Client Control Protocol (SCCP) phones and operates only on an IPv4 address. For example, issuing the ip sourceaddress 172.16.0.1 port 2400 command in telephony service configuration mode configures the CME router to receive IP phone messages on 172.16.0.1 on Transmission Control Protocol (TCP) port 2400. If the portkeyword is not specified, the CME router receives the IP phone messages on TCP port 2000.

The CME router will not receive messages from IP phones by using IPv6. In order to configure the CME router to receive messages from IP phones by using IPv6, you should issue the ip sourceaddress command with an IPv6 address instead of an IPv4 address. You can also configure the source address to operate in dualstack mode by issuing the secondary keyword followed by an IPv4 address. For example, the ip sourceaddress 2001:DB8:A::1 secondary 172.16.0.1 command configures the CME router to receive IP phone messages at either the IPv6 address of 2001:DB8:A::1 or the IPv4 address of 172.16.0.1.

You cannot configure whether the CME router will receive credential services messages from telephony service configuration mode. Issuing the ip sourceaddressipaddresscommand in credentials configuration mode configures the CME router to receive credential services messages from a particular IP address. Issuing the no form of this command in credentials configuration mode disables that ability.

Reference:

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucme/command/reference/cme\\_cr/cme\\_i1ht.html#wp3725679205](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/command/reference/cme_cr/cme_i1ht.html#wp3725679205)

#### QUESTION 147

You issue the showrunning config command on a CME router and receive the following partial output:

```
dial-peer voice 1 voip
 destination-pattern
 session target ipv4:192.168.0.1
!
dial-peer voice 2 voip
 destination-pattern 302....
 session target ipv4:192.168.0.2
!
dial-peer voice 3 voip
 destination-pattern 3021234
 session target ipv4:192.168.0.3
!
dial-peer voice 4 voip
 destination-pattern 302
 session target ipv4:192.168.0.4
```

A caller dials 3021234.

Which of the following dial peers will the router use? (Select the best answer.)

A. 1

- B. 2
- C. 3
- D. 4

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

The Cisco Unified Communications Manager Express (CME) router will use dial peer 4 to route the voice data when a caller dials 3021234. When a caller dials 3021234, the router collects the digits as the caller dials them. The router compares the dialed digits against dial peer destination patterns on a digitbydigit basis. Because dial peer 4 most specifically matches the dialed string 302, the router will immediately process the call by using dial peer 4 as soon as the caller completes the 302 sequence of characters.

If multiple dial peers explicitly match the destination pattern, the most specific match for the pattern will be used. For example, if dial peer 4 were removed from this scenario, a caller dialing 3021234 would immediately match all three of the remaining dial peers. Dial peer 3, because it explicitly defines the dialed string, would be the most specific match. Dial peer 1, because its destination pattern contains seven wildcards, would be the least specific match.

The router will not use dial peer 3 to route the voice data when a caller dials 3021234. Although dial peer 3 is the most specific destination pattern match for the entire string of dialed digits, the router will process the most specific match on a digitbydigit basis. Therefore, the router will process the call as soon as dial peer 4 is matched, before the caller has had a chance to complete the full sevendigit string.

The router will not use dial peer 1 or dial peer 2 to route the voice data when a caller dials 3021234. Although the destination pattern configured for dial peer 1 would match any sevendigit dialed string, the destination pattern is not the most specific match for 3021234. Similarly, the destination pattern configured for dial peer 2 would match the dialed string, but it is a less specific match than dial peer 4, because four of the seven digits in the dial peer 2 destinationpattern command are wildcards.

Reference:

<https://www.cisco.com/c/en/us/support/docs/voice/call-routing-dial-plans/14074-in-dial-peer-match.html#topic9>

#### **QUESTION 148**

Which of the following are not Cisco Unity Connection features that you can modify in the Phone section of the User Templates Basics page? (Select 3 choices.)

- A. CoS
- B. partition
- C. search space
- D. voice mail password
- E. web application password
- F. time zone

**Correct Answer:** DEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Explanation:**

You cannot modify the Cisco Unity Connection time zone feature in the Phone section of the User Templates Basics page. If your company's Cisco Unity Connection implementation must support users in different time zones, you can create a unique user template for each time zone. Within each template, you can configure the time zone in the Location section of the User Templates Basics page. You can also adjust the system default language in this section.

In addition, you can modify neither the voice mail password nor the web application password in the Phone section of a Cisco Unity Connection User Templates Basics page. Cisco Unity Connection users have two passwords: the voice mail system password that is issued by using the telephone user interface (TUI) and the web application password that is issued by using Cisco Unity Connection's webbased graphical user interface (GUI). The voice mail password is a personal identification number (PIN) that enables a user to access his or her voice mailbox in Cisco Unity Connection. The web application password is an alphanumeric password that enables a user to access and modify specific Cisco Unified Communications settings by using a browser.

To access the Voice Mail Password Settings section of a user template, you should click Templates > User Templates in Cisco Unity Connection and select Voice Mail from the Choose Password dropdown menu. To access the Web Application Password Settings section of a user template, you should click Templates > User Templates in Cisco Unity Connection, then select Web Application from the Choose Password dropdown menu.

You can modify Class of Service (CoS) features in the Phone section of a Cisco Unity Connection User Templates Basics page. CoS settings enable an administrator to apply a specific set of privileges to Cisco Unity Connection users. In addition, you can modify partition features and search space features in the Phone section of a Cisco Unity Connection user template. A partition is a logical grouping of Voice over IP (VoIP) route patterns and directory numbers (dns). A search space is an ordered list of partitions that a device is allowed to search for patterns that match a dialed number.

**Reference:**

**QUESTION 149**

You are configuring digest authentication so that the identity of SIP phones can be challenged by the UCM to which they are connected. After configuring an appropriate security profile, you apply the profile to each SIP phone on the network. After creating a digest user in the UCM Administration End User window, you notice that a Cisco 7961G IP phone is not able to authenticate with UCM. Which of the following should you do? (Select 2 choices.)

- A. Associate the digest user with the SIP phone in UCM Administration.
- B. Configure the SIP realm on a SIP trunk.
- C. Reset the phone.
- D. Specify digest credentials in the Application User Configuration window.
- E. Upload the configuration file to the TFTP server.

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Explanation:**

You should associate the digest user with the Session Initiation Protocol (SIP) phone in Cisco Unified Communications Manager (UCM) Administration and then reset the Cisco 7961G IP phone in order to enable the phone to use digest authentication to verify its identity with the UCM to which it is connected.

The digest credentials for most Cisco IP phones are stored in the phone's configuration file, which is downloaded from a Trivial File Transfer Protocol (TFTP) server when the phone is started or reset. On Cisco 7940G and 7960G SIP IP phones, the digest credentials must be manually entered from the IP phone.

Digest credentials consist of a unique user ID, password, and digest realm. UCM generates a Message Digest 5 (MD5) hash from these values and a random number. A checksum is generated from the hash. The user name and checksum are then stored in the UCM database in an encrypted format.

To enable UCM to authenticate a SIP phone, you should first configure a security profile for SIP phones and verify that the Enable Digest Authentication check box has been selected. Next, you should apply the security profile to the SIP phones that you want to be authenticated. After the security profile has been created and applied, you should configure a digest user in the UCM Administration End User window, where you specify the digest user ID and password that you want the SIP phone to use to authenticate. Finally, you must associate the digest user with the SIP phone that you want to be authenticated and reset that SIP phone so that it downloads its new configuration. The new configuration contains the digest credentials.

You do not need to upload the SIP phone configuration file to the TFTP server. UCM updates the configuration file so that it can be downloaded from the TFTP server by the IP phones. However, for security reasons, you might want to ensure that TFTP traffic between the server and the IP phones is encrypted. Otherwise, the digest credentials will be included in a configuration file that is sent across the network as clear text.

You do not need to specify digest credentials in the Application User Configuration window. The Application User Configuration window can be used to specify digest credentials for SIP applications that you want to authenticate with UCM.

There is nothing in this scenario to indicate that you should configure the SIP realm on a SIP trunk. You would need to configure a SIP realm if you were receiving digest authentication challenges over a SIP trunk. Reference:

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/security/9\\_0\\_1/secugd/CUCM\\_BK\\_CCB00C40\\_00\\_cucm-security-guide-90/CUCM\\_BK\\_CCB00C40\\_00\\_cucm-security-guide\\_chapter\\_01100.html#CUCM\\_TK\\_S2044B79\\_00](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/9_0_1/secugd/CUCM_BK_CCB00C40_00_cucm-security-guide-90/CUCM_BK_CCB00C40_00_cucm-security-guide_chapter_01100.html#CUCM_TK_S2044B79_00)

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/security/9\\_0\\_1/secugd/CUCM\\_BK\\_CCB00C40\\_00\\_cucm-security-guide-90/CUCM\\_BK\\_CCB00C40\\_00\\_cucm-security-guide\\_chapter\\_01.html#CUCM\\_RF\\_D4C84CE2\\_00](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/9_0_1/secugd/CUCM_BK_CCB00C40_00_cucm-security-guide-90/CUCM_BK_CCB00C40_00_cucm-security-guide_chapter_01.html#CUCM_RF_D4C84CE2_00)

#### QUESTION 150

You are unable to create a new user from UCM Administration.

Which of the following is most likely the cause of the problem? (Select the best answer.)

- A. The Telephone Number field is empty.
- B. An IP phone has not been associated with the account you are creating.
- C. The Cisco Unity User check box has not been selected.
- D. Users have been synchronized from LDAP.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Of the available choices, most likely you are unable to create a new user from Cisco Unified Communications Manager (UCM) Administration because users have been synchronized from Lightweight Directory Access Protocol (LDAP). New users can be directly created from UCM Administration only if LDAP server synchronization is disabled. You can determine whether LDAP synchronization is enabled by navigating to System > LDAP > LDAP System in UCM Administration.

If users are not able to view telephone numbers in the corporate directory, you should verify that the Telephone Number field is not empty. Users are capable of searching UCM directory information from IP phones or applications. However, in order for users to see that information, the appropriate fields must be filled in for each UCM user in UCM Administration or in the LDAP directory from which UCM obtains the information.

If the UCM user you created was not also created in Cisco Unity Connection, you should verify that the Cisco Unity User check box was selected for that user in UCM Administration. When you create a user in UCM Administration, you can simultaneously create a Cisco Unity Connection account for that user by selecting the Cisco Unity User check box in UCM Administration. However, you will still need to edit the newly created Cisco Unity Connection user account in Cisco Unity Connection to complete the configuration.

It is not likely that you cannot create a user in UCM Administration if an IP phone has not been associated with the account. You cannot associate a device with an end user unless the end user account has already been created. Reference:

<https://www.cisco.com/c/en/us/obsolete/unified-communications/cisco-unified-communications-manager-version-7.1.html#wp1059267>

### QUESTION 151

You want to delete 100 unassigned dns from the UCM database.

Which of the following sets of steps could you use? (Select 2 choices.)

- A. Use Bulk Administration > Phones > Delete Phones > Delete Unassigned DN to find and remove the dns.
- B. Use Call Routing > Route Plan Report to find and remove the dns.
- C. Use Call Routing > Directory Number to find and remove the dns.
- D. Use Device > Phone > Directory Number Configuration to find and remove the dns.
- E. Use Device > Phone > Device Information to find and remove the dns.

**Correct Answer:** AB

**Section:** (none)

**Explanation**



### Explanation/Reference:

Explanation:

You could use either Bulk Administration > Phones > Delete Phones > Delete Unassigned DN or Call Routing > Route Plan Report to find and remove 100 unassigned directory numbers (dns) from the Cisco Unified Communications Manager (UCM) database. An unassigned dn is a dn that is not associated with a specific device, such as an IP phone, but that can still be used to forward calls to voice mail or to another dn that is associated with a device. For UCM to load and use an unassigned dn, the Activecheck box must be selected for the dn. The Active check box is only displayed for unassigned dns.

The UCM Bulk Administration > Phones > Delete Phones > Delete Unassigned DN window automatically searches for and displays a list of unassigned dns in the UCM database. Once the list of unassigned dns is complete, you should select the Run Immediately radio button and then click Submit to immediately delete the unassigned dns from the UCM database.

To find 100 dns by using Call Routing > Route Plan Report, you should choose Unassigned DN from the Find dropdown menu and then click the Find button. Once the list of unassigned dns is complete, you can select the check box beside each dn that you want to delete and then click the Delete Selected button to immediately delete the unassigned dns from the UCM database. Alternatively, you can remove all unassigned dns at once by clicking the Delete All Found Items button instead of the Delete Selected button.

Problems with unassigned dns can cause an IP phone that is attempting to autoregister with UCM to display the following error:

Registration Rejected: Error DBConfig

Therefore, you should remove unassigned dns from the autoregistration configuration if this error occurs.

You cannot use Device > Phone > Directory Number Configuration to find and remove 100 unassigned dns from the UCM database. The Directory Number Configuration window in UCM is for adding dns to an IP phone, updating dn associations with an IP phone, and removing dns from an IP phone. Although you can add new dns to the UCM database by using the Directory Number Configuration window, you cannot remove a dn from the UCM database by using that window.

You can also use the Directory Number Configuration window to reassign dns that have been removed. The Route Plan Report can also be used to accomplish this task.

You cannot use Call Routing > Directory Number to find and remove 100 unassigned dns from the UCM database. However, similar to Device > Phone > Directory Number Configuration, you can use Call Routing> Directory Number to add a dn to the UCM database or to update information about the dn in the UCM database. You can also add a dn to a phone immediately after you add the phone to UCM by clicking the Line [1] -Add a new DN link or the Line [2] -Add a new DN link in the Association Information area, which is displayed on the left side of the Phone Configuration window in UCM.

You cannot use Device > Phone > Device Information to find and remove 100 unassigned dns from the UCM database. However, you can use this option to configure the IP phone Media Access Control (MAC) address, security profile, device pool, phone button template, location, privacy settings, and mobility mode.

Reference:

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/bat/8\\_0\\_2/bat-802-cm/t03delph.html#wp1355300](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/bat/8_0_2/bat-802-cm/t03delph.html#wp1355300)

<https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/71440-ccm4x-unassigneddns.html#maintask1>

#### QUESTION 152

Which of the following terms defines a value that represents voice quality in a network depending on codec and region? (Select the best answer.)

- A. Jitter
- B. QoS
- C. MOS
- D. R-Factor



**Correct Answer: C**

**Section: (none)**

**Explanation**

#### **Explanation/Reference:**

Explanation:

Of the available choices, the term Mean Opinion Score (MOS) defines a value that represents voice quality in a network depending on codec and region. MOSs are calculated scores that are mitigated by voice quality hindrances, such as latency and jitter. In addition, MOS scales are not standard across codecs and regions. Therefore, the MOS scale for one codec might not be applicable to another codec. Devices such as the Cisco Network Analysis Module (NAM) monitor active Realtime Transport Protocol (RTP) streams in order to gather the statistical data to compute the MOS.

An R-Factor is also a value that represents voice quality in a network. However, the way R-Factor measurements are calculated is the same across all codecs and regions. Therefore, R-Factor measurements might be a simpler means of evaluating an enterprise that spans regions or deploys a number of different codecs. Quality of Service (QoS) is a Voice over IP (VoIP) technique that ensures call quality and integrity by mitigating delay and dropped packets, which can interrupt the flow of a VoIP call. Typical QoS techniques include buffer management and the use of multiple transmission queues to separate types of multimedia packets. Because voice traffic is sent in real time, quality is critical.

Jitter is a variation in delay that can cause packets to arrive out of sequence or at a different rate than they were sent. As a result, the end user might experience choppiness in the audio connection. Thus shorter packet roundtrip times contribute to better voice quality. Reference:

[https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/branch-routers-series-network-analysis-module-nme-nam/white\\_paper\\_c11-520524.html](https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/branch-routers-series-network-analysis-module-nme-nam/white_paper_c11-520524.html)

#### QUESTION 153

You are the administrator for a small VoIP network connected to an ITSP in the United States. The topology consists of one voice router, a UCM, and three PoE-capable switches. All of the IP phones are receiving power. However, none of the IP phones on the network are registering with UCM. In which of the following fault domains should you begin troubleshooting? (Select the best answer.)

- A. the IP phones
- B. the cables connecting the IP phones to the switches
- C. the network switches that are connected to the IP phones
- D. the UCM configuration

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation

Because none of the IP phones on the network are registering with Cisco Unified Communications Manager (UCM), you should begin troubleshooting at the UCM configuration. Licensing problems or other configuration issues could be preventing IP phones from registering with UCM. You might also begin troubleshooting at the voice router instead of the UCM if all the IP phones on the network are able to register with UCM but are not able to make calls beyond the router.

You would not begin troubleshooting at the IP phones, because all the IP phones are affected. If only one user were experiencing the problem, you could begin troubleshooting the IP phone fault domain.

You would not begin the troubleshooting process by examining the cables connecting the IP phones to the switch. You might check the cable connecting the IP phone to the switch or the switch port to which the cable is connected if a single IP phone were a Power over Ethernet (PoE) device that was not receiving power from the switch, or if Cisco Unified Communications Manager (UCM) reported that the device is of an unknown type. You might also check the network cable and switch port if the device were powered by a power supply but unable to register and download a configuration.

It is not likely that you would begin troubleshooting the network switches, because all users are affected by the problem. You might begin troubleshooting the problem at the network switches if an entire department within an organization were reporting a problem or if only the users connected to a given switch were experiencing a problem.

Reference:

<https://www.cisco.com/c/en/us/obsolete/unified-communications/cisco-unified-communications-manager-version-7.1.html#wp1111505>

#### **QUESTION 154**

You administer a UCM network of 500 IP phones

You need to add 50 new IP phones to your company's UCM network before the end of the workday. Which of the following does Cisco recommend you do? (Select the best answer.)

- A. Add a second UCM server to the cluster.
- B. Add the phones by using the BAT.
- C. Enable auto-registration in UCM.
- D. Provision the IP phones manually in UCM.

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Cisco recommends that you enable auto-registration in Cisco Unified Communications Manager (UCM) to add fewer than 100 new IP phones to a UCM network. There are three ways to add IP phones to a UCM database: by configuring auto-registration, by using the Bulk Administration Tool (BAT), and by manually provisioning the IP phones in the UCM administrative graphical user interface (GUI). Both auto-registration and the BAT provide a means of adding many phones to the database simultaneously. However, Cisco does not recommend using the BAT if you need to add fewer than 100 IP phones.

Auto-registration enables UCM to automatically add new IP phones to the UCM database as the IP phones are connected to the network. When a new IP phone is connected to the network, UCM will automatically assign an unused directory number (dn) to the IP phone from a pool of available dn numbers.

Auto-registration is a security risk because rogue devices can be connected to the network and registered with UCM by using auto-registration. In addition, you could accidentally register a valid IP phone with a dn from the wrong dn pool if you leave auto-registration enabled after you have completed an auto-registration process. Therefore, Cisco recommends that you enable auto-registration only for short periods of time, such as when you need to add fewer than 100 IP phones to the network. In this scenario, you want to add 50 new IP phones to your company's UCM network before the end of the workday. Because of the time limitation and the small number of IP phones, enabling auto-registration would require the least amount of administrative effort.

You do not need to provision the IP phones manually in UCM. Although you can manually add an IP phone to a UCM database, adding 50 new IP phones by using manual provisioning would require more administrative effort than by using auto-registration or the BAT. When you are manually provisioning an IP phone in UCM, you must fill in the MAC Address field, the Device Pool field, the Phone Button Template field, and the Device Security Profile field. In this scenario, you want to add 50 new IP phones to your company's UCM network before the end of the workday. Because of the time limitation and the number of IP phones, enabling autoregistration would require the least amount of administrative effort. Therefore, you should not manually provision the IP phones. You do not need to add a second UCM server to the cluster. UCM supports a maximum of 7,500 devices as a standalone server and a maximum of 30,000 IP phones per UCM cluster. In this scenario, you administer a network of 500 IP phones. In addition, you are adding only 50 new IP phones, which brings the total number of IP phones to 550.

You do not need to add the phones by using the BAT. The BAT enables a UCM administrator to add or modify multiple IP phones at once. However, Cisco recommends that you use the BAT to add 100 or more new IP phones to a UCM network. In this scenario, using the BAT would require more administrative effort than using auto-registration because the BAT requires you to provide Media Access Control (MAC) addresses for the IP phones that are being added. Autoregistration does not require you to provide MAC addresses.

Reference: [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/admin/8\\_0\\_2/ccmsys/accm-802-cm/a02autor.html#wp1020237](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/8_0_2/ccmsys/accm-802-cm/a02autor.html#wp1020237)



<https://vceplus.com/>

