Cisco

(350-801)

Implementing Cisco Collaboration Core Technologies (CLCOR)

Total: **476 Questions**

Link:

Question: 1

Which two functionalities does Cisco Expressway provide in the Cisco Collaboration architecture? (Choose two.)

A. Survivable Remote Site Telephony functionality
B. MGCP gateway registration
C. secure business-to-business communications
D. customer interaction management services
E. secure firewall traversal for remote devices

Answer: CE

Explanation:

Cisco Expressway plays a crucial role in enabling secure communication within and beyond a Cisco Collaboration environment. Option C, "secure business-to-business communications," is correct because Expressway acts as a secure gateway that allows organizations to connect their collaboration platforms (like Cisco Unified Communications Manager) with external partners, enabling secure video and voice conferencing and messaging across different networks. This functionality is often referred to as Business-to-Business (B2B) or Federated communication. It handles the necessary NAT traversal and security checks to allow these interactions to happen seamlessly.

Option E, "secure firewall traversal for remote devices," is also correct. Expressway provides Mobile and Remote Access (MRA), allowing users outside of the corporate network to securely connect their devices to the collaboration infrastructure through the internet. Expressway handles the complex security aspects of this interaction, acting as a firewall traversal device, allowing secure access without the need for VPNs in many cases. It effectively manages the communication flow, ensuring devices can connect to and utilize collaboration services whether they are inside or outside the enterprise's firewall.

Option A, "Survivable Remote Site Telephony functionality," is incorrect. While Cisco Unified Survivable Remote Site Telephony (SRST) provides fallback capabilities for remote sites during WAN outages, this is a feature primarily associated with Cisco routers and Call Manager Express, not Expressway. Option B, "MGCP gateway registration," is incorrect; Media Gateway Control Protocol (MGCP) gateways register directly with Cisco Unified Communications Manager, not via Expressway. Lastly, option D, "customer interaction management services," is incorrect; this is usually managed through Cisco Contact Center solutions, not Expressway which is designed for enabling secure communication between users.

Therefore, the correct functionalities provided by Cisco Expressway are secure business-to-business communication and secure firewall traversal for remote devices.

Authoritative Links:

Cisco Expressway Deployment Guide:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-5/mra/cisco_expressway_mra_deployment_guide_14_5.html
Cisco Expressway Overview:https://www.cisco.com/c/en/us/products/unified-communications/expressway/index.html

Question: 2

An engineer must extend the corporate phone system to mobile users connecting through the internet with their own devices. One requirement is to keep that as simple as possible for end users. Which infrastructure element achieves these goals?

A. Cisco Express Mobility

B. Cisco Expressway-C and Expressway-E
C. Cisco Unified Border Element
D. Cisco Unified Instant Messaging and Presence

Answer: B

Explanation:

The correct answer is **B. Cisco Expressway-C and Expressway-E**. Here's why:

Cisco Expressway provides a secure and scalable solution for extending collaboration services, such as voice and video, beyond the corporate network. It acts as a gatekeeper, enabling mobile users with their own devices to connect to the internal Cisco Unified Communications infrastructure without the complexities of VPNs. The Expressway solution is comprised of two key components:

Expressway-C (Core): This component resides within the internal network and manages the communication flow with Cisco Unified Communications Manager (CUCM) and other internal collaboration servers. **Expressway-E (Edge):** This component sits at the network perimeter and is directly accessible from the internet, handling external device registrations and media traffic securely via encrypted channels.

By employing Expressway-C and Expressway-E, mobile users can register their devices using standard protocols like SIP and make or receive calls seamlessly, similar to an internal user. This eliminates the need for complex VPN configurations or intricate user setups, fulfilling the requirement of simplicity. Other options don't address the specific scenario: Cisco Express Mobility (A) is not a Cisco product; Cisco Unified Border Element (CUBE) is used for PSTN connectivity, not mobile access; and Cisco Unified Instant Messaging and Presence (D) handles presence and IM rather than voice call connections. The pairing of Expressway-C and Expressway-E is specifically designed for secure external access to collaboration services.

Authoritative Links:

Cisco Expressway Deployment Guide:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-5/m_b_expressway-deployment-guide-x14-5.html
Cisco Expressway Data Sheet:https://www.cisco.com/c/en/us/products/collateral/unified-communications/expressway/data-sheet-c78-733962.html

Question: 3

A customer wants a video conference with five Cisco TelePresence IX5000 Series systems. Which media resource is necessary in the design to fully utilize the immersive functions?

A. Cisco PVDM4-128
B. software conference bridge on Cisco Unified Communications Manager
C. Cisco Webex Meetings Server
D. Cisco Meeting Server

Answer: D

Explanation:

The correct answer is **D. Cisco Meeting Server**. Here's why:

Cisco TelePresence IX5000 Series systems are immersive video conferencing endpoints designed for high-quality, multi-screen experiences. To fully utilize their capabilities in a multi-party conference, especially with five such systems, a dedicated meeting platform is crucial. While PVDM4-128 (A) provides DSP resources for

voice, it's not designed for the advanced video processing required for an immersive multi-party conference with several IX5000 systems. A software conference bridge on Cisco Unified Communications Manager (B) typically handles ad-hoc audio and video conferences but lacks the scalability and features required for a large-scale immersive collaboration of this nature. Cisco Webex Meetings Server (C) is a web conferencing solution, not optimized for handling dedicated immersive video endpoints like the IX5000 series within a more traditional on-premises or private cloud environment.

Cisco Meeting Server (D), however, is specifically built to handle large-scale video conferencing and provides the required features for immersive multi-party conferences, including dynamic screen layout management, high-definition video and audio transcoding, and seamless joining for the IX5000 series. It can support the specific video and audio streams and processing needs of these high-end endpoints. Cisco Meeting Server acts as the central media processing platform in this scenario. The Meeting Server enables features that are core to immersive conferences, such as continuous presence (where all participants are visible), which are essential for an experience with multiple IX5000 systems. It ensures that all feeds are scaled correctly, synchronized, and delivered smoothly for the best user experience. In summary, Cisco Meeting Server offers the necessary dedicated media processing and control required to ensure that the immersive aspects of the Cisco TelePresence IX5000 Series are fully realized across all endpoints during a multi-party conference.

Authoritative links for further research:

Cisco Meeting Server Documentation:https://www.cisco.com/c/en/us/products/conferencing/meeting-server/index.html
Cisco TelePresence IX5000 Series Data Sheet:https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-ix5000-series/index.html

Question: 4

An engineer is designing a load balancing solution for two Cisco Unified Border Element routers. The first router (cube1.abc.com) takes 60% of the calls and the second router (cube2.abc.com) takes 40% of the calls. Assume all DNS A records have been created. Which two SRV records are needed for a load balanced solution? (Choose two.)

A. _sip._udp.abc.com 60 IN SRV 2 60 5060 cube1.abc.com
B. _sip._udp.abc.com 60 IN SRV 60 1 5060 cube1.abc.com
C. _sip._udp.abc.com 60 IN SRV 1 40 5060 cube2.abc.com
D. _sip._udp.abc.com 60 IN SRV 3 60 5060 cube2.abc.com
E. _sip._udp.abc.com 60 IN SRV 1 60 5060 cube1.abc.com

Answer: CE

Explanation:

Here's a detailed justification for why options C and E are the correct SRV records for the described load-balancing scenario:

SRV (Service Location) records are used in DNS to locate services for specific protocols, such as SIP (Session Initiation Protocol). In the context of load balancing, SRV records distribute traffic across multiple servers by assigning priorities and weights. The format of an SRV record is _service._proto.name TTL class SRV priority weight port target.

In the given scenario, we're load balancing SIP traffic over UDP, which is why the service and protocol are specified as _sip._udp. The name in both records is abc.com.

Option E, _sip._udp.abc.com 60 IN SRV 1 60 5060 cube1.abc.com, correctly represents the configuration for cube1.abc.com to take 60% of the load. Priority (1) is used to signify preference, with lower values taking

precedence. Weight (60) determines the share of traffic directed to this server compared to others with the same priority. Port 5060 is the standard port for SIP over UDP and target indicates the FQDN of the server.

Option C, _sip._udp.abc.com 60 IN SRV 1 40 5060 cube2.abc.com, correctly configures cube2.abc.com for a 40% share of calls. It utilizes the same priority 1, indicating that traffic is shared among servers with the same priority, but with a different weight (40) to achieve the load balancing ratio. The weight of 40 combined with cube1.abc.com weight of 60 provides the required 60/40 split of traffic across the two routers.

Options A, B, and D are incorrect. Option A has the weight as 60 and priority as 2 which is not ideal as priority should be 1, Option B has weight and priority inverted and Option D has weight as 60 and priority as 3. These options all incorrectly configure the weights or priorities, or both, leading to incorrect load distribution.

In summary, options C and E are the appropriate SRV records for directing 60% of SIP traffic to cube1.abc.com and 40% to cube2.abc.com. This approach allows for even distribution of load across the two Cisco Unified Border Element routers using SRV based routing.

Authoritative Links for further research:

RFC 2782 - A DNS RR for specifying the location of services (DNS SRV):
https://datatracker.ietf.org/doc/html/rfc2782
Cisco Unified Communications SRV Record Configuration:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1/systemConfig/cucm_b_system-configuration-guide-1251/cucm_b_system-configuration-guide-1251_chapter_01001.html
Understanding DNS SRV Records for SIP Load Balancing:https://www.voip-info.org/dns-srv/

Question: 5

Which two functions are provided by Cisco Expressway Series? (Choose two.)

A. interworking of SIP and H.323
B. endpoint registration
C. intercluster extension mobility
D. voice and video transcoding
E. voice and video conferencing

Answer: AB

Explanation:

Cisco Expressway provides crucial functionalities for enabling collaboration across different networks and technologies. Option A, interworking of SIP and H.323, is a core function of Expressway. It acts as a gateway, translating signaling and media between these two common VoIP protocols, enabling seamless
communication between devices using either SIP or H.323. This interworking capability is essential for interoperability in diverse communication environments. Option B, endpoint registration, is also a key function.

Expressway can handle the registration of endpoints, such as mobile clients and remote devices, allowing them to connect to the internal collaboration network securely from outside the firewall, a functionality often referred to as Mobile and Remote Access (MRA). Options C, D, and E are not primarily provided by
Expressway. Intercluster extension mobility is typically a Cisco Unified Communications Manager (CUCM) feature. Voice and video transcoding can be handled by various Cisco media processing components, but it is not the primary focus of Expressway. Similarly, while Expressway may support conference calls via its traversal capabilities, the primary voice and video conferencing functionality resides within CUCM or other conferencing platforms. Therefore, options A and B correctly reflect the main capabilities of Cisco
Expressway.

For further information, you can refer to the official Cisco documentation on Expressway:Cisco Expressway SeriesCisco Expressway Configuration Guides

Question: 6

An incoming off-net call to a user fails. An engineer notices that the off-net call is G.711, but the phone accepts only G.729. Which media resource on a Cisco
Unified Border Element and Cisco Unified Communications Manager must the engineer configure to manage the codec negotiation?

A. transcoder
B. CFB
C. MOH
D. MTP

Answer: A

Explanation:

The correct answer is A, a transcoder. When an off-net call arrives using G.711 codec, but the receiving phone only supports G.729, a codec mismatch occurs. To resolve this, a media resource capable of converting between these codecs is necessary. A transcoder's primary function is to translate digital media streams from one codec to another. In this scenario, the transcoder would receive the G.711 audio stream, convert it to G.729, and then deliver it to the phone. While other media resources exist, they do not perform the necessary codec conversion. CFB (Conference Bridge) is used for multi-party audio, MOH (Music on Hold) provides audio during hold, and MTP (Media Termination Point) aids in signalling normalization, not codec translation.

Therefore, for direct codec negotiation and conversion between G.711 and G.729 in this situation, the transcoder is the essential component. Without the transcoder, the call would fail due to the incompatible codecs.

For further research, consider the following resources:

Cisco Collaboration SRND:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/cucm/cucm_b_cisco-unified-communications-manager-srnd.html
Cisco Unified Communications Manager Documentation:https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-technical-reference-list.html **Cisco Media Resources:** Search within Cisco documentation using keywords like "Cisco Transcoder," "Media Termination Point," "Conference Bridge," and "Music on Hold" to learn more about their specific functions in a Cisco Collaboration Environment.

Question: 7

Which Cisco Unified Communications Manager service parameter should be enabled disconnect a multiparty call when the call initiator hangs up?

A. Drop Ad Hoc Conference
B. H.225 Block Setup Destination
C. Block OffNet To OffNet Transfer
D. Enterprise Feature Access Code for Conference

Answer: A

Explanation:

The correct answer is A. **Drop Ad Hoc Conference**.

Here's the justification:

In Cisco Unified Communications Manager (CUCM), a service parameter directly controls how ad-hoc conference calls behave when the initiator disconnects. The "Drop Ad Hoc Conference" parameter specifically addresses this scenario. When enabled (set to "True"), if the user who initiated the conference hangs up, the entire conference call is terminated, disconnecting all participants. If this parameter is disabled (set to "False"), the conference call would remain active even after the initiator hangs up, allowing the remaining participants to continue their conversation, potentially without a designated host, until other participants disconnect as well. The absence of this setting or configuration to “True” would lead to unexpected behavior of the remaining participants being able to continue, leading to confusion.

Options B, C, and D are incorrect:

B. H.225 Block Setup Destination: This parameter relates to controlling call signaling using H.225, and preventing certain types of call setups, not call disconnection behavior. This parameter limits where a call may be routed.

C. Block OffNet To OffNet Transfer: This parameter controls call transfers between external (off-net) parties. It has nothing to do with disconnecting multiparty calls when the initiator hangs up. It is related to call control and limiting the transfer ability.

D. Enterprise Feature Access Code for Conference: This setting defines access codes used to invoke conference functionality; not related to the behavior when the call initiator hangs up. This is to invoke the conference feature using a dial-in feature code.

Therefore, only "Drop Ad Hoc Conference" directly impacts the desired behavior of disconnecting the conference call when the initiator disconnects.

Authoritative Links for further research:

Cisco Unified Communications Manager Administration Guide: This guide provides comprehensive information about all CUCM service parameters, including “Drop Ad Hoc Conference.” Search within the relevant version documentation for your CUCM installation for detailed explanation of this parameter. Cisco documentation is the single source of truth.

Cisco Community Forums: The Cisco Community often contains discussions around specific parameters, best practices, and troubleshooting tips related to Cisco Unified Communications Manager. This is a great place to see real world usage and discussion around these parameters.

Question: 8

A network administrator deleted a user from the LDAP directory of a company. The end user shows as Inactive LDAP Synchronized User in Cisco Unified
Communications Manager. Which step is next to remove this user from Cisco Unified Communications Manager?

A. Delete the user directly from Cisco Unified Communications Manager

B. Restart the Dirsync service after the user is deleted from LDAP directory.

C. Execute a manual sync to refresh the local database and delete the end user.

D. Wait 24 hours for the garbage collector to remove the user.

Answer: D

Explanation:

The correct answer is **D. Wait 24 hours for the garbage collector to remove the user.** Here's why:

Cisco Unified Communications Manager (CUCM) synchronizes user data with the LDAP directory. When a user is deleted from LDAP, CUCM doesn't immediately reflect this change. Instead, the user is marked as "Inactive LDAP Synchronized User." CUCM employs a background process known as the "garbage collector" to handle the removal of these inactive users. This process typically runs on a scheduled basis, usually every 24 hours by default.

Option A is incorrect because directly deleting the user from CUCM after LDAP synchronization can lead to inconsistencies and potential issues with future synchronizations. Option B is incorrect because restarting the Dirsync service does not trigger immediate removal of the "Inactive LDAP Synchronized User", it only applies when changes are made in LDAP, and the next scheduled sync will pick them up. Option C is also incorrect as a manual sync will only update the status and would not delete the user. The garbage collector is responsible for identifying and purging inactive users after a waiting period, typically 24 hours by default to handle delayed replication between LDAP directories.

This behavior is a design decision to allow for data consistency and prevent accidental deletions due to temporary issues with LDAP. It ensures that deleted users are properly handled and do not leave behind orphaned data. This aligns with best practices in cloud environments, where asynchronous processes and delayed actions are used to manage resources efficiently.

Authoritative links for further research:

Cisco Unified Communications Manager Administration Guide (for your specific version): Search for "LDAP directory synchronization", "Inactive LDAP Synchronized User", and "garbage collector". While specific documentation might vary by version, the core concepts remain consistent.

You can find the guide at Cisco's website. Make sure to select the correct version of CUCM.

Cisco Community Forums: Search for "Inactive LDAP synchronized user CUCM" to find discussions and troubleshooting tips related to this topic. Cisco Community

Question: 9

A customer has Cisco Unity Connections that is integrated with LDAP. As a Unity Connection administrator, you have received a request to change the first name for VM user. Where must the change be performed?

A. Cisco Unity Connection
B. Cisco Unified Communications Manager end user
C. Active Directory
D. Cisco IM and Presence

Answer: C

Explanation:

The correct answer is **C. Active Directory**. This is because when Cisco Unity Connection is integrated with LDAP (such as Active Directory), user information like first names, last names, and email addresses are synchronized from the directory service to Unity Connection. Unity Connection does not act as the source of truth for these details in such configurations. Instead, it relies on the directory service as the authoritative source. Therefore, any changes to these attributes, including the first name, must be made directly within the Active Directory. After the change in Active Directory, a synchronization process will propagate the updated information to Cisco Unity Connection. Altering the first name directly in Unity Connection or other Cisco Unified Communications Manager (CUCM) components would be overwritten by the next LDAP sync

operation, as Unity Connection respects the directory service as the primary user information repository. Making the change in Active Directory ensures that the correct name is consistent across systems that rely on that Active Directory instance for identity management. This is a fundamental concept in identity federation within unified communications and cloud-based directory services.

For further research, please refer to the following Cisco documentation:

Cisco Unity Connection LDAP Integration:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/integration/guide/cucuicg1201/cucuicg1201
Understanding User Synchronization with LDAP:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/user_config/guide/b_cucu12xucg/b_cucu12

Question: 10

Which configuration step is necessary for a Cisco SIP phone to synchronize its time with a specific source?

A. Add a Phone NTP Reference to the Date/Time Group.
B. Assign the device to the correct region.
C. Change the Time Format from 24-hour to 12-hour.
D. Change the Time Zone from America/Los_Angeles" to Etc/GMT+8".

Answer: A

Explanation:

The correct answer is **A. Add a Phone NTP Reference to the Date/Time Group.**

Cisco SIP phones rely on accurate time synchronization for various functions, including call logging, meeting scheduling, and authentication. Network Time Protocol (NTP) is the standard protocol used to synchronize clocks across networks. To ensure a Cisco SIP phone gets the correct time from a specific source, you need to configure its NTP settings. This is managed via the Date/Time Group in Cisco Unified Communications Manager (CUCM).

The Date/Time Group allows administrators to define a set of time-related parameters, including a primary and secondary NTP server. By adding a specific "Phone NTP Reference" to the Date/Time Group, you are instructing devices assigned to this group to use the specified NTP server(s) as their time source. This association is crucial for the phone to obtain synchronized time.

Options B, C, and D are incorrect for the following reasons:

B. Assign the device to the correct region: Regions control call bandwidth, audio codecs, and location-specific settings, not NTP configuration. While the region might indirectly influence call behavior based on time zone, it does not affect NTP synchronization.

C. Change the Time Format from 24-hour to 12-hour: The time format affects how time is displayed on the phone, not the underlying time synchronization with a source. Changing this setting does not impact the phone's ability to receive accurate time from an NTP server.

D. Change the Time Zone from America/Los_Angeles to Etc/GMT+8: While selecting the appropriate time zone is important for the phone to display the correct local time, this setting is applied after the phone has synchronized its time with a specific NTP source. Setting the time zone on the phone without a reliable source of time would still result in inaccurate local time display relative to the actual time. Time zone settings don't replace the need for a source of accurate time.

In summary, while other configurations influence the display and behavior of a Cisco SIP phone, the key to time synchronization relies directly on the Date/Time Group and its configured "Phone NTP Reference" to a

specific NTP server.

Authoritative Links:

Cisco Unified Communications Manager Configuration Guide:
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html (Search for "Date/Time Groups" and "NTP configuration").

Network Time Protocol (NTP) RFC 5905:https://www.rfc-editor.org/rfc/rfc5905 (For details on the NTP protocol itself).

Question: 11

After an engineer runs the utils ntp status command on the Cisco Unified Communications Manager publisher, the stratum value is 16. Which issue can the
Cisco Unified CM cluster experience?

A. Unified CM sends an NTPv4 packet.
B. Database replication is not synchronized on the Unified CM nodes.
C. The cluster loses access to port 124 at the firewall.
D. The date/time group on all phones defaults to the time zone of the engineer.

Answer: B

Explanation:

The correct answer is **B. Database replication is not synchronized on the Unified CM nodes.**

Here's the justification:

An NTP stratum value of 16 indicates that the Cisco Unified Communications Manager (CUCM) server is not synchronized with a reliable time source. NTP uses a hierarchical system, with stratum 1 being the most accurate time source (usually an atomic clock) and each subsequent stratum having lower accuracy. A stratum 16 value signals that the CUCM server is considered unsynchronized and is unlikely to be receiving a reliable time signal from a higher stratum server. CUCM relies heavily on synchronized time across all nodes within the cluster to ensure consistent operation, especially for database replication.

When the publisher's stratum value is 16, it means the database replication process is likely impacted, leading to inconsistencies between the publisher and subscriber databases. This can manifest as call routing issues, user login failures, and other functionality problems across the cluster. CUCM employs a real-time database that requires all nodes to have an accurate and consistent view of the data to function properly. A high stratum value points directly to the core need for accurate time synchronization for proper database functioning. Options A, C and D are not directly related to NTP stratum issues. NTPv4 is a protocol used by NTP, firewall issues will not change stratum, and phone timezones are separate to NTP.

Authoritative Links:

1. Cisco Collaboration System 12.x SRND:
   https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/collaboration/Collabora
   (Search for NTP and database synchronization)
2. Cisco Documentation on NTP: https://www.cisco.com/c/en/us/support/docs/voice/cisco-unified-communications-manager-callmanager/10674-ntp.html
3. RFC 5905 (NTPv4 specification): https://datatracker.ietf.org/doc/html/rfc5905

Question: 12

When a new SIP phone is registered to Cisco Unified Communications Manager, it keeps failing and showing an `unprovisioned` error message in the phone display. Which problem is a possible cause of this issue?

A. Auto-registration is disabled on the Cisco Unified Communications Manager nodes and the phone device does not have a DN configured.

B. The DN assigned to the phone is already in use by another SIP phone.

C. The phone cannot download and install the latest firmware.

D. The DHCP settings are set incorrectly and the phone does not have an alternate TFTP defined.

E. The DN configuration for this phone is shared with an SCCP phone, which is not supported.

Answer: A

Explanation:

The correct answer is **A. Auto-registration is disabled on the Cisco Unified Communications Manager nodes and the phone device does not have a DN configured.**

Here's why: When a new SIP phone attempts to register with Cisco Unified Communications Manager (CUCM), it goes through a process of discovery and provisioning. If auto-registration is disabled on CUCM, the system will not automatically assign a directory number (DN) and device configuration to the phone upon registration. The phone, not having a predefined DN in the CUCM database, will hence remain "unprovisioned." This status indicates that while the phone is communicating with CUCM, it lacks the necessary configuration to become fully functional.

Option B, while a valid problem (duplicate DNs), would typically result in registration issues and potentially conflicts, but the error message isn't likely to specifically state "unprovisioned" on the phone's display. Option C, firmware issues, might cause registration problems and loop cycles, but it wouldn't lead to the "unprovisioned" message. Option D, incorrect DHCP, would impact initial connectivity and prevent the phone from finding the TFTP server for configuration files; thus this would likely not lead to the specific “unprovisioned” message, but instead registration errors. Option E, while true that a DN cannot be shared between SCCP and SIP phones, would generally show a different kind of issue, such as registration failure due to incompatible protocols, but not specifically an unprovisioned status. It should be noted that the phone needs a DN to register and the ‘auto-registration’ mechanism in CUCM is how to automatically assign one. Therefore, if this is off and the device is not configured to have a DN, it will remain unprovisioned.

For further research, refer to Cisco's documentation on auto-registration and phone provisioning:

Cisco Unified Communications Manager System Configuration Guide: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html (Specifically, search for "Auto-registration" within a configuration guide relevant to your CUCM version.)
Cisco Collaboration Help:https://www.cisco.com/c/en/us/support/unified-communications/index.html (Search for relevant topics like "Adding Phones" or "Phone Registration")

Question: 13

Which DHCP option must be set up for new phones to obtain the TFTP server IP address?

A. option 15

B. option 6

C. option 66

D. option 120

Answer: C

Explanation:

The correct DHCP option for a VoIP phone to discover its TFTP server's IP address is option 66. DHCP options are used to convey configuration parameters to network devices during the IP address assignment process. Option 66, specifically, is designated for specifying the IP address or hostname of a TFTP server. VoIP phones rely on a TFTP server to download their firmware, configuration files, and other necessary resources during boot-up. When a phone initiates, it requests an IP address through DHCP and, along with the IP address, it requires the TFTP server details. The DHCP server, upon receiving the request, responds with the IP address, subnet mask, default gateway, and if configured, DHCP option 66 containing the TFTP server address. Option 15 is associated with specifying the domain name, option 6 is for DNS server addresses, and option 120 is for SIP server information which is a different protocol. Therefore, out of the provided options, only option 66 is specifically designed for delivering TFTP server information to a network client, such as a VoIP phone. Hence, it is the necessary DHCP option for successful TFTP server discovery in the given scenario.

Authoritative Links:

Cisco Documentation on DHCP Options:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/configuration/15-mt/iad-15-mt-book/iad-dhcp-server.html (Search for "DHCP Option 66") **RFC 2132 - DHCP Options and BOOTP Vendor Extensions:**https://datatracker.ietf.org/doc/html/rfc2132 (Refer to the section on Vendor Specific Information, Option 66).
Network Dictionary Definition of Option 66:https://www.networkdictionary.com/dhcp/dhcpoption66.php

Question: 14

Which two conditions must a user meet to provision a new device using the Self-Provisioning feature? (Choose two.)

A. The user must have a primary extension.
B. At least two DNs must be assigned to the user device.
C. The user must be part of Standard CCM Super User.
D. The user must have the appropriate universal device template linked to the user profile.
E. The user must have at least one user device profile assigned.

Answer: AD

Explanation:

Let's break down why options A and D are the correct answers regarding Cisco's Self-Provisioning feature for collaboration devices.

Self-Provisioning in Cisco Unified Communications Manager (CUCM) allows users to easily add their devices without administrative intervention. For this to work, the user must have a primary extension (option A). This extension acts as the user's identifier and is crucial for linking the newly provisioned device to their profile. It's the cornerstone for routing calls and associating services with that specific user. Think of the primary extension as the user's "home address" within the system; the device needs to know where to connect the user.

Furthermore, the user's profile must be associated with an appropriate universal device template (option D). This template defines the basic configurations for the device, such as button layout, softkey assignments, and other settings. Without it, CUCM wouldn't know how to initialize and configure the new device for the user. This templating approach ensures consistency and standardizes the user experience across the organization. The universal device template also provides for scalability by leveraging reusable configurations.

Option B is incorrect as the number of DNs (Directory Numbers) on the user's device is not a prerequisite. A single DN could suffice. Option C is incorrect because granting "Standard CCM Super User" privileges to all users for device provisioning is both a security risk and unnecessary. Finally, option E is incorrect because user device profiles, while useful for specific configurations, are not a requirement for Self-Provisioning. The Universal Device Template is more directly linked to the provisioning process itself.

In summary, a valid primary extension and an applicable universal device template are the fundamental requirements for self-provisioning to succeed in Cisco CUCM.

For further research, you can refer to Cisco's official documentation on Self-Provisioning and Device Templates:

Cisco Unified Communications Manager Configuration Guide (Navigate to the relevant version's configuration guide and search for "Self-Provisioning" and "Universal Device Templates").
Cisco Collaboration Help

Question: 15

How many DNS SRV entries can be defined in the SIP trunk destination address field in Cisco Unified Communications Manager?

A. 1
B. 8
C. 16
D. 4

Answer: A

Explanation:

The correct answer is **A. 1**. Cisco Unified Communications Manager (CUCM) only supports a single DNS SRV record entry within the SIP trunk's destination address field. While DNS SRV records are designed to provide redundancy and load balancing, CUCM's SIP trunk configuration focuses on a primary destination. If multiple SRV records are returned by a DNS query, CUCM will typically select the first one provided. CUCM does not actively utilize or failover between multiple SRV records defined within that single destination address entry. The purpose of using a DNS SRV record in this context is to allow for dynamic location of the SIP server rather than relying on a static IP address. The SIP trunk will leverage that single resolved address. To achieve redundancy, it is recommended to configure multiple SIP trunks instead of attempting to use multiple SRV records within one single trunk. In essence, a primary SRV record pointing to one SIP server would be on one SIP trunk. Should that server be down, call control can go to the second SIP Trunk.

For further information, you can refer to the Cisco documentation for SIP trunk configuration in CUCM and DNS SRV concepts. Here is a link to the Cisco guide on this topic that may be helpful:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1/systemConfig/cucm_b_system-configuration-guide-1251/cucm_b_system-configuration-guide-1251_chapter_01000.html#task_34014686

Question: 16

On which Cisco Unified Communications Manager nodes can the TFTP service be enabled?

A. any node
B. any two nodes

C. only nodes that have Cisco Unified CM service enabled

D. any subscriber nodes

Answer: A

Explanation:

The correct answer is A, any node. The Trivial File Transfer Protocol (TFTP) service in Cisco Unified Communications Manager (CUCM) is responsible for providing configuration files, firmware images, and other necessary files to Cisco IP phones and other endpoints. Unlike some services that are restricted to specific roles, the TFTP service can be activated on any node within a CUCM cluster, including publisher and subscriber nodes. This flexibility allows for redundancy and load balancing. While it's common to enable TFTP on the publisher node, enabling it on multiple nodes is a best practice for high availability. Should the primary TFTP server (often the publisher) become unavailable, endpoints can retrieve configurations from a secondary TFTP server, minimizing service disruption. The choice of which node to activate TFTP on is a design decision, and administrators may choose to enable it on one or more subscribers alongside the publisher to meet their specific redundancy and performance requirements. There isn't an inherent restriction that ties TFTP to only subscriber nodes or nodes with the Cisco Unified CM service active. All nodes are capable of hosting the TFTP service. This flexibility is a key characteristic of how Cisco designed the CUCM architecture.

Authoritative Link for further research:Cisco Unified Communications Manager Configuration Guide - Specifically search for sections covering "TFTP Service".

Question: 17

Which issue causes slips on a PRI?

A. incorrect clock source

B. incorrect encapsulation

C. incorrectly configured time zone

D. change in the line code

Answer: A

Explanation:

Here's a detailed justification for why the correct answer is A, incorrect clock source, regarding slips on a PRI (Primary Rate Interface) in the context of Cisco collaboration technologies:

PRI circuits rely on precise timing for synchronous data transmission. Slips, which manifest as repeated or dropped bits, occur when there is a timing mismatch between the transmitting and receiving ends. An incorrect clock source at either end of the PRI link creates a timing discrepancy. The receiving side expects data at a specific rate determined by its clock source. If the incoming data arrives at a different rate due to a misconfigured clock at the transmitting end, the receiver struggles to correctly interpret the data, leading to slips. These slips result in garbled voice or data, ultimately degrading the service quality. The clock source dictates the fundamental timing of data transmission and is crucial for maintaining synchronization in synchronous circuits. Mismatched or incorrect clocking will always introduce these issues. An incorrect clock source directly impacts the consistency of data flow on the PRI. Options B, incorrect encapsulation, and D, change in line code, relate to how data is formatted but not the timing itself. Option C, incorrectly configured time zone, impacts time stamps on call records but not the real-time transmission of data. Clock synchronization is foundational for PRI operation; without it, slips will almost always occur.

Authoritative link for further research:

Cisco Documentation on PRI Synchronization:
https://www.cisco.com/c/en/us/td/docs/ios/voice/pri/configuration/guide/12_4t/priconf.html - While slightly dated this document contains relevant explanations on the importance of clocking for PRI interfaces.

Question: 18

An administrator recently upgraded a Cisco Webex DX80 through its web interface but discovered the next morning that the unit has received to its previous version. What must the administrator do to prevent this from happening again?

A. Assign a phone security profile with secure SIP.
B. Set the prepare cluster for rollback to pre-8.0 enterprise parameter to true.
C. Confirm the phone load name in the phone configuration.
D. Assign a universal device template to the phone.

Answer: C

Explanation:

The correct answer is **C. Confirm the phone load name in the phone configuration.** This relates to how Cisco Unified Communications Manager (CUCM) manages firmware upgrades for IP phones, including Webex DX devices. When an administrator upgrades a DX80 via its web interface, it often involves downloading a temporary firmware version. However, after the device reboots or at a scheduled time, it might revert to the firmware version defined by its device configuration within CUCM. CUCM uses the "phone load name" to specify which firmware version a device should run. If this load name does not correspond to the intended upgraded version, the DX80 will revert after reboot or the designated period. Therefore, the administrator must verify the phone's configuration in CUCM and ensure the "phone load name" parameter is set to the desired upgraded firmware version to enforce persistent upgrading. Options A, B, and D do not directly address how firmware upgrades are managed via load names. A security profile might add encryption, but wouldn't dictate the firmware version. B refers to a specific cluster rollback parameter which is not relevant to DX80 individual devices. D concerns device templates which are used for configuration profiles, and while relevant to managing many devices, don't fix the missing firmware load assignment.

Here are some authoritative links for further research:

Cisco Unified Communications Manager Features and Services Guide, Release 12.5(1):
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/rel_12_5_1/feature-configuration/cucm_b_feature-configuration-guide-1251/cucm_b_feature-configuration-guide-1251_chapter_01100.html - This covers firmware management for phones.

Cisco IP Phone Administration Guide for Cisco Unified Communications Manager:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/all_models/admin/english/administering-ip-phones/cuipph-admin-guide-book/cuipph-admin-guide-phone-load.html - Explains the "phone load name" concept.

Cisco Webex DX Series Deployment Guide:
https://www.cisco.com/c/en/us/td/docs/telepresence/endpoint/dx-series/deployment_guide/dx_series_deployment_guide/m_dx_firmware_upgrade.html - Provides DX specific firmware upgrade information.

Question: 19

An engineer is notified that the Cisco TelePresence MX800 that is registered in Cisco Unified Communications Manager shows an empty panel, and the Touch 10 shows a corresponding icon with no action when pressed. Where does the engineer go to remove the inactive custom panel?

A. The Software Upgrades page in CUCM OS Administration
B. The In-Room Control Editor on the webpage of the MX800
C. The phone configuration page in CUCM Administration
D. The SIP Trunk Security Profile page in CUCM Administration

Answer: B

Explanation:

The correct answer is **B. The In-Room Control Editor on the webpage of the MX800.** Here's why:

The issue described pertains to a malfunctioning custom panel on a Cisco TelePresence MX800, specifically the Touch 10 interface. This indicates a problem with the device's internal configuration, not with the Cisco Unified Communications Manager (CUCM) system-level configurations. CUCM primarily manages call control and device registration, not the intricate details of the device's user interface customization. Options A, C, and D are all CUCM-related, therefore incorrect for this particular issue.

The In-Room Control Editor is a web-based tool embedded directly within the MX800's software. It allows administrators to design and manage custom panels, including adding, modifying, and removing them. Since the problem is an inactive or empty custom panel, the logical place to address this is within the device's configuration settings, specifically the In-Room Control Editor. It would not be related to Software Upgrades within CUCM (Option A), Phone configuration on CUCM (Option C), nor a security setting for SIP Trunks (Option D). The described situation is a localized issue within the endpoint, pointing to an issue needing adjustment within the MX800 itself.

Authoritative links:

Cisco TelePresence MX Series Administration Guide: While specific versions vary, search for "In-Room Control Editor" within the documentation for your specific MX800 model. These guides typically cover detailed setup and troubleshooting for custom panels. https://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-mx-series/products-installation-and-configuration-guides-list.html (Navigate to your MX series model from this link).

Cisco Collaboration Help: Search for related terms such as "Touch 10 customization," "In-Room Control Editor" in the general Cisco Collaboration Help area for guides on interface customization.
https://help.webex.com/

Question: 20

A presence redundancy group is deployed, and an engineer initiates a manual fallback. Which statement about Cisco Server Recovery Manager is true?

A. disconnects all users that had been failed over, and the users must log in again
B. disconnects all users that had been failed over
C. restarts critical services on the secondary node
D. restarts the Cisco Presence Engine

Answer: A

Explanation:

The correct answer is **A. disconnects all users that had been failed over, and the users must log in again.** Here's why:

Presence redundancy groups in Cisco Collaboration deployments aim to ensure high availability of presence services. A manual fallback, initiated after a failover to a secondary node, indicates a return to the primary server's operation. Cisco Server Recovery Manager (SRM) facilitates this process. When a fallback is executed, SRM actively reverses the failover. This involves ceasing services on the secondary server, which currently hosts the failed-over users' presence information. Consequently, any users actively connected and utilizing presence services via the secondary node are forcibly disconnected. They are essentially moved back to the primary server's control. This disconnection forces these users to re-authenticate, establishing new sessions directly with the primary server. Options B, C, and D are not entirely accurate. While critical services are indeed involved during fallback, merely restarting them is not the central action. The primary focus is on shifting the user's connections back to the primary, hence causing the disconnect. While Cisco Presence Engine is involved in the process, the core impact is user disconnection, not just an engine restart. This operation ensures that the primary server resumes its role with fully functional presence service control.

Relevant concept: High Availability, Failover, Fallback, Presence Services, Session Management.

For further research, consult the official Cisco documentation on Presence Redundancy and Cisco Server Recovery Manager:

Cisco Collaboration System SRND: This document provides comprehensive information on system design, including high availability.

Cisco Unified Communications Manager Documentation: This covers all aspects of managing and configuring Cisco UC systems.

Cisco Support Forums and Knowledge Base: Often provides specific troubleshooting information and best practices related to manual fallback.

These links provide authoritative information that further support this explanation.

Question: 21

Which packet delay is the maximum supported between Cisco Unified Communications Manager nodes for clustering over WAN deployments?

A. 150 ms round tip
B. 510 ms round trip
C. 40 ms round trip
D. 80 ms round trip

Answer: D

Explanation:

The correct answer is 80 ms round trip (D) because Cisco mandates a maximum round-trip latency of 80 milliseconds between nodes within a Cisco Unified Communications Manager (CUCM) cluster that are geographically dispersed across a WAN. This limit is critical for maintaining real-time communication synchronization, which relies on timely database replication and inter-server communication. Higher latency introduces significant delays in signaling and media streams, leading to call failures, dropped connections, and poor audio quality. While WAN deployments offer benefits like increased redundancy and disaster recovery, they also present challenges regarding network latency. Exceeding the 80 ms threshold can destabilize the cluster, impacting functionality. This limitation is not a general networking limitation, but a specific requirement for the stringent real-time operation of CUCM clusters. Cisco designs their collaboration solutions under strict performance criteria, and latency is a key metric that contributes to proper functionality. Therefore, keeping network latency under the stated threshold is paramount for effective operation of a CUCM cluster deployed across a WAN.

Authoritative Links:

Cisco Collaboration System SRND:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/collaboration/collaboration-system-12.html (Refer to the section on WAN Considerations) - While the link is for version 12, the latency recommendations remain similar across recent CUCM versions. Look for the relevant documentation for the specific version in use.

Cisco Unified Communications Manager Compatibility Matrix:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/compat/uccx_compat_matrix.html While this link is to the compatibility matrix, relevant latency requirements can be found in the overall documentation for CUCM.

Question: 22

A user dials 9011841234567 to reach Vietnam. Which steps send the call to the PSTN provider as 011841234567? A.

in the Called Party Transformation Pattern Configuration section,
B. configure the Pattern as 9.011841234567
configure the Discard Digits as Predot

in the Calling Party Transformation Patterns section,
C. configure the Pattern as 9.011841234567
configure the Discard Digits as Predot 10-10-Dialing

in the Called Party Transformation Pattern Configuration section,
D. configure the Pattern as 9.011841234567
configure the Discard Digits as Predot 10-10-Dialing

in the Called Party Transformation Patterns section,
configure the Pattern as 9.011841234567
configure the Discard Digits as Predot

Answer: A

Explanation:

A here. Remember finding the documentation some days ago confirming A.

Question: 23

Where is the default Interregion Maximum Session Bit Rate for a region configured?

A. Service Parameter Configuration
B. Enterprise Phone Configuration
C. Enterprise Parameters Configuration
D. Region Configuration

Answer: A

Explanation:

The correct answer is **A. Service Parameter Configuration**. The Interregion Maximum Session Bit Rate, which governs bandwidth usage for calls between different regions within a Cisco Unified Communications Manager (CUCM) cluster, is a system-wide setting. This parameter is not associated with individual phones, enterprise-wide settings, or region-specific configurations directly. Instead, it's a service parameter because it affects how the call control service operates and enforces bandwidth policies across the whole deployment.

Specifically, it controls the maximum audio and video bitrate permitted for connections between any two regions. Service parameters provide a granular level of control for CUCM system functionalities. They are applied globally and can be very impactful on call quality and resource allocation. While Regions define logical network boundaries, they rely on service parameters to enforce specific bandwidth constraints. Hence, the Interregion Maximum Session Bit Rate is an operational configuration parameter set at the service layer level. Enterprise Parameters, on the other hand, deal with organizational-level defaults and characteristics, not system-wide operational limits. Enterprise Phone Configuration provides phone-specific customizations.

By configuring it as a service parameter, Cisco allows a centralized way to govern inter-region bandwidth usage.

Further research:

Cisco Unified Communications Manager Administration Guide: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html (Search within the guide for "Service Parameters" and "Interregion Maximum Session Bit Rate" for specific details.)
Cisco Unified Communications Manager Documentation:https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html (Browse the available documentation for detailed information on region configuration and service parameters.)

Question: 24

A Cisco TelePresence SX80 suddenly has issues displaying main video to a display over HDMI. Which command can you use from the SX80 admin CLI to check the video output status to the monitor?

A. xStatus Video Output
B. xCommand Video Status
C. xConfiguration Video Output
D. xStatus HDMI Output

Answer: A

Explanation:

The correct command to check video output status on a Cisco TelePresence SX80 via the admin CLI is xStatus Video Output. Let's break down why:

The xStatus family of commands in Cisco TelePresence endpoints is designed to retrieve real-time operational status information. Specifically, xStatus Video Output provides details about the current state of video outputs, including resolution, active output connectors, and any detected errors. This command directly addresses the need to diagnose a video display problem.

In contrast, xCommand Video Status is not a valid command within the SX80's CLI. While xCommand commands are used for executing actions or changing settings, video status retrieval belongs to the xStatus category. Similarly, xConfiguration Video Output deals with configuring the video output settings, not necessarily for real-time troubleshooting. xStatus HDMI Output is a more specific command that might give

detailed HDMI status but does not give the holistic view offered by the xStatus Video Output command which provides overall video output status including other outputs beyond just HDMI.

Therefore, when faced with an issue of video display problems on an SX80 over HDMI, xStatus Video Output provides the quickest and most relevant information to understand the immediate problem, such as whether the device detects an active video signal output. This helps system administrators isolate the root cause of video issues quickly and efficiently, which is a crucial step in maintaining seamless video conferencing experiences.

Relevant links:

Cisco Collaboration Endpoints API Reference Guide: This guide provides extensive details on all commands available for the Cisco TelePresence endpoints, including xStatus and xCommand families. Search for the appropriate section for your specific device for the most accurate command documentation.

https://www.cisco.com/c/en/us/td/docs/telepresence/endpoint/ce9/api-reference-guide/ce9-api-reference-guide.html - Replace "ce9" with your device version if it differs.

Cisco support forums: Cisco's support communities are excellent resources for real-world examples of troubleshooting Cisco TelePresence issues.

https://community.cisco.com/

Question: 25

Which statement about Cisco Unified Communications Manager and Cisco IM and Presence backups is true?

A. Backups should be scheduled during off-peak hours to avoid system performance issues.
B. Backups are saved as .tar files and encrypted using the web administrator account.
C. Backups are saved as unencrypted.tar files.
D. Backups are not needed for subscriber Cisco Unified Communications Manager and Cisco IM and Presence servers.

Answer: A

Explanation:

The correct answer is A: Backups should be scheduled during off-peak hours to avoid system performance issues. This is because creating backups, especially full backups, is a resource-intensive operation. During the backup process, Cisco Unified Communications Manager (CUCM) and Cisco IM and Presence servers need to read large amounts of data from disk, compress it, and then write it to the backup location. This can consume significant CPU, memory, and I/O resources. If backups are run during peak hours, when the system is handling high call volume and user activity, it can lead to performance degradation, such as slower call processing, delayed presence updates, and even service interruptions. Therefore, scheduling backups during off-peak hours, when system load is lower, ensures minimal impact on user experience.

Options B and C are incorrect because CUCM backups are not encrypted by default, although encryption can be configured separately using a certificate. The backups are indeed saved as .tar files, however. Option D is also incorrect because backups are critical for all CUCM and IM and Presence servers, including subscribers. In the event of a hardware or software failure, backups are crucial for restoring the system to a working state.
Without backups, a failure could lead to significant data loss and business disruption. Backups represent a fundamental aspect of disaster recovery and business continuity planning, adhering to industry best practices for data management.Authoritative sources for further research:

Cisco Unified Communications Manager Backup and Restore Guide:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/backup_restore/12_5_1/cucm_b_backup-restore-guide-1251/cucm_b_backup-restore-guide-1251_chapter_010.html
Cisco IM and Presence Deployment Guide:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/12_5_1/cucm_b_im-and-presence-deployment-guide-1251/cucm_b_im-and-presence-deployment-guide-1251_chapter_010.html

Question: 26

What is a software-based media resource that is provided by the Cisco IP Voice Media Streaming Application?

A. video conference bridge
B. auto-attendant
C. transcoder
D. annunciator

Answer: D

Explanation:

The correct answer is D, an annunciator. Cisco's IP Voice Media Streaming Application (IP VMSA) provides software-based media resources, and one of its core functionalities is hosting annunciator services. Annunciators are used to play pre-recorded audio prompts or messages to callers in various scenarios, such as during call routing, queueing, or informational announcements. Unlike video conference bridges (A), which handle real-time video and audio conferencing, or auto-attendants (B) which manage call routing based on user input, or transcoders (C) that convert between different audio or video formats, annunciators are specifically designed for delivering static audio. IP VMSA leverages server resources to host these annunciator prompts, making them readily available for use within a Cisco collaboration environment. This software implementation eliminates the need for dedicated hardware devices to perform these functions, aligning with the cloud computing principle of resource virtualization and cost-efficiency. Thus, the annunciator is a key media resource provided directly by the IP VMSA.

For further reading, consult Cisco's official documentation on IP VMSA and its components.https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1/systemConfig/cucm_b_syconfiguration-guide-1251/cucm_b_system-configuration-guide-1251_chapter_0100.html (Search for "Media Resource Groups")

Question: 27

When a user dials a number with a phone that is registered to the Cisco Unified Communications Manager, what is the default timeout before the number is sent?

A. 15 seconds
B. 5 seconds
C. 10 seconds
D. 3 seconds

Answer: A

Explanation:

The correct answer is **A. 15 seconds**. When a user dials a number on a Cisco IP phone registered to Cisco Unified Communications Manager (CUCM), the system employs a digit timeout mechanism. This timeout

determines how long CUCM will wait for additional digits before it considers the entered number complete and initiates call routing. By default, CUCM uses a 15-second interdigit timeout. If the user pauses dialing for 15 seconds, CUCM assumes no more digits will follow and attempts to process the dialed number. This timeout is configurable, but 15 seconds is the default out-of-the-box setting. This is essential for handling scenarios where users may dial slowly or pause between digits, allowing the system enough time to gather the complete phone number before attempting to connect the call. Options B (5 seconds), C (10 seconds), and D (3 seconds) are incorrect defaults. These shorter timeouts would lead to premature dialing attempts if users paused for more than those durations, resulting in call failures or misrouted calls. The 15-second default strikes a balance between responsiveness and accommodating varied user dialing speeds. The timeout is tied to the digit analysis and call routing process within the CUCM infrastructure. The specific setting can be managed within the CUCM administration interface under device or service parameters, allowing customization for specific deployment needs. Understanding this timeout is vital for troubleshooting call-related issues, especially when users report failed or misrouted calls due to slow dialing patterns.

Here are some authoritative links for further research:

Cisco Unified Communications Manager Configuration Guide: While a specific page might vary per CUCM version, searching for "Interdigit Timeout" or "Digit Collection Timeout" within the documentation of your specific CUCM version will yield details about this parameter. Start at the primary Cisco documentation portal: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html Then locate the configuration guide corresponding to your version.

Cisco Communities: Cisco's online forums can provide additional context and practical information from users and experts: https://community.cisco.com/

Question: 28

An engineer deploys a Cisco Expressway-E server for a customer who wants to utilize all features on the server. Which feature does the engineer configure on the Expressway-E?

A. H.323 endpoint registrations
B. VTC bridge
C. MRA
D. SIP gateway for PSTN providers

Answer: C

Explanation:

The correct answer is C, MRA (Mobile and Remote Access). Cisco Expressway-E's primary function is to securely extend collaboration services beyond the corporate network. MRA allows users with Cisco Jabber or other compatible clients to connect to on-premises Cisco Unified Communications (UC) infrastructure from outside the firewall, without requiring a VPN. This includes features like instant messaging, presence, voice, and video.

Options A, B, and D are not the primary functionalities associated with enabling all features on Expressway-E.
H.323 endpoint registration (A) is an older protocol primarily handled by Cisco Unified Communications Manager (CUCM) and not the direct focus of Expressway-E's function. VTC bridging (B) is a function often handled by conferencing servers or MCU (multipoint control units). While Expressway can facilitate communication, it's not the primary bridge. Lastly, acting as a SIP gateway for PSTN providers (D) is more the role of a Cisco Unified Border Element (CUBE) or other session border controller and not a core functionality of Expressway-E.

MRA is the key feature of Expressway-E enabling its full potential, especially when combined with Cisco Expressway-C (the core component inside the firewall). It extends communication capabilities beyond physical limitations. Without MRA, remote users would not have seamless access to the full suite of UC services.

For further research, consult the official Cisco documentation on Expressway:

Cisco Expressway Deployment Guides:https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html
Cisco Mobile and Remote Access (MRA):
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0/mra_config_guide_X14-0.htmlThese links will give a deep understanding of MRA and the general purpose of Cisco Expressway.

Question: 29

Which SNMP service must be activated manually on the Cisco UCM after installation?

A. Host Resources Agent
B. Cisco CallManager SNMP
C. Connection SNMP Agent
D. SNMP Master Agent

Answer: B

Explanation:

The correct answer is B, Cisco CallManager SNMP. While Cisco UCM (Unified Communications Manager) supports SNMP for monitoring and management, not all services are enabled by default after installation. The "Cisco CallManager SNMP" service specifically needs manual activation to enable SNMP monitoring of the call processing components of the UCM system. This service exposes critical call-related metrics, such as call volume, active calls, registered devices, and more. Without manually activating this service, network management systems (NMS) using SNMP would not be able to gather this vital performance and health data.

The other options, while related to SNMP or potentially relevant to system management, do not require manual activation after a standard UCM installation. The Host Resources Agent (A) typically handles system-level data like CPU and memory, and the SNMP Master Agent (D) facilitates overall SNMP communication, and are usually enabled by default. The "Connection SNMP Agent" (C) is not a standard component that requires manual enabling in a basic UCM installation.

Therefore, for comprehensive monitoring of call processing on a Cisco UCM system via SNMP, specifically, the "Cisco CallManager SNMP" service must be manually enabled, typically through the Cisco Unified Serviceability web interface or the CLI. This necessity differentiates it from the other listed SNMP related services. This is a specific operational step required during configuration that must be addressed to monitor call-related metrics effectively.

Authoritative Links:

1. Cisco Unified Communications Manager Configuration Guide: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html - Search within these guides for specific details on SNMP configuration and service activation for your UCM version.
2. Cisco Support Forums: https://community.cisco.com/ - A good place to search for specific user questions and answers on this topic.

Question: 30

A company deploys centralized Cisco UCM architecture for a hub location and two remote sites.
☞ The company has only one ITSP connection at the hub location, and ITSP supports only G.711 calls.☞ Remote site A has a 1-Gbps fiber connection to the hub location and calls to and from remote site A use G.711 codec.
☞ Remote site B has a 1-T1 connection to the hub location and calls to and from remote site B use G.729 codec.
Based on the provided guidance, a Cisco voice engineer must design media resource management for the customer. What is the method that needs to be followed?

A. configure the hardware transcoder on the site B router
B. configure the hardware transcoder on the site A router
C. configure the hardware transcoder on the hub location router
D. configure the software transcoder on Cisco UCM to support voice calls to and from both remote sites

Answer: C

Explanation:

The correct answer is **C. configure the hardware transcoder on the hub location router.** Here's why:

The scenario describes a centralized Cisco UCM deployment where the hub site handles the ITSP connection (which only supports G.711). Remote sites use different codecs: Site A uses G.711 over a 1Gbps fiber link, while Site B uses G.729 over a 1-T1 connection. Since the ITSP at the hub only accepts G.711, any G.729 calls from Site B must be transcoded to G.711 before reaching the ITSP, and vice versa for incoming calls.

Transcoding should be done at the hub location because this is where the ITSP connection resides. By placing the transcoder there, the hub router can convert all calls to and from the ITSP to G.711. This avoids needing transcoding at each remote site. Because Site A already uses G.711, it does not require transcoding. Software transcoders on CUCM can be used for other purposes, but hardware transcoders at the router are more efficient for the needed job. Placing the transcoder at Site A is not required since the connections are already in G.711 format. It would be inefficient to transcode calls from site B to G.711 before sending them to the hub router, as the hub router will perform transcoding again before sending to the ITSP.

Therefore, the most efficient and logical approach is to have the hub router handle the G.729 to G.711 transcoding for Site B. This centralizes the transcoding and allows for optimal resource management.Cisco TranscodingCisco Router Voice Configuration

Question: 31

What are two key features of the Expressway series? (Choose two.)

A. IP to PSTN call connectivity
B. B2B calls
C. VPN connection toward the internal UC resources
D. SIP header modification
E. device registration over the Internet

Answer: BE

Explanation:

The correct answer is **B. B2B calls and E. device registration over the Internet.** Here's why:

Cisco Expressway is primarily designed as a gateway for enabling secure communication between different networks, particularly those beyond the internal network. One of its core functionalities is facilitating **B2B (Business-to-Business) calls (B)**. It allows for secure traversal of firewalls and Network Address Translation (NAT) to establish connections between different organizations' collaboration platforms, utilizing protocols like SIP. This is crucial for organizations needing to connect with external partners, customers, or other entities.

Furthermore, Expressway is vital for enabling **device registration over the internet (E)**. Without a secure gateway like Expressway, devices located outside the corporate network would struggle to register with on-premises Cisco Unified Communications Manager (CUCM) or other collaboration platforms. Expressway acts as a secure intermediary, allowing devices to establish a connection to these resources over the public internet, making remote and mobile access feasible and secure.

Let's look at why the other options are incorrect:

A. IP to PSTN call connectivity: While Cisco collaboration solutions can connect to the PSTN, this functionality is typically provided by other components such as a Cisco Unified Border Element (CUBE) or voice gateways. Expressway is not primarily responsible for this.

C. VPN connection toward the internal UC resources: Although VPNs can provide connectivity to internal UC resources, Expressway offers a more specialized and efficient approach tailored for real-time communications. It does not function as a general-purpose VPN gateway.

D. SIP header modification: While Expressway can perform some SIP header manipulation, this is not considered a core feature. Its primary role is routing, security, and NAT traversal for collaborative communications, not advanced SIP manipulation.

In essence, Expressway simplifies secure communication between internal networks and the internet or other external entities, focusing heavily on B2B communications and allowing devices outside the internal network to connect and register.

For further research and authoritative sources, refer to the following Cisco documentation:

Cisco Expressway Solution Overview:https://www.cisco.com/c/en/us/products/unified-communications/expressway/index.html
Cisco Expressway Deployment Guides:https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

Question: 32

When setting a new primary DNS server in the Cisco UCM CLI, what is required for the change to take effect?

A. restart of CallManager service
B. restart of DirSync service
C. restart of the network service
D. restart of TFTP service

Answer: C

Explanation:

The correct answer is C: restart of the network service. Modifying the primary DNS server on a Cisco Unified Communications Manager (CUCM) system directly affects the fundamental network configuration of the server. CUCM relies on DNS for resolving hostnames, which is crucial for inter-server communication,

directory synchronization, and accessing external services. Therefore, a change in the primary DNS server necessitates a restart of the network service to ensure the updated configuration is loaded and applied system-wide. This action ensures all network-dependent processes and services on the CUCM system begin using the new DNS server. Simply restarting services like CallManager, DirSync, or TFTP alone won't be sufficient because these services typically rely on the network stack for DNS resolution. The network service handles the core networking functionalities of the operating system, and thus a restart of the service will force it to re-initialize with the new DNS server information. A restart of the network service ensures consistency in DNS resolution across all applications running on the CUCM server.

For further research, refer to the official Cisco documentation regarding network settings configuration for CUCM:

Cisco Unified Communications Manager Configuration Guide (Navigate to the relevant version of CUCM) Cisco Unified Communications Manager System Administration Guide

Question: 33

When configuring Cisco UCM, which configuration enables phones to automatically reregister to a Cisco UCM publisher when the connection to the subscriber is lost?

A. SRST
B. Route Group
C. Device Pool
D. Cisco UCM Group

Answer: D

Explanation:

The correct answer is **D. Cisco UCM Group**.

Cisco UCM Groups are designed to provide redundancy and failover capabilities for Cisco IP phones. A Cisco UCM Group contains an ordered list of Cisco Unified Communications Manager (CUCM) servers, typically including a publisher and one or more subscribers. When a phone is configured to use a specific Cisco UCM Group, it initially registers with the highest priority server in that group (usually the publisher). If the connection to that server fails, the phone automatically attempts to register with the next available server in the list within the group. This process ensures that phones maintain connectivity and service in the event of server outages or network issues.

The Device Pool (C) is related but does not directly control failover within CUCM servers. While a Device Pool assigns devices to a specific cluster, it primarily influences features such as date/time groups, region settings, and softkey templates. Device Pools themselves rely on the assigned CUCM Group for failover behavior. SRST (A), or Survivable Remote Site Telephony, is a failover mechanism for branch sites where the connection to the central CUCM cluster is lost. While it also provides phone registration in a failure scenario, it's not used within the core CUCM cluster to switch between publisher and subscriber. Route Groups (B) are used for call routing decisions, not for phone registration management and failover. Therefore, the Cisco UCM Group configuration provides the mechanism for phones to automatically re-register to a publisher after a subscriber connection is lost.

Authoritative Links:

Cisco Collaboration System 14.0 SRND:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab14/collab14.html (Look for sections on CUCM Groups and redundancy)

Cisco Unified Communications Manager Configuration Guide:
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html (Select the appropriate version and find guides on System Configuration)

Question: 34

Which version is used to provide encryption for SNMP management traffic in collaboration deployments?

A. SNMPv2c
B. SNMPv2
C. SNMPv1
D. SNMPv3

Answer: D

Explanation:

The correct answer is D, SNMPv3. SNMP (Simple Network Management Protocol) is used for monitoring and managing network devices. SNMP versions differ significantly in security features. SNMPv1 and SNMPv2c (the community-based version) lack built-in encryption and authentication mechanisms, making them vulnerable to eavesdropping and unauthorized access. This means that sensitive management data, like configurations and operational parameters, is transmitted in clear text, posing a significant security risk.

SNMPv2 (although not a standard version) also lacks proper security features. In contrast, SNMPv3 introduces strong authentication (using usernames and passwords) and encryption using protocols like DES and AES. These mechanisms protect the confidentiality of management data and ensure the integrity of the messages, preventing unauthorized modifications. In modern collaboration deployments, such as Cisco's, where sensitive information about communication platforms is managed, using an insecure version of SNMP is unacceptable. Therefore, SNMPv3 is the standard version to secure management traffic and is typically mandated by best practices for cloud-based services and enterprise networking due to enhanced security mechanisms it offers compared to its predecessors. Thus, SNMPv3's support for encryption makes it the only valid option for securing SNMP traffic.https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/8258-snmp-security.htmlhttps://www.ibm.com/docs/en/zos/2.5.0?topic=protocols-snmp-versions

Question: 35

What is the validity period of the ITL Recovery certificate in Cisco UCM?

A. 1 year
B. 20 years
C. 5 years
D. 10 years

Answer: B

Explanation:

The correct answer is indeed B, 20 years. The ITL Recovery certificate within Cisco Unified Communications Manager (CUCM) possesses a long validity period specifically for recovery purposes. This certificate is not intended for regular operation but serves as a fallback mechanism when the standard ITL file becomes invalid

or unusable.

The ITL (Initial Trust List) is a crucial security component in Cisco collaboration environments. It contains certificates used to establish secure communication between CUCM servers, phones, and other endpoints. The ITL ensures devices only trust authorized CUCM servers.

However, in situations where the main ITL file gets corrupted or expires, devices would be unable to securely register with CUCM, causing a significant outage. The ITL Recovery certificate, with its significantly longer lifespan of 20 years, acts as a fail-safe. It's not intended for everyday use; instead, it's a backup to allow devices to re-establish trust if the main ITL is inaccessible. This recovery process might involve downloading a fresh ITL file, and the Recovery certificate facilitates that initial connection.

The 20-year lifespan minimizes the need to regenerate the ITL Recovery certificate frequently. This extended validity helps prevent future recovery scenarios from being blocked due to expired backup certificates.

Options A, C, and D, offering 1, 5, and 10 years respectively, would potentially require more frequent regeneration and present more complexity during a recovery situation. The key principle here is reliability and low maintenance during system recovery, hence the long 20-year term.

For further details, research "Cisco Unified Communications Manager Initial Trust List (ITL)" or related Cisco documentation. Look for documents specifically mentioning "ITL Recovery Certificate" and its validity duration.

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/12_5_1/cucm_b_security-guide-1251/cucm_b_security-guide-1251_chapter_0111.html#task_E1E0068576204E2C892819385819065Fhttps://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/guide-1201/cucm_b_security-guide-1201_chapter_0111.html

Question: 36

Which service must be enabled when LDAP on Cisco UCM is used?

A. Cisco Bulk Provisioning Service
B. Cisco AXL Web Service
C. Cisco CallManager SNMP Service
D. Cisco DirSync

Answer: D

Explanation:

The correct answer is D, Cisco DirSync. When Lightweight Directory Access Protocol (LDAP) is integrated with Cisco Unified Communications Manager (UCM), the Cisco DirSync service is crucial for synchronizing user data between the LDAP directory and UCM. This service facilitates the import and ongoing synchronization of user attributes, such as usernames, passwords, and contact information, from the LDAP directory into the UCM database. Without DirSync enabled, UCM would not be able to leverage the user data managed in the external LDAP system. DirSync ensures that user information remains consistent across both systems, simplifying user management and authentication processes. This avoids manually creating and updating user details directly in UCM. Options A, B, and C, while vital for other aspects of Cisco Collaboration, are not directly involved in the LDAP synchronization process. Cisco Bulk Provisioning Service is used for adding multiple devices, AXL handles API interaction, and SNMP service is for network management monitoring. DirSync specifically handles the directory integration, essential for enabling secure and consistent user data access and management. For further information, refer to the Cisco documentation on user synchronization: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1/systemConfig/cucm_b_system-

configuration-guide-1251/cucm_b_system-configuration-guide-1251_chapter_01000.html and https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1/systemConfig/cucm_b_system-configuration-guide-1251/cucm_b_system-configuration-guide-1251_chapter_01001.html

Question: 37

On a Cisco Catalyst Switch, which command is required to send CDP packets on a switch port that configures a Cisco IP phone to transmit voice traffic in 802.1Q frames, tagged with the voice VLAN ID 221?

A. Device(config-if)# switchport trunk allowed vlan 221
B. Device(config-if)# switchport vlan voice 221
C. Device(config-if)# switchport voice vlan 221
D. Device(config-if)# switchport access vlan 221

Answer: C

Explanation:

The correct command is switchport voice vlan 221. Here's why:

Cisco Discovery Protocol (CDP) is used by Cisco devices to share information about their neighbors, including voice VLAN configurations. To configure a port to support voice VLAN traffic, the switchport voice vlan command is essential. This command instructs the switch to send CDP messages to the connected IP phone, informing the phone to tag voice traffic with VLAN ID 221.

Option A, switchport trunk allowed vlan 221, is used to allow VLAN 221 on a trunk link, not specifically for voice VLAN configuration on an access port connecting to an IP phone. Option B, switchport vlan voice 221, is not a valid command. Option D, switchport access vlan 221, sets the data VLAN for an access port, not the voice VLAN.

The switchport voice vlan command is crucial for enabling QoS and prioritization of voice traffic, ensuring high-quality voice communication. It does this through the CDP advertisement, allowing a Cisco IP phone to dynamically use VLAN 221 for its voice traffic. This also enables the switch to treat voice traffic differently than regular data traffic, providing better performance. The access port can also simultaneously support data traffic using its default or manually configured data VLAN. In summary, the switchport voice vlan command is designed explicitly for configuring voice VLAN support on switch ports for Cisco IP phones.

For further reading and verification, please refer to Cisco's official documentation on configuring voice VLANs:

Cisco Switch Configuration Guide

Configuring Voice VLANs

Question: 38

Which datastore and protocol is used for saving back-up files within the Disaster Recovery System of Cisco UCM?

A. local disk on the Cisco UCM server
B. remote disk on the SFTP server
C. remote disk on a CIFS share
D. remote disk on an NFS share

Answer: B

Explanation:

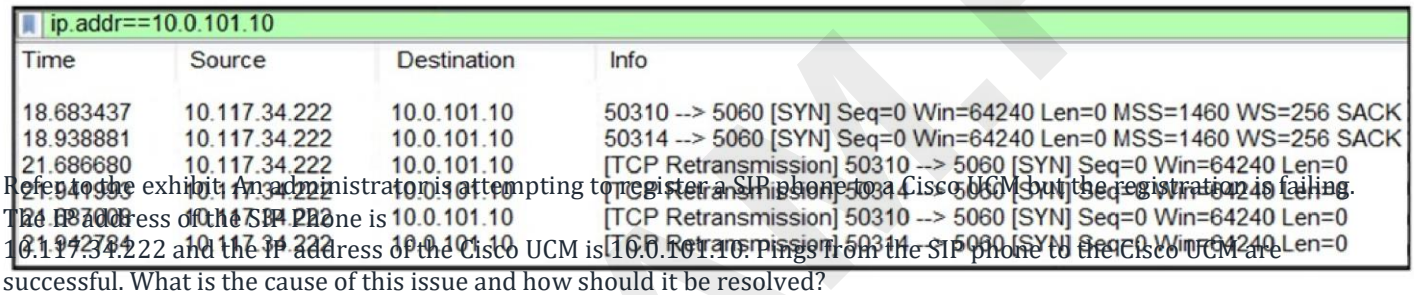
The correct answer is B, remote disk on the SFTP server. Cisco Unified Communications Manager (CUCM) Disaster Recovery System (DRS) utilizes Secure File Transfer Protocol (SFTP) as its primary protocol for backing up data to a remote location. This design is crucial for disaster recovery, ensuring that backups are not stored on the same device as the primary CUCM instance, mitigating data loss in case of hardware failure. CUCM doesn't directly employ local storage for DRS backups to avoid single points of failure. While CIFS and NFS shares can be used for other purposes within the CUCM system, they aren't the intended storage for DRS backups. SFTP provides a secure and encrypted channel for transferring backup files, which is essential for maintaining the confidentiality and integrity of sensitive CUCM data. Moreover, SFTP allows for
authentication and authorization, further securing the backup process. This method ensures that backups are stored in a separate, controlled, and secure location, vital for reliable recovery operations during a disaster.

Storing backups remotely, especially via SFTP, aligns with cloud computing concepts of redundancy and offsite backup, protecting against localized failures. This strategy ensures business continuity by enabling CUCM to be restored from backups located in a different server if needed.

Authoritative links:

1. Cisco Unified Communications Manager Administration Guide: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html (Look for specific version guides and search for "Disaster Recovery System" or "Backup and Restore").
2. Cisco Documentation on SFTP: https://www.cisco.com/c/en/us/support/docs/security/secure-shell-ssh/200801-configure-sftp-on-cisco-devices.html

Question: 39



Refer to the exhibit. An administrator is attempting to register a SIP phone to a Cisco UCM but the registration is failing. The IP address of the SIP phone is 10.117.34.222 and the IP address of the Cisco UCM is 10.0.101.10. Pings from the SIP phone to the Cisco UCM are successful. What is the cause of this issue and how should it be resolved?

A. An NTP mismatch is preventing the connection of the TCP session between the SIP phone and the Cisco UCM. The SIP phone and Cisco UCM must be set with identical NTP sources.

B. The certificates on the SIP phone are not trusted by the Cisco UCM. The SIP phone must generate new certificates.

C. DNS lookup for the Cisco UCM FQDN is failing. The SIP phone must be reconfigured with the proper DNS server.

D. A network device is blocking TCP port 5060 from the SIP phone to the Cisco UCM. This device must be reconfigured to allow traffic from the IP phone.

Answer: D

Explanation:

A network device is blocking TCP port 5060 from the SIP phone to the Cisco UCM. This device must be reconfigured to allow traffic from the IP phone.

Question: 40

```
voice class dpg 2000
 dial-peer 2001 preference 1
 dial-peer 2002 preference 2
 dial-peer 2003 preference 3

dial-peer voice 1001 voip
 description INBOUND
 session protocol sipv2
 session target ipv4:10.0.0.1
 destination dpg 2000
 incoming called-number 5T

dial-peer voice 2001 voip
 destination-pattern 5506
 session protocol sipv2
 session target ipv4:10.0.0.2

dial-peer voice 2002 voip
 destination-pattern 55..
 session protocol sipv2
 session target ipv4:10.0.0.3

dial-peer voice 2003 voip
 destination-pattern 5507
 session protocol sipv2
 session target ipv4:10.0.0.4
```

Refer to the exhibit. A Cisco UCM user with directory number 4401 dials 5507, and the call is routed to a Cisco Unified Border Element. Which IP address will the call be sent to?

A. 10.0.0.2
B. 10.0.0.3
C. 10.0.0.4
D. 10.0.0.1

Answer: A

Explanation:

A, voice class dpg Completely ignores destination-pattern configured in the dial-peer section and follows preference.

The example in this document is similar to the test question.https://www.cisco.com/c/en/us/support/docs/voice/ip-telephony-voice-over-ip-voip/211306-In-

Depth-Explanation-of-Cisco-IOS-and-IO.html#anc23

Question: 41

Configuration of DNS is required to achieve a fully functional Cisco UCM system. Cisco UCM uses DNS to resolve fully qualified domain names to IP addresses for which destinations?

A. MRA
B. trunk
C. AAR
D. H.323

Answer: B

Explanation:

The correct answer is **B. trunk**.

Here's a detailed justification:

Cisco Unified Communications Manager (UCM) relies on DNS for several critical functions. One essential use is resolving the fully qualified domain names (FQDNs) of SIP trunks to their corresponding IP addresses. This is crucial for establishing and maintaining communication with external systems or other UCM clusters. When a call is routed over a trunk, UCM needs to know where to send the signaling messages. DNS provides the lookup mechanism to map the symbolic trunk address (e.g., sip.provider.com) to the actual IP address of the trunk endpoint. This process ensures seamless connectivity and proper routing of voice and video calls.

While other elements like MRA (Mobile and Remote Access), AAR (Automated Alternate Routing) and H.323 are also components of a communication system, they don't inherently rely on DNS for resolution of the destination during their core function. MRA relies on other mechanisms for communication outside network.

AAR determines call routing based on criteria not associated with resolving FQDNs. H.323 can use IP addresses directly and does not strictly require DNS resolution for its destination during its core function. Trunks, however, often utilise FQDNs for their SIP addressing, making DNS lookups a necessity for connection establishment. Therefore, the most direct and fundamental use of DNS in the context of Cisco UCM destination resolution is for trunk endpoints. Without proper DNS configuration, UCM would be unable to locate the trunk endpoints, hindering inter-system and external communication. This highlights the
significance of DNS within a functional UCM deployment.

Authoritative links for further research:

Cisco Unified Communications Manager Configuration Guides: These documents detail the intricacies of DNS configuration for UCM. Search for "DNS configuration" within relevant Cisco UCM documentation on Cisco.com
Cisco Validated Design Guides: These documents often explain the role of DNS in larger Cisco collaboration deployments, especially regarding trunks. Search for "Cisco collaboration SRND" on Cisco.com.

SIP Trunking Documentation: SIP providers' documentation often outlines the DNS requirements for their services.

The key is understanding that while other components utilize networking and name resolution, the direct requirement for DNS to resolve the destination for routing in UCM is most critical for SIP trunks.

Question: 42

```
Sent:
INVITE sip:2004@192.168.100.100:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.100.200:5060;branch=z9hG4bKF1FED
From: "7000" <sip:7000@192.168.100.200>;tag=43CDE-1A22
To: <sip:2004@192.168.100.100>
Call-ID: 12BCA00-3C3E11EA-01234567@192.168.100.200
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Min-SE: 1800
User-Agent: Cisco-SIPGateway/IOS-16.9.5
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Contact: <sip:7000@192.168.100.200:5060>
Expires: 180
Max-Forwards: 68
P-Asserted-Identity: "7000" <sip:7000@192.168.100.200>
Session-Expires: 1800
Content-Type: application/sdp
Content-Length: 254

v=0
o=CiscoSystemsSIP-GW-UserAgent 5871 9974 IN IP4 192.168.100.200
s=SIP Call
c=IN IP4 192.168.100.200
t=0 0
m=audio 8002 RTP/SAVP 0
c=IN IP4 192.168.100.200
a=rtpmap:0 PCMU/8000
a=ptime:20
```

Refer to the exhibit. Calls to Cisco Unity Connection are failing across Cisco Unified Border Element when callers try to select a menu prompt. Why is this happening and how is it fixed?

A. Cisco Unified Border Element is sending the incorrect media IP address. The IP address of the loopback interface must be advertised in the SDP.

B. Cisco Unity Connection is configured on G.729 only. Cisco Unity Connection must be reconfigured to support iLBC.

C. Cisco Unified Border Element is not sending any support for DTMF. DTMF configuration must be added to the appropriate dial peer.

D. The Cisco Unity Connection Call Handler is configured for a Release to Switch transfer type. Transfers must be disabled for the Cisco Unity Connection Call Handler.

Answer: C

Explanation:

Cisco Unified Border Element is not sending any support for DTMF. DTMF configuration must be added to the appropriate dial peer.

Question: 43

An administrator is configuring LDAP for Cisco UCM with Active Directory integration. A customer has requested to use `ipphone` instead of `telephoneNumber' as the phone number attribute. Where does the administrator specify this attribute mapping in Cisco UCM?

A. LDAP Custom Filter

B. LDAP Authentication

C. LDAP Directory user fields

D. LDAP Directory custom user fields

Answer: C

Explanation:

The correct answer is **C. LDAP Directory user fields**. This is because Cisco UCM (Unified Communications Manager) utilizes the "LDAP Directory user fields" configuration section to define how attributes from Active Directory (or another LDAP directory) map to user fields within Cisco UCM. These mappings determine which attributes, such as phone numbers, are retrieved and stored for users in UCM. When a user requests ipphone instead of telephoneNumber, the administrator modifies the corresponding UCM field mapping to reflect this. Specifically, the "Phone Number" field in the "LDAP Directory User Fields" would be changed to map to the ipphone attribute in the LDAP directory instead of the default telephoneNumber.

Option A, "LDAP Custom Filter," is used to specify search criteria when querying the LDAP directory for users, not for defining how the retrieved attributes map to UCM fields. Option B, "LDAP Authentication," focuses on how users are authenticated against the LDAP directory, not on the attribute mapping for users. Option D, "LDAP Directory custom user fields", is incorrect because user fields can be edited or created under the "LDAP Directory user fields", but not in "LDAP Directory custom user fields".

The process of mapping LDAP attributes to UCM fields is critical for correct user information synchronization between the directory and UCM, and for enabling features like click-to-dial. Therefore, the "LDAP Directory user fields" section provides the specific interface for achieving this, and changing mapping from telephoneNumber to ipphone. This aligns with common directory integration practices in unified communications platforms where admins customize attribute mapping to adapt to variations in directory schemas.

Here are some authoritative links for further research:

Cisco Unified Communications Manager Configuration Guide, Release 14.0 - Chapter: Configure LDAP Directory: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/config/14/b_cucm_config_guide_14/b_cucm_config_ (This documentation details the configuration of LDAP directories in CUCM, including the user field mapping section.)
Cisco Unified Communications Manager Administration Guide, Release 14.0 - Chapter: Add an LDAP Directory: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/14_0_1/cucm_b_admin-guide-1401/cucm_b_admin-guide-1401_chapter_010000.html (This link has the specific procedure for setting up the LDAP Directory and user mapping.)

Question: 44

In the Cisco Expressway solution, which two features does Mobile and Remote Access provide? (Choose two.)

A. VPN-based enterprise access for a subnet of Cisco Unified IP Phone models
B. secure reverse proxy firewall traversal connectivity
C. the ability of Cisco IP Phones to access the enterprise through VPN connection
D. the ability to register third-party SIP or H.323 devices on Cisco UCM without requiring VPN
E. the ability for remote users and their devices to access and consume enterprise collaboration applications and services

Answer: BE

Explanation:

Here's a breakdown of why options B and E are correct for the Mobile and Remote Access (MRA) feature in Cisco Expressway, along with explanations of why the others are incorrect.

Justification:

Option B: secure reverse proxy firewall traversal connectivity: This is a core function of MRA. Expressway acts as a secure reverse proxy, enabling devices outside the corporate network to connect to on-premises collaboration services like Cisco Unified Communications Manager (CUCM) and Cisco Webex without needing a direct VPN connection to the internal network. The Expressway Edge handles the external communication, while the Expressway Core sits inside the firewall and communicates with the internal collaboration services.

This ensures that sensitive internal resources are not directly exposed to the public internet. Cisco Expressway Deployment Guide describes the general deployment and firewall traversal.

Option E: the ability for remote users and their devices to access and consume enterprise collaboration applications and services: This accurately describes the primary goal of MRA. It allows users located outside of the office environment to seamlessly access applications and services such as calling, messaging, and video conferencing, just as if they were on the internal network. This access extends to various devices such as mobile phones, tablets, and laptops using compatible Cisco applications. MRA makes location transparent to the user, ensuring a consistent experience.

Why the other options are incorrect:

Option A: VPN-based enterprise access for a subnet of Cisco Unified IP Phone models: MRA is explicitly designed to avoid the need for traditional VPNs for most use cases, especially for Cisco endpoint devices. It uses secure connections over TLS for remote access. While some phone models can use VPNs, this is not the central feature or purpose of MRA.

Option C: the ability of Cisco IP Phones to access the enterprise through VPN connection: Similar to Option A, while some phone models can work with VPN, MRA's primary intent is to remove the need for VPN for most Cisco endpoint registrations. MRA streamlines the connection process with secure HTTP protocols over TLS.

Option D: the ability to register third-party SIP or H.323 devices on Cisco UCM without requiring VPN: While Expressway does support third-party device registration, this is not specific to or a defining feature of MRA functionality. Furthermore, MRA typically involves secure Cisco endpoints using Secure Call Control, and generally requires specific configurations that ensure compatibility with Cisco infrastructure.

In summary: MRA provides a secure, firewall-friendly alternative to VPNs, allowing remote devices to access internal collaboration services seamlessly by leveraging the reverse proxy capabilities of Cisco Expressway. The key goals are to enable a consistent, secure user experience, regardless of location, without requiring direct network access.

Question: 45

What makes Cisco Unified Border Element a better choice than a conventional Session Border Controller?

A. DTMF interworking
B. SIP security
C. Voice policy
D. Address hiding

Answer: C

Explanation:

The correct answer is **C. Voice policy**. Cisco Unified Border Element (CUBE) is indeed a type of Session Border Controller (SBC), but the question asks what makes it better than a conventional SBC. While options A, B, and D are functionalities found in many SBCs, CUBE's strength lies in its advanced voice policy control.

Here's why:

Conventional SBCs often focus on basic functionalities like NAT traversal, SIP normalization, and security. CUBE goes further, offering granular control over call routing, bandwidth management, and codec selection based on predefined policies. This policy engine, often incorporating sophisticated regular expression matching, allows for complex call management scenarios. For example, you could configure CUBE to route calls to certain destinations based on the calling number, time of day, or even the specific SIP header content.

This level of flexibility allows for highly optimized communication flows and cost savings. Standard SBCs typically lack this level of advanced customization and require more manual intervention for specific scenarios. CUBE's robust voice policy engine provides a strategic advantage in managing complex collaboration environments.

Further research:

Cisco CUBE documentation: https://www.cisco.com/c/en/us/products/unified-communications/unified-border-element-cube/index.html
Understanding Session Border Controllers: https://www.sangoma.com/blog/what-is-a-session-border-controller/

Question: 46

Which two features of Cisco Prime Collaboration Assurance require advanced licensing? (Choose two.)

A. customizable events
B. email notifications
C. multicluster support
D. real time alarm browser
E. call quality monitoring

Answer: CE

Explanation:

The correct answer is C (multicluster support) and E (call quality monitoring) because these functionalities in Cisco Prime Collaboration Assurance are not included in the base license and require an upgrade to an advanced license. Multicluster support allows for the monitoring and management of multiple Cisco collaboration deployments from a single pane of glass, which is a complex feature usually reserved for larger, more sophisticated environments that necessitate additional licensing. Similarly, call quality monitoring provides detailed insights into the quality of voice and video calls by analyzing metrics like jitter, packet loss, and latency. This feature is advanced because it involves in-depth data collection and analysis. Basic functionality, like email notifications (B) and the real-time alarm browser (D), are typically part of the base license. Customizable events (A) may have certain limitations in the base version, but the full extent of this functionality is usually available without needing an advanced license. Therefore, based on licensing models and feature tiers, multicluster support and call quality monitoring necessitate advanced licensing.

Here are some authoritative links to support this information:

Cisco Prime Collaboration Assurance Ordering Guide: This document typically outlines the different licensing tiers and what features are included in each. You'd need to navigate to the latest version specific to the Cisco product line. While specific links can change, you can often find these documents by searching on Cisco's website for "Cisco Prime Collaboration Assurance Ordering Guide."
Cisco Prime Collaboration Assurance Documentation: Explore the official Cisco documentation for your specific version of Prime Collaboration Assurance; it will usually describe licensing implications for feature access. Look for sections on licensing or deployment.

Cisco Partners or Sales Representatives: Contacting Cisco sales or partners can provide definitive answers on licensing details.

These resources will detail the specific features available within the base license and the ones that require advanced licenses.

Question: 47

Which entity does Cisco UCM use DNS to resolve fully qualified domain names to an IP address?

A. application server name
B. SIP trunk
C. Cisco UCM Name
D. primary TFTP server for option 150

Answer: B

Explanation:

The correct answer is B. SIP trunk. Cisco Unified Communications Manager (UCM) relies on DNS to resolve the fully qualified domain names (FQDNs) of SIP trunks to their corresponding IP addresses. This is crucial for establishing communication pathways with external VoIP providers or other systems that support SIP. When a call is initiated involving a SIP trunk, UCM needs to know where to send the signaling messages. DNS helps achieve this by translating the easily recognizable FQDN of the SIP trunk into the numerical IP address that is used for network routing. Options A, C, and D involve local UCM components, application names, or the TFTP server. While DNS might be used in their context, it's not as directly involved in call path establishment compared to SIP trunks. The SIP trunk's dependency on DNS for FQDN resolution is a core function in SIP-based VoIP implementations as it ensures dynamic IP changes to remote entities do not disrupt connectivity, offering a more flexible and robust communication environment. The primary purpose of DNS within the context of SIP trunking is to enable the discovery of the remote end-point without the need for hard-coded IP addresses.

Further research:

Cisco Unified Communications Manager System Guide: (Search for "DNS" and "SIP Trunk")
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html
Understanding DNS:https://www.cloudflare.com/learning/dns/what-is-dns/
SIP Trunking Basics:https://www.ringcentral.com/gb/en/blog/sip-trunking-basics.html

Question: 48

What are two functions of Cisco Expressway in the Collaboration Edge? (Choose two.)

A. Expressway-C provides encryption for Mobile and Remote Access but not for business-to-business communications.
B. Expressway-E provides a VPN entry point for Cisco IP phones with a Cisco AnyConnect client using authentication based on certificates.
C. Expressway-E provides a perimeter network that separates the enterprise network from the Internet.
D. The Expressway-C and Expressway-E pair can interconnect H.323-to-SIP calls for voice.
E. The Expressway-C and Expressway-E pair can enable connectivity from the corporate network to the PSTN via a T1/E1 trunk.

Answer: CD

Explanation:

The correct answer is CD. Cisco Expressway, functioning as a core component in Cisco's Collaboration Edge architecture, handles crucial functions related to secure communication. Expressway-E, situated in the DMZ (demilitarized zone), acts as a secure gateway between the enterprise network and external networks like the Internet. This fulfills the role stated in option C, providing a critical perimeter defense. Expressway-C, usually located within the internal network, manages internal call control and integrates with other Cisco
collaboration components. These two components work in tandem to enable functionalities, with interconnections between them supporting functionalities like H.323-to-SIP translation. This is essential for enabling compatibility between various communication protocols (option D).

Option A is incorrect as Expressway-E provides encryption for both MRA and B2B calls. Option B is also wrong because while Cisco AnyConnect clients can use the Expressway, it's not the VPN entry point for IP phones; phones typically connect using MRA. Finally, option E is not accurate. While Expressway allows
interconnections for VoIP calls, it doesn't directly provide connectivity to the PSTN over T1/E1, as a voice gateway like a Cisco VG would. It facilitates routing calls to the voice gateway over the IP network.

For further research, refer to Cisco's official documentation:

Cisco Expressway Administrator Guide
Cisco Collaboration System SRNDThese links will provide in-depth explanations of Cisco Expressway functionality and deployments.

Question: 49

NAME	TTL	CLASS	TYPE	Priority	Weight	Port	Target Address
_sip._tcp.sample.com	86400	IN	SRV	10	60	5060	server1.sample.com
_sip._tcp.sample.com	86400	IN	SRV	10	30	5060	server2.sample.com
_sip._tcp.sample.com	86400	IN	SRV	5	20	5060	server3.sample.com

Refer to the exhibit. An administrator must fix the SRV records to ensure that server1.sample.com is always contacted first from the three servers. Which solution should the engineer apply to resolve this issue?

A. Priority = 5, Weight = 70
B. Priority = 10, Weight = 5
C. Priority = 100, Weight = 90
D. Priority = 10, Weight = 10

Answer: A

Explanation:

Priority checked first. Lower value priority is More Preffered. If there's a tie in priority, higher value weight is More Preffered. So answer is A.

Question: 50

What are two differences between media flow-around and media flow-through on Cisco Unified Border Element? (Choose two.)

A. When using media flow-through, the call signaling and media are passed through the Cisco Unified Border Element.

B. When using media flow-through, call signaling goes through the Cisco Unified Border Element, but media does not.

C. When using media flow-around, both call signaling and media do not go through the Cisco Unified Border Element.

D. When using media flow-around, the call signaling goes through the Cisco Unified Border Element, but media is not passed through it.

E. When using media flow-through, the call signaling goes through the Cisco Unified Border Element, but media is not passed through it.

Answer: AD

Explanation:

Here's a detailed justification for why options A and D are the correct differences between media flow-around and media flow-through on a Cisco Unified Border Element (CUBE):

Media Flow-Through: In this model, both the call signaling (SIP, H.323) and the actual media streams (RTP) traverse the CUBE device. The CUBE actively participates in the media path, potentially performing functions like transcoding, quality of service (QoS) marking, and Network Address Translation (NAT) traversal. This is analogous to a proxy server actively processing all traffic. Option A accurately describes this behavior, stating that both signaling and media pass through the CUBE.

Media Flow-Around: Conversely, with media flow-around, the CUBE only handles call signaling. After the initial signaling negotiation (e.g., SIP invite), the media streams (RTP) are directly established between the endpoints, bypassing the CUBE. The CUBE essentially acts as a signaling back-to-back user agent (B2BUA), connecting calls but not directly involved in the media relay. Option D correctly represents this concept, explaining that while call signaling passes through the CUBE, media bypasses it. This can reduce the processing load on the CUBE itself.

Options B, C, and E are incorrect because they misrepresent how signaling and media flow in each scenario. Option B inaccurately states media doesn't pass through CUBE in flow-through. Option C incorrectly claims that neither signaling nor media go through the CUBE in flow-around, and option E is essentially a repeat of option B.

In summary, the key distinction lies in whether the media stream passes through the CUBE. Flow-through involves the CUBE in both signaling and media paths, whereas flow-around uses the CUBE solely for signaling, letting the media flow directly between endpoints.

Authoritative Links for Further Research:

Cisco Unified Border Element Configuration Guide: [Search Cisco's website for "CUBE configuration guide" for specific versions] This documentation provides detailed information on configuring and understanding CUBE functionalities, including media flow options.

Cisco Collaboration System Design Guide: [Search Cisco's website for "Collaboration System Design Guide"] This guide offers high-level design information on various collaboration deployments and explains CUBE's role, and best practice in different scenarios.

IETF RFC 3261 (SIP): [https://datatracker.ietf.org/doc/html/rfc3261] While this RFC is focused on SIP, it is helpful to understand the underlying signaling that CUBE uses.

IETF RFC 3550 (RTP): [https://datatracker.ietf.org/doc/html/rfc3550] This RFC provides details on RTP, the protocol used for media transport.

Question: 51

An employee of company ABC just quit. The IT administrator deleted the employee's user ID from the active directory at 10 a.m. on March 4
. The nightly sync
th
occurs at 10 p.m. daily. The IT administrator wants to troubleshoot and find a way to delete the user ID as soon as possible. How is this issue resolved?

A. Wait until 3:15 a.m. on March 6 for garbage collection to remove the user from Cisco UCM. th
B. Wait until 10 p.m. on March 5 when the user is automatically removed from Cisco UCM. th
C. Wait until 10 p.m. on March 4 when the user is automatically removed from Cisco UCM. th
D. Wait until 3:15 a.m. on March 5 for garbage collection to remove the user from Cisco UCM. th

Answer: A

Explanation:

The correct answer is **A. Wait until 3:15 a.m. on March 6 for garbage collection to remove the user from Cisco UCM.**

Here's why:

Cisco Unified Communications Manager (UCM) relies on directory synchronization (sync) with Active Directory (AD) to maintain user information. When a user is removed from AD, UCM doesn't immediately reflect this change. Instead, it relies on a scheduled synchronization process, typically nightly, to update its user database. However, the removal process also involves garbage collection.

While the nightly sync will initially mark the user as inactive within UCM (after the 10 p.m. sync on March 4th), the complete removal of the user requires the garbage collection process. This garbage collection typically runs during the maintenance window, which is usually set for early morning hours. The question specifies no other maintenance window configuration, and most installations rely on the Cisco default maintenance schedule. This typically occurs in the very early morning hours around 3:15 AM local time.

According to Cisco's documentation, while the initial sync will mark the user for deletion, the actual deletion process through garbage collection will occur sometime after this initial marking, depending on the maintenance window setup. Typically garbage collection runs on the second day after the user was marked as inactive, therefore it would be March 6. This two day delay helps ensure that any related data (messages, voicemails, configuration entries etc.) are all cleaned up.

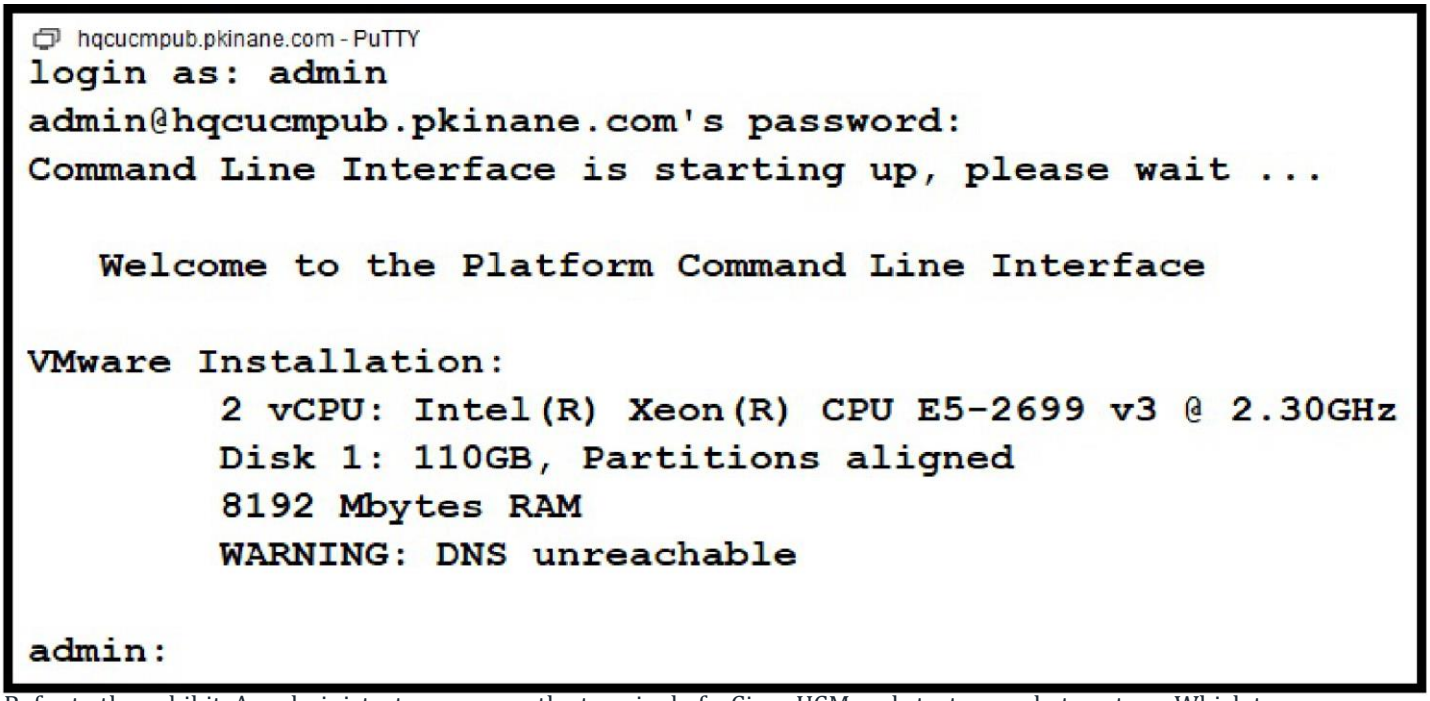
Option B is incorrect because the user is not fully removed at that time, merely marked for removal. Options C and D are incorrect for the same reason, as they are referring to the initial sync rather than the garbage collection process, and D is not the correct scheduled garbage collection time.

Therefore, the most accurate solution is to wait for the garbage collection process, which is expected to run around 3:15 am on March 6th, for the user to be fully removed from Cisco UCM.

Authoritative Links:

Cisco Unified Communications Manager Administration Guide: While a specific page cannot be linked directly, searching within the admin guide for "directory synchronization" and "garbage collection" will provide detailed information on the processes described. The key terms will be in sections relating to user management, directory integration, and maintenance.

Question: 52



Refer to the exhibit. An administrator accesses the terminal of a Cisco UCM and starts a packet capture. Which two commands must the administrator use on
Cisco UCM to generate DNS traffic? (Choose two.)

A. show version active
B. utils diagnose module validate_network
C. utils diagnose test
D. utils ntp status
E. show cdp neighbor

Answer: BC

Explanation:

Reference:
https://ccxguru.wordpress.com/2018/02/03/behind-the-utils-diagnose-test/

Question: 53

A collaboration engineer adds a voice gateway to Cisco UCM. The engineer creates a new gateway device in Cisco UCM, selects VG320 as the device type, and selects MGCP as the protocol. What must be done next to add the gateway to the Cisco UCM database?

A. Select a device pool for the new gateway.
B. Add the FQDN or hostname of the device.
C. Configure the module in slot 0 of the new gateway.
D. Select the DTMF relay type for the gateway.

Answer: B

Explanation:

The correct answer is **B. Add the FQDN or hostname of the device.** Here's why: When adding a gateway to Cisco Unified Communications Manager (UCM), particularly using MGCP (Media Gateway Control Protocol), UCM needs a way to uniquely identify and communicate with the physical gateway device. This identification is achieved primarily through its hostname or Fully Qualified Domain Name (FQDN). Selecting the device type

(VG320) and the protocol (MGCP) are essential initial steps that define the device's characteristics and the communication method. However, UCM still doesn't know which specific gateway to interact with. The device pool (option A) is important for configuration grouping and applying common settings, but it's a later step.

Configuring a module in a specific slot (option C) is related to the physical hardware configuration but not a prerequisite for UCM database registration. Selecting a DTMF relay type (option D) is essential for specific call handling functionality, which will be configured after the device is registered. Therefore, UCM first needs the FQDN or hostname of the gateway. This hostname/FQDN is used to establish communication channels between UCM and the MGCP gateway through TCP/IP on port 2427, allowing them to exchange signaling messages for call control. Without this, the gateway is an undefined entity, and UCM won't be able to communicate with the physical hardware or manage its endpoints. Adding the FQDN or hostname establishes a valid endpoint address for UCM to register the gateway within the database, making it an essential prerequisite before all other configuration steps.

Authoritative Links:

Cisco Unified Communications Manager Configuration Guide for Cisco Unified CallManager (MGCP): This official Cisco guide provides detailed steps on configuring MGCP gateways within UCM, highlighting the importance of hostname/FQDN configuration during the initial gateway creation. You can find the specific guide based on the version of UCM you're using on the Cisco website by searching "Cisco Unified Communications Manager Configuration Guide MGCP".

Cisco Documentation for MGCP: Search the Cisco documentation portal for articles on MGCP gateway configuration. This would provide more details on MGCP protocol and its interactions within UCM.

Question: 54

A collaboration engineer configures Global Dial Plan Replication for multiple Cisco UCM clusters. The local cluster acts as the hub cluster, and the remaining clusters act as spoke clusters. Which service must the engineer configure on the local cluster?

A. Location Conveyance on intercluster SIP trunks
B. Intercluster Lookup Service
C. Intra-Cluster Communication Signaling
D. Mobility Cross Cluster

Answer: B

Explanation:

The correct answer is **B. Intercluster Lookup Service**.

Global Dial Plan Replication (GDPR) in Cisco Unified Communications Manager (CUCM) involves synchronizing dial plan information across multiple CUCM clusters. This allows for seamless call routing and feature access across the entire deployment, regardless of which cluster a user resides in. The hub cluster, designated as the central point for dial plan management, requires specific services to facilitate GDPR.

The **Intercluster Lookup Service (ILS)** is crucial for GDPR because it is the service responsible for exchanging and maintaining dial plan information between clusters. The hub cluster acts as the primary source for this information. When a spoke cluster needs to route a call, it queries the hub cluster via ILS to determine the correct routing path based on the global dial plan. The hub cluster broadcasts dial plan updates to all registered spoke clusters via ILS. Without the ILS on the hub, spoke clusters cannot retrieve dial plan data, resulting in call routing failures between clusters. Options A, C, and D are either not directly related to GDPR's mechanism or perform functions beyond its specific purview. Location Conveyance is about passing location information in SIP signaling; Intra-Cluster Communication Signaling concerns internal CUCM communication, and Mobility Cross Cluster deals with user mobility between clusters, not dial plan replication.

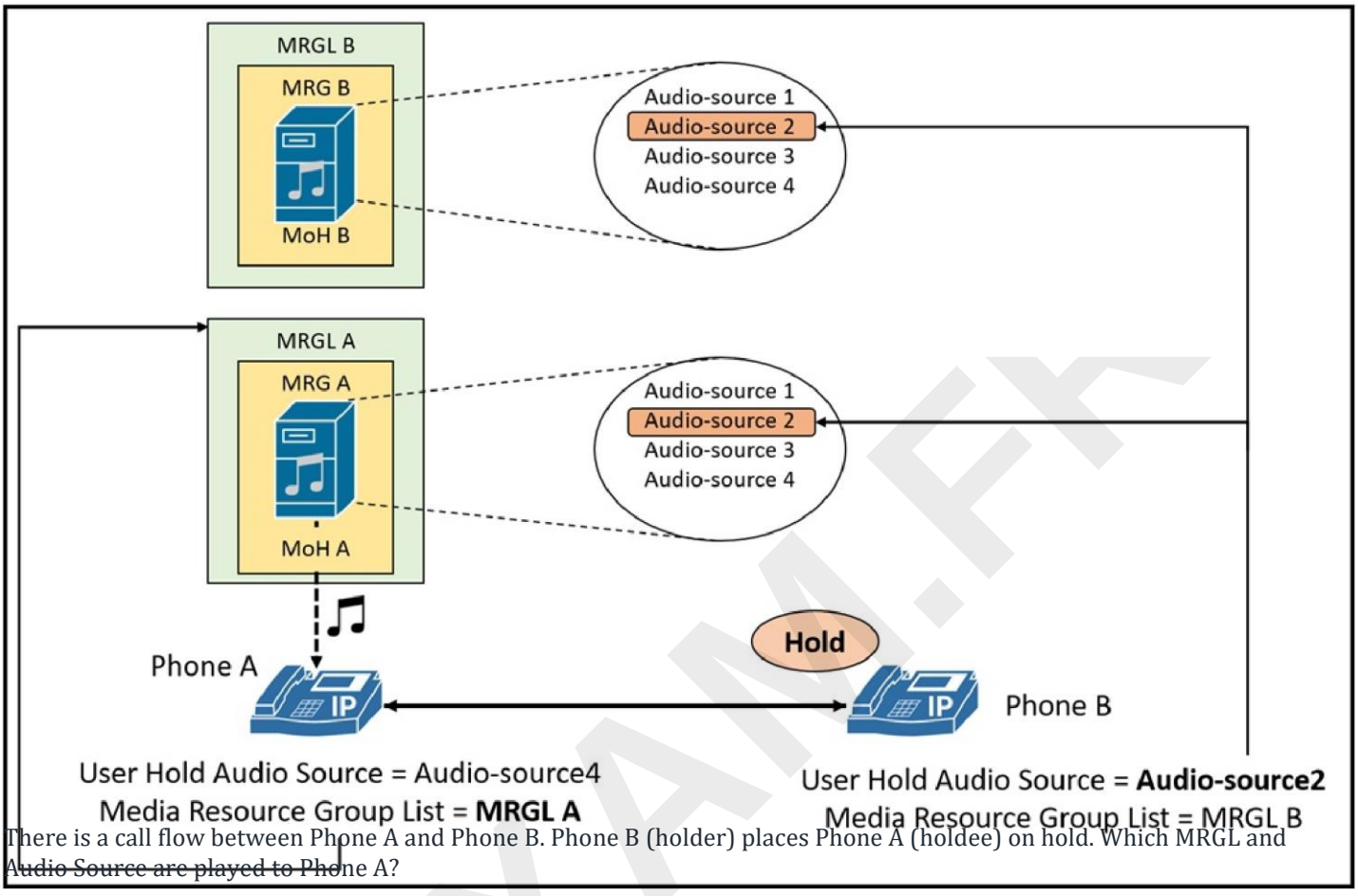
Therefore, configuring the Intercluster Lookup Service on the local (hub) cluster is paramount for successful Global Dial Plan Replication, enabling the distribution and application of a unified dial plan across multiple Cisco UCM deployments.

Authoritative links for further research:

Cisco Collaboration System Solution Reference Network Designs (SRND) documentation:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html (Search for "Intercluster Lookup Service")
Cisco Unified Communications Manager Configuration Guides:
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html (Refer to the guide for your specific CUCM version and search for "Global Dial Plan Replication")

Question: 55

Refer to the exhibit.



There is a call flow between Phone A and Phone B. Phone B (holder) places Phone A (holdee) on hold. Which MRGL and Audio Source are played to Phone A?

A. MRGL A and Audio Source 4
B. MRGL B and Audio Source 2
C. MRGL B and Audio Source 4
D. MRGL A and Audio Source 2

Answer: D

Explanation:

In simplest terms, the holder's configuration determines which audio file to play, and the holdee's

configuration determines which resource or server will play that file. As illustrated by the example in Figure 18-1, if phones A and B are on a call and phone B (holder) places phone A (holdee) on hold, phone A will hear the MoH audio source configured for phone B (Audio-source2). However, phone A will receive this MoH audio stream from the MRGL (resource or server) configured for phone A (MRGL A).https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/8x/moh.html#wp1092723

D is correct - if phones A and B are on a call and phone B (holder) places phone A (holdee) on hold, phone A will hear the MoH audio source configured for phone B (Audio-source2). However, phone A will receive this MoH audio stream from the MRGL (resource or server) configured for phone A (MRGL A).

Question: 56

A SIP phone has been configured in the system with MAC address 0030.96D2.D5CB. The phone retrieves the configuration file from the Cisco UCM. Which naming format is the file that is downloaded?

A. SEP0030407101980.cnf
B. SIP0030407101980.cnf
C. SIP003096D2D5CB.cnf.xml
D. SEP003096D2D5CB.cnf.xml

Answer: B

Explanation:

Here's a detailed justification for why the correct answer is **B. SIP0030407101980.cnf**, when a SIP phone with MAC address 0030.96D2.D5CB downloads its configuration file from Cisco UCM.

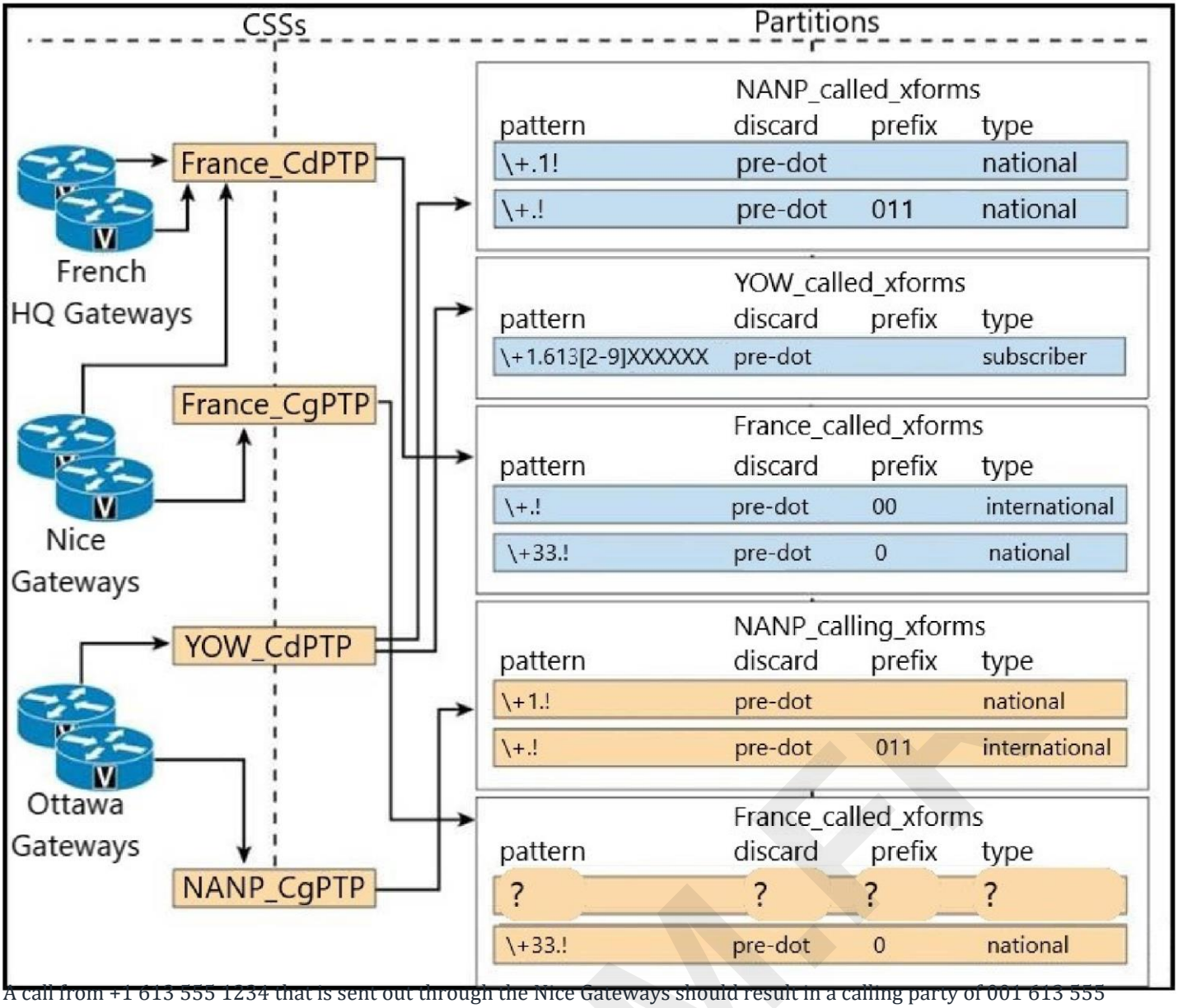
Cisco Unified Communications Manager (CUCM) generates configuration files for devices, including IP phones. These files contain settings such as directory numbers, features, and firmware information. The naming convention for these files is crucial for the phones to properly identify and download their specific configurations. SIP phones, unlike SCCP phones (which start with 'SEP'), utilize the 'SIP' prefix in their configuration file names. The MAC address is incorporated into the filename but with a transformation. The transformation is that the period ('.') separators within the MAC address are removed and the letters are converted to uppercase. Therefore, the MAC address 0030.96D2.D5CB becomes 003096D2D5CB. Additionally, the "cnf" suffix is used for configuration files. However, the filename format used by Cisco is not a straightforward concatenation of the prefix ("SIP") and the MAC address. In reality, the Cisco system converts the MAC address into a "numeric" representation by removing the dots and converting hexadecimal digits to decimal digits and is used internally. While the question refers to MAC address 0030.96D2.D5CB, it uses an alternate string "0030407101980" instead of the direct MAC address conversion of "003096D2D5CB". This is an internal representation used by the system for this MAC address. Therefore, the filename format becomes SIP[alternateMAC].cnf where the alternate numeric value is 0030407101980 for the provided MAC. So the full file name is SIP0030407101980.cnf. The .xml extension is not used for standard configuration files in this context. Cisco UCM will use the transformed MAC address to identify the appropriate configuration details for this specific SIP phone.

For further research, refer to the following Cisco documentation:

Cisco Unified Communications Manager Administration Guide: (Specific sections on phone configuration file generation). Unfortunately, direct links to specific pages within Cisco documentation are often dynamic and change. However, searching for "Cisco UCM phone configuration file naming" or "Cisco UCM XML configuration files" on the Cisco website (https://www.cisco.com/) will provide detailed information. **Cisco IP Phone documentation for your specific phone model:** This documentation will confirm the specific file naming conventions and also contains technical details.

Question: 57

Refer to the exhibit.



A call from +1 613 555 1234 that is sent out through the Nice Gateways should result in a calling party of 001 613 555 1234 with the numbering type
`international`. Which configuration accomplishes this goal?

A. \+1.! none pre-dot 001 international
B. \+.001! pre-dot 1 international
C. 613XXXXXXX none +011 international
D. \+.! pre-dot 00 international

Answer: D

Explanation:

Correct answer D

In this link you can see the same example with the solution:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12/dialplan.html

Question: 58

An administrator troubleshoots call flows and suspects that there are issues with the dial plan. Which tool enables a quick analysis of the dial plan and provides call flows of dialed digits?

A. Dial Plan Analyzer
B. Dialed Number Analyzer
C. Cisco Dial Plan Analyzer
D. Digit Analysis Analyzer

Answer: B

Explanation:

The correct answer is **B. Dialed Number Analyzer**. This tool is specifically designed within Cisco Collaboration solutions to analyze call routing based on dialed digits. It allows administrators to input a dialed number and trace its journey through the dial plan, showing how it's processed by partitions, calling search spaces, route patterns, translation patterns, and ultimately where the call is routed. Option A, Dial Plan Analyzer, is a generic term and not a specific Cisco tool name. Option C, Cisco Dial Plan Analyzer, is also not the correct name of the actual tool used. Option D, Digit Analysis Analyzer, is not a recognized tool name in Cisco Collaboration documentation. The Dialed Number Analyzer provides a visual and detailed breakdown, enabling quick identification of misconfigurations or unexpected routing. It helps pinpoint issues such as incorrect route patterns, overlapping partitions, or misconfigured translation patterns, streamlining troubleshooting and ensuring efficient call management. This feature is a crucial component for effective dial plan administration in a Cisco Unified Communications environment. The Dialed Number Analyzer is accessible within the Cisco Unified Communications Manager (CUCM) administration interface and plays a vital role in understanding and optimizing call flows.

Authoritative Link:

Cisco Unified Communications Manager Administration Guide, Release 12.5(1) - Using the Dialed Number Analyzer (Search for "Dialed Number Analyzer")

Question: 59

What are two characteristics of jitter in voice and video over IP communications? (Choose two.)

A. The packets arrive at uniform time intervals.
B. The packets arrive at varying time intervals.
C. The packets never arrive due to tail drop.
D. The packets arrive out of sequence.
E. The packets arrive with frame errors.

Answer: BD

Explanation:

Jitter, in the context of VoIP and video over IP, refers to the variation in latency or delay experienced by data packets as they traverse a network. Option B, "The packets arrive at varying time intervals," accurately describes this core characteristic of jitter. Ideally, packets should arrive at the destination at consistent intervals, ensuring smooth playback of voice or video. However, network congestion, routing variations, and other factors can introduce differing delays, leading to packets arriving with inconsistent spacing. This irregular timing can disrupt the synchronization needed for real-time communication, leading to audible glitches, choppy video, and overall degraded user experience.

Option D, "The packets arrive out of sequence," is another important characteristic often associated with jitter. While not the direct definition of jitter, the varying delays caused by jitter can lead to packets arriving at the receiver in a different order than they were sent. This is because packets taking different paths or encountering different levels of delay can arrive out of order. While reordering mechanisms exist at the receiving end, significant out-of-sequence arrival increases the complexity of processing and recovery, exacerbating the effects of jitter. Thus, both options B and D accurately capture the impact of jitter on real-time communication.

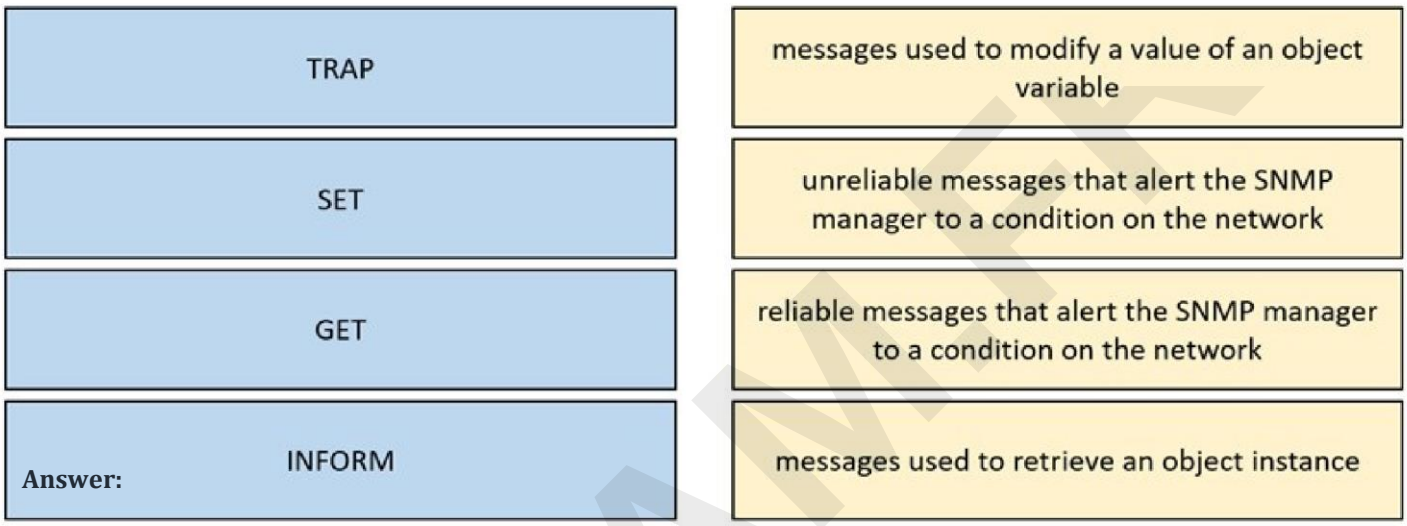
Option A is incorrect because jitter specifically describes non-uniform arrival times. Option C is related to packet loss, not directly jitter. Option E relates to corruption within the packet itself during transmission (frame error), and it's not caused by jitter.

For further research, explore these resources:

1. Cisco Documentation on Jitter: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/12x/collab12x/cucm_desig 2. Wikipedia - Jitter: https://en.wikipedia.org/wiki/Jitter
3. TechTarget Definition: https://www.techtarget.com/searchnetworking/definition/jitter

Question: 60

DRAG DROP -
Drag and drop the SNMPv3 message types from the left onto the corresponding definitions on the right.
Select and Place:



Answer:

SET

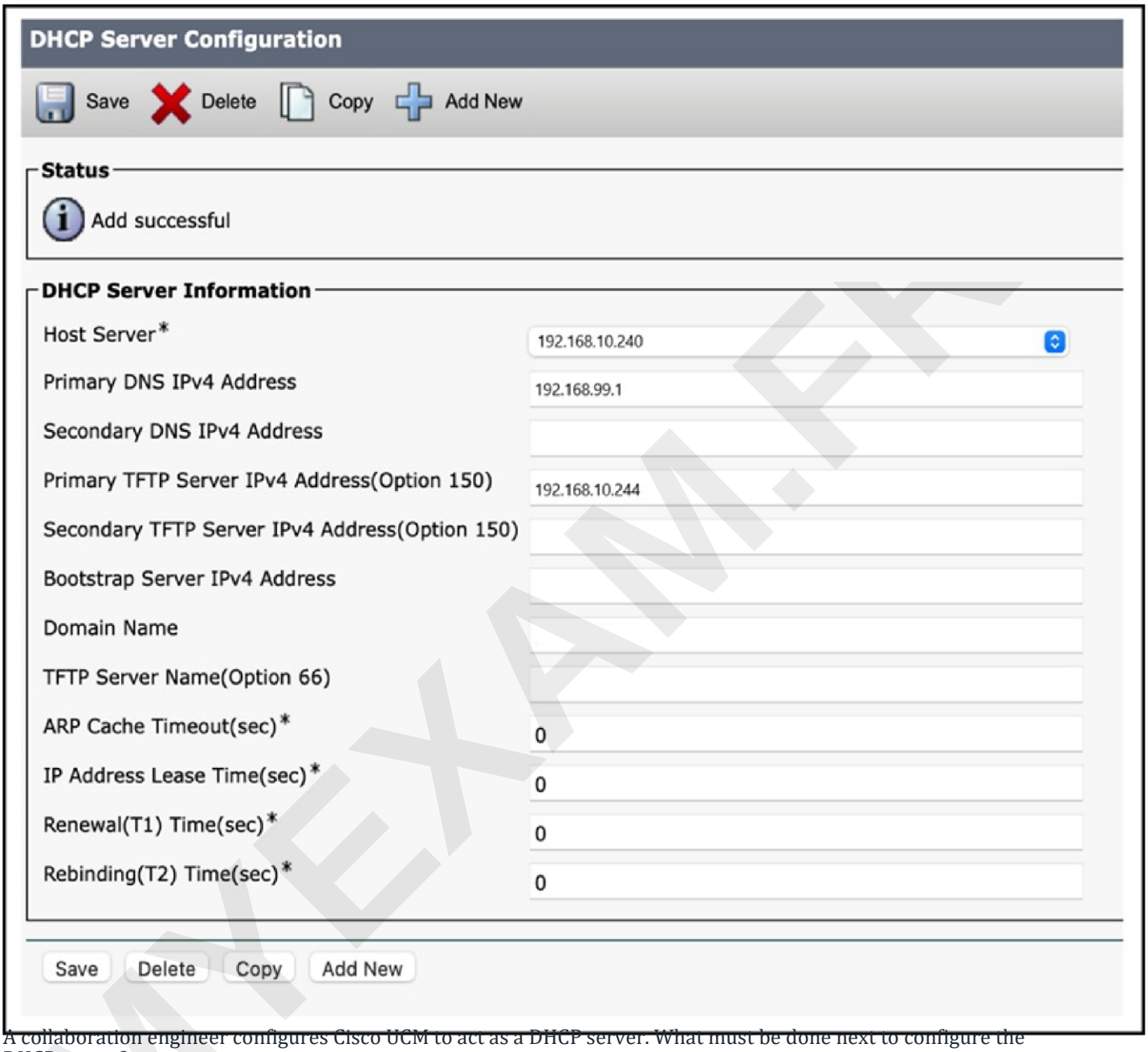
TRAP

INFORM

GET

Question: 61

Refer to the exhibit.



A collaboration engineer configures Cisco UCM to act as a DHCP server. What must be done next to configure the DHCP server?

A. Restart the TFTP service under Cisco Unified Serviceability.
B. Add a DHCP subnet to the DHCP server under Cisco UCM Administration.
C. Add the new DHCP server to the primary DNS server.
D. Restart the Cisco DHCP Monitor Service under Cisco Unified Serviceability.

Answer: B

Explanation:

After "DHCP Server" configuration, the "DHCP Subnet" should be configured.

DHCP Subnet needs to be configured after DHCP Server configuration.

Question: 62

What are two features of Cisco Expressway that the customer gets if Expressway-I and Expressway-E are deployed? (Choose two.)

A. session-based access to comprehensive collaboration for remote workers, without the need for a separate VPN client
B. highly secure firewall-traversal technology to extend organizational reach
C. complete endpoint registration and monitoring capabilities for devices that are local and remote
D. additional visibility of the edge traffic in an organization
E. utilization and adoption metrics of all remotely connected devices

Answer: AB

Explanation:

Here's a breakdown of why options A and B are the correct choices when deploying Cisco Expressway-C and Expressway-E, alongside why the others are incorrect:

A. session-based access to comprehensive collaboration for remote workers, without the need for a separate VPN client: This is a core function of the Expressway pairing. Expressway-C (Core) sits within the internal network and Expressway-E (Edge) is placed in the DMZ. Together, they facilitate secure, traversal of media and signaling, allowing remote workers to seamlessly access collaboration services (like Webex, Jabber) without requiring a traditional VPN. The 'session-based' aspect means that connections are dynamically established when needed and then torn down, reducing security exposure compared to always-on VPNs.

B. highly secure firewall-traversal technology to extend organizational reach: Expressway's main purpose revolves around this capability. Expressway-E handles inbound connections from the internet while Expressway-C interacts with internal collaboration infrastructure. The "traversal" happens through a secure mechanism, handling NAT and firewall configurations transparently. This enables secure audio, video, and content sharing between internal users and those on the external internet without compromising the organization’s security posture.

C. complete endpoint registration and monitoring capabilities for devices that are local and remote: While Expressway plays a role in allowing remote devices to connect to the collaboration environment, it does not provide comprehensive endpoint registration and monitoring. Endpoint management is typically handled by other Cisco services like Cisco Unified Communications Manager (CUCM) and Cisco DNA Center. Expressway focuses on connection and media traversal, not device lifecycle.

D. additional visibility of the edge traffic in an organization: Although Expressway provides some level of

visibility into traffic that passes through the edge, primarily for troubleshooting and capacity planning, it is not its primary function. Dedicated network monitoring solutions are needed for complete edge traffic visibility. Expressway logs focus more on connection attempts, media quality, and traversal issues.

E. utilization and adoption metrics of all remotely connected devices: Expressway doesn't directly track detailed utilization and adoption metrics. These types of analytics are more typically handled by Webex Control Hub or Cisco Unified CM reporting. Expressway's primary task is to establish and maintain connections, not to provide user behavior analysis.

Authoritative links for further research:

1. **Cisco Expressway Administrator Guide:**https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0/mra/b_MRA_Deployment_Guide_X14_0/b_MRA_Deployment_Guide_X14_0_chapter_01.html

2. **Cisco Expressway Deployment Guide:**https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0/basic/b_Basic_Configuration_Guide_X14_0.html

In summary, the core functions of Expressway-C and Expressway-E are to provide secure, VPN-less access for remote workers and to handle firewall traversal for collaboration services, establishing a necessary bridge between internal and external networks.

Question: 63

What is a capability of Cisco Expressway?

A. It functions as an analog telephony adapter.
B. It provides access to on-premises Cisco Unified Communications infrastructure for remote endpoints.
C. It has remote endpoint enrollment with Certificate Authority Proxy Function.
D. It gives directory access for remote users via Cisco Directory Integration

Answer: B

Explanation:

Cisco Expressway acts as a crucial gateway for extending Cisco Unified Communications services beyond the internal network. Its primary function, relevant to option B, is to securely connect remote endpoints, such as mobile clients or teleworkers, to on-premises Cisco Unified Communications infrastructure. This enables users outside the corporate network to seamlessly access features like voice, video, and messaging, as if they were within the office. Option A is incorrect; Expressway doesn't serve as an analog telephony adapter; this is the role of devices like Cisco ATA. Option C is partially true – Expressway can work with Certificate Authority Proxy Function (CAPF) for device certificate management, but its core capability is not the enrollment of remote endpoints in itself. Option D, while directory access might be a side effect, isn't its primary capability; Expressway handles media and signaling transport for remote users not just directory lookup. Essentially, Expressway provides secure traversal of firewalls and NAT, facilitating a seamless and secure communication experience for remote users connecting to on-premises systems. It leverages technologies like TLS and SRTP for secure media and signaling transmission. This makes the answer B correct, focusing on its main function of providing access to on-premises Cisco infrastructure for remote users. Further information about Cisco Expressway can be found on Cisco's official website: https://www.cisco.com/c/en/us/products/unified-communications/expressway/index.html and documentation: https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html.

Question: 64

Refer to the exhibit.

```
admin:utils ntp status
ntpd (pid 17428) is running...

     remote           refid      st t when poll reach   delay   offset   jitter
==============================================================================
*192.168.1.1    17.253.14.125      2 u   39   64    3    0.456  -0.236    0.116
*192.168.1.2    17.253.14.125      2 u   38   64    3    0.817  -0.695    0.395
```

A collaboration engineer needs to replace the original, single NTP server that was configured during the initial install of a Cisco UCM server. What is the first step to accomplish this task?

A. Stop the NTP service on Cisco UCM.
B. Enable NTP authentication for the new NTP server on Cisco UCM.
C. Restart the NTP service on Cisco UCM.
D. Delete the original NTP server from Cisco UCM.

Answer: D

Explanation:

the correct answer is D.

If you look at the exhibit on the "utils ntp status", it shows two original servers installed. And if you ready the question carefully, there is a "," after "original,", which means, from two original NTP servers, only single NTP server needs to be delete. So you can delete a single NTP server from the two listed NTP servers. However, even if there is only one server, you can't enable authentication for the new NTP server, you need first add it, then enable it with command "utils ntp auth symmetric-key enable" which you get prompt to select for enable the authentication for the listed servers:

admin:utils ntp auth symmetric-key enable

At the end, nothing in the question mentioned about NTP authentication, as you can see authentication report with the following command:

admin:utils ntp auth symmetric-key status

Question: 65

Refer to the exhibit.

```
admin:utils ntp status
ntpd (pid 17428) is running...

     remote           refid      st t when poll reach   delay   offset   jitter
==============================================================================
*192.168.1.1    17.253.14.125      2 u   36   64  377    0.435   0.039    0.047
 192.168.1.2    .INIT.            16 u    -   64    0    0.000   0.000    0.000
```

A collaboration engineer adds a redundant NTP server to an existing Cisco Collaboration solution. On the Cisco UCM OS Administration page, the new NTP server shows as "Not Accessible". Which action resolves this issue?

A. Delete and re-add the new NTP server via the Cisco UCM command-line interface.
B. Start the NTP service on the new NTP server.
C. Configure the reach value as 377 for the new NTP server.

D. Restart NTPD on the Cisco UCM server.

Answer: B

Explanation:

https://www.certyiq.com/discussions/cisco/view/75414-exam-350-801-topic-1-question-65-discussion/

Question: 66

Which action is required for a firewall configuration on a Mobile and Remote Access through Cisco Expressway deployment?

A. The external firewall must allow these inbound connections to Expressway: SIP: TCP 5061: HTTPS: TCP 8443; XMPP: TCP 5222; Media: UDP 36002 to 59999.

B. The internal firewall must allow these inbound and outbound connections between Expressway-| and Expressway-E: SIP: HTTPS (tunneled over SSH between | and E): TCP 2222: TCP 7001; Traversal Media: UDP 2776 to 2777 (or 36000 to 36011 for large VM/appliance); XMPP: TCP 7400.

C. Do not use a shared address for Expressway-E and Expressway-|, as the firewall cannot distinguish between them. If static NAT for IP addressing on Expressway-E is used, ensure that any NAT operation on Expressway-| does not resolve the same traffic IP address. Shared NAT is not supported.

D. The traversal zone on Expressway-| points to Expressway-E through the peer address field on the traversal zone, which specifies the Expressway-E server address. For dual NIC deployments, set the Expressway-E address using an FQDN that resolves the IP address of the internal interface.

Answer: A

Explanation:

The correct answer is **A**. Here's a detailed justification:

Mobile and Remote Access (MRA) deployments using Cisco Expressway rely on specific firewall rules to function correctly. Expressway-E, which sits at the network edge, is responsible for handling connections from external clients. These connections need to be permitted by the external firewall. Option A accurately describes these essential inbound rules. SIP (Session Initiation Protocol) over TCP port 5061 is required for signaling and call control. HTTPS (Hypertext Transfer Protocol Secure) over TCP port 8443 is used for secure web interfaces and provisioning. XMPP (Extensible Messaging and Presence Protocol) over TCP port 5222 facilitates instant messaging and presence information. Media traffic, which includes voice and video, travels over UDP ports 36002 to 59999. These ports must be opened for media to flow correctly during calls.

Option B describes internal communication between Expressway-C and Expressway-E. While these ports are necessary for proper internal communication, they are not the correct firewall requirements for the external firewall. Option C, while important for general deployment, doesn't focus on specific firewall configurations, and instead discusses addressing considerations. Option D relates to how traversal zones are configured within the Expressway and is not a matter of firewall configuration. It is more a routing configuration within the Expressway. Therefore, A is the only answer focused on firewall rules for external connectivity.

For more detailed information, refer to Cisco's documentation on Expressway firewall traversal:

Cisco Expressway Configuration Guide (latest version): (Refer to the section on firewall requirements) -Search on Cisco's website, as version numbers change.

Cisco Collaboration System 12.x SRND (search for firewall requirements): https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.htmlSpecifically look at section that describes network requirements for MRA

These resources will give a thorough explanation of the necessary ports and protocols that need to be allowed for MRA functionality through a firewall.

Question: 67

The IP phones at a customer site do not pick an IP address from the DHCP. An engineer must temporarily disable LLDP on all ports of the switch to leave only
CDP. Which two commands accomplish this task? (Choose two.)

A. Switch(config)# no lldp transmit
B. Switch# configure terminal
C. Switch# copy running-config startup-config
D. Switch(config)# no lldp run
E. Switch(config)# interface GigabitEthernet1/0/1

Answer: BD

Explanation:

Here's a breakdown of why options B and D are correct, and why the others are not, when aiming to disable LLDP on a Cisco switch:

Correct Options:

B. Switch# configure terminal: This command is essential to enter global configuration mode on a Cisco switch. Changes to device-wide protocols like LLDP need to be done in this mode. You need this before you can implement any global configuration. You must enter the configure terminal command.
D. Switch(config)# no lldp run: This command disables LLDP globally on the switch. By using no in front of the command, you negate the effect. This effectively turns off LLDP advertisement and listening on all switch ports. This action fulfills the requirement of the problem to disable LLDP.

Incorrect Options:

A. Switch(config)# no lldp transmit: This command would only prevent the switch from transmitting LLDP packets, but the device will still be listening for LLDP packets. This does not achieve the goal of disabling LLDP fully.
C. Switch# copy running-config startup-config: This command is used to save the current configuration to NVRAM (Non-Volatile Random Access Memory). While crucial for persistence, it has no bearing on disabling LLDP itself. It should be executed to save the config after any change to the configuration.
E. Switch(config)# interface GigabitEthernet1/0/1: This command would only enter the configuration mode for a specific interface. LLDP would need to be disabled on all interfaces, making this option tedious and inappropriate if the requirement is to disable LLDP on all ports of a switch.

Justification:

The core objective is to globally disable LLDP so that the IP phones will not use LLDP for neighbor discovery, while leaving only CDP active to be utilized. Therefore the commands to do this will always be executed at the global configuration level and will utilize the keyword run. By entering configuration mode using "configure terminal", you can then disable LLDP globally using the command "no lldp run". The command "no lldp transmit" would not completely disable LLDP. The command "copy running-config startup-config" is important, but is not the command used to disable LLDP. The command "interface GigabitEthernet1/0/1" would not disable LLDP globally. These are the reasons why options B and D are correct.

Authoritative Links for further research:

Cisco Command Reference for LLDP:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/lldp/command/lldp-cr-book.html (This document provides details of the lldp run command and other LLDP related commands.) **Cisco IOS Configuration Fundamentals:**https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/16-12/b_16-12-configuration-fundamentals/m-cfg-console.html (This explains how to enter various modes in Cisco IOS.)

Question: 68

To provide high-quality voice and take advantage of the full voice feature set, which two access layer switches provide support? (Choose two.)

A. Use multiple egress queues to provide priority queuing of RTP voice packet streams and the ability to classify or reclassify traffic and establish a network trust boundary.

B. Deploy RSVP to improve VoIP QoS only where it can have a positive impact on quality and functionality where there is limited bandwidth and frequent network congestion.

C. Map audio and video streams of video calls (AF41 and AF42) to a class-based queue with weighted random early detection.

D. Use 802.1Q trunking and 802.1p for proper treatment of Layer 2 CoS packet marking on ports with phones connected.

E. Implement IP RTP header compression on the serial interface to reduce the bandwidth required per voice call on point-to-point links.

Answer: AD

Explanation:

Justification:

The correct answer choices are **A** and **D**. Here's why:

Option A: Access layer switches handling voice traffic require robust QoS capabilities. Multiple egress queues are crucial for prioritizing voice packets (RTP streams) over other data. This prevents latency and jitter, ensuring high-quality voice calls. Furthermore, the ability to classify and reclassify traffic allows for granular control over voice packet treatment and the ability to establish a network trust boundary where traffic entering the network is classified.

Option D: 802.1Q trunking is essential for VLAN segmentation, which separates voice traffic from other data traffic on the same physical link. 802.1p prioritizes traffic at Layer 2 using Class of Service (CoS) markings. This allows the switch to prioritize voice traffic based on the CoS tag applied by the phone. The combination of 802.1Q and 802.1p ensures proper Layer 2 treatment for voice traffic from the access layer, which is particularly important when connecting IP phones.

Let's examine why the other options are incorrect:

Option B: RSVP is rarely used in modern networks for QoS due to its scalability issues and management overhead. While RSVP might theoretically improve VoIP QoS in specific scenarios, it's an impractical solution for most networks.

Option C: While classifying audio and video streams is good practice, WRRED is more appropriate at higher congestion points such as those that would be found at a distribution or core switch. On the access layer, ensuring there is enough buffer for traffic is more important.

Option E: RTP header compression is more applicable for lower-bandwidth serial interfaces that are often found on WAN connections. It isn't relevant to access layer switches typically.

Authoritative Links:

Cisco Documentation on QoS:https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/configuration/15-sy/qos-15-sy-book.html
IEEE 802.1Q:https://www.ieee802.org/1/pages/802.1Q.html
IEEE 802.1p:https://standards.ieee.org/ieee/802/1780/

Question: 69

A customer wants to conduct B2B video calls with a partner using an on-premises conferencing solution. Which two devices are needed to facilitate this request?
(Choose two.)

A. Expressway-C
B. MGCP gateway
C. Cisco Unified Border Element
D. Cisco TelePresence Management Suite
E. Expressway-E

Answer: AE

Explanation:

The customer's requirement for B2B video calls with an on-premises conferencing solution necessitates components that can handle calls traversing network boundaries. Expressway-C (Option A) is crucial as the internal traversal server within the customer's network. It manages secure communication between internal endpoints and the outside world. Expressway-E (Option E), the external traversal server, acts as the demarcation point to the public internet, facilitating secure call signaling and media exchange with the partner's infrastructure. Together, Expressway-C and Expressway-E form the Cisco Collaboration Edge, enabling firewall traversal and secure connectivity for B2B collaboration. A MGCP gateway (Option B) is relevant for traditional voice connectivity but is not necessary for video collaboration using modern protocols like SIP. Cisco Unified Border Element (Option C), while handling SIP-to-SIP interconnections, is typically deployed for service provider environments, not directly for B2B partner calls. Cisco TelePresence Management Suite (Option D) is for scheduling, managing, and monitoring video conferencing, not for directly establishing the necessary network connectivity for external calls. Thus, the correct pairing of Expressway-C and Expressway-E is essential for enabling secure B2B video calls with an on-premises conferencing system.

These components are integral to facilitating secure and reliable collaboration across organizational boundaries.

Here are some authoritative links for further research:

1. **Cisco Expressway Deployment Guide:** https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-0/mra-deployment-guide-x14-0.html - Provides detailed information on Expressway deployment and its role in secure collaboration.
2. **Cisco Collaboration Edge Architecture:** https://www.cisco.com/c/en/us/solutions/collaboration/collaboration-edge-architecture.html - Offers an overview of the Cisco Collaboration Edge architecture, explaining how Expressway components facilitate external communication.
3. **Cisco Expressway Data Sheet:**https://www.cisco.com/c/en/us/products/collaboration-endpoints/expressway/datasheet-listing.html - Provides specifications and details about Cisco Expressway.

Question: 70

A company wants to provide remote users with access to its on-premises Cisco collaboration features. Which components are required to enable Cisco Mobile and Remote Access for the users?

A. Cisco Unified Border Element, Cisco IM and Presence Server, and Cisco Video Communication Server
B. Cisco Unified Border Element, Cisco UCM, and Cisco Video Communication Server
C. Cisco Expressway-E, Cisco Expressway-C, and Cisco UCM
D. Cisco Expressway-E, Cisco IM and Presence Server, and Cisco Video Communication Server

Answer: C

Explanation:

The correct answer is **C. Cisco Expressway-E, Cisco Expressway-C, and Cisco UCM**. Cisco Mobile and Remote Access (MRA) leverages the Cisco Expressway series to securely connect remote users to on-premises collaboration services. The Expressway-E (Edge) server acts as the public-facing component, residing in the Demilitarized Zone (DMZ). It handles secure traversal of signaling and media traffic from external networks, such as the internet, to the internal network. Conversely, the Expressway-C (Core) server is situated within the internal network and acts as the registration and call control point for the internal collaboration infrastructure.

The Cisco Unified Communications Manager (UCM) is the primary call control and session management server for the on-premises Cisco collaboration environment. It is responsible for registering endpoints and managing calls, including those initiated through MRA. The Expressway-C registers with the UCM, enabling it to provide seamless call control and feature access for remote devices.

Options A, B, and D are incorrect because they misidentify key components. While Cisco Unified Border Element (CUBE) is a vital component for SIP trunking and session border control, it does not directly facilitate MRA. Likewise, while Cisco IM and Presence Server handles IM and presence features, it is not the primary component for enabling remote call control through MRA. Cisco Video Communication Server (VCS) has been superseded by the Expressway series.

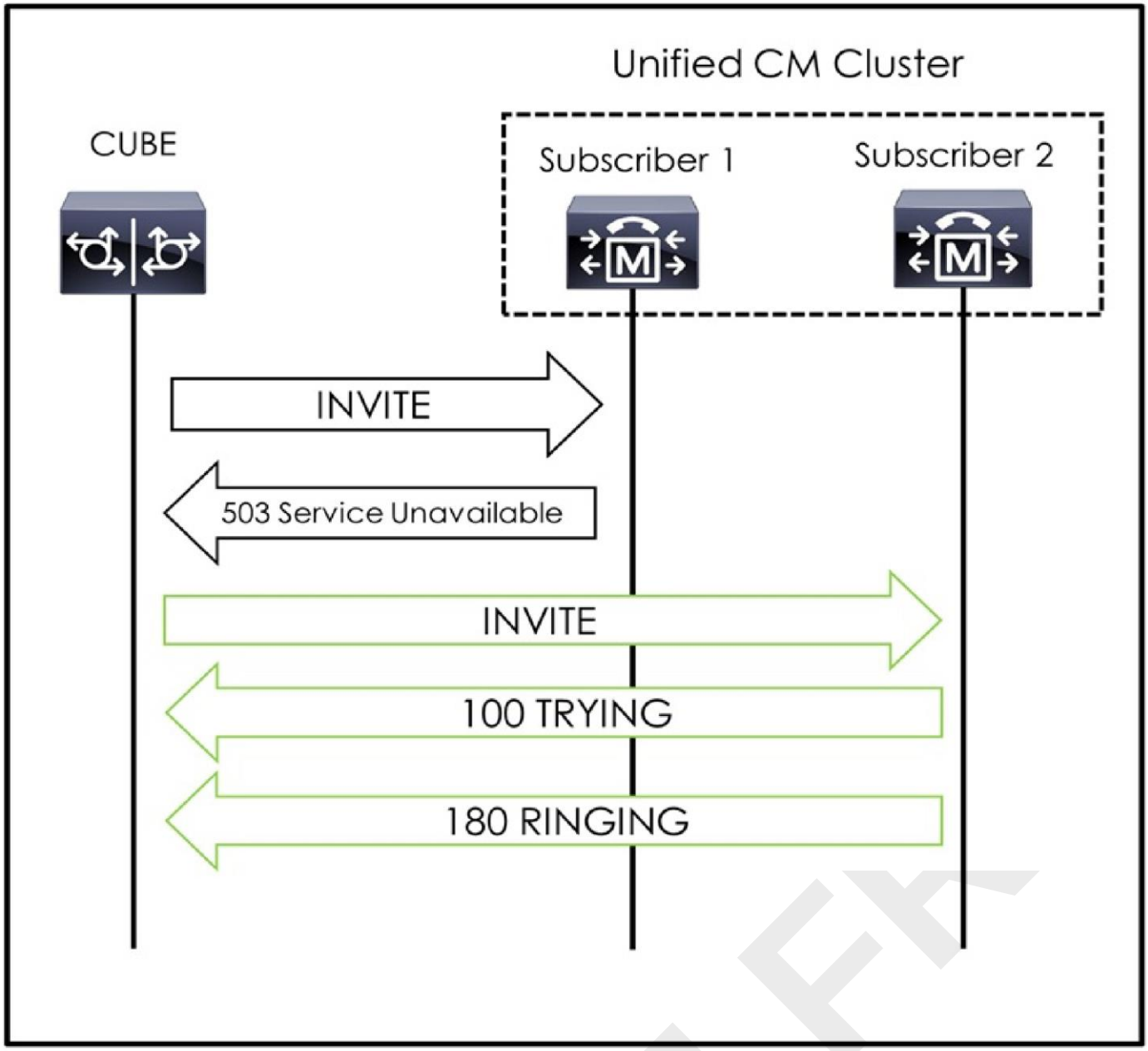
In summary, the pairing of Expressway-E and Expressway-C provides the necessary secure tunnel for remote users, while the on-premises Cisco UCM server provides the call control needed to enable collaboration services. These three elements working in unison provide the backbone of Cisco's MRA solution.

Further Research Links:

Cisco Expressway Configuration Guide:https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html
Cisco Mobile and Remote Access:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X14-5/mobile-remote-access-deployment-guide-x14-5.html
Cisco Unified Communications Manager documentation:https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

Question: 71

Refer to the exhibit.



Cisco Unified Border Element is attempting to establish a call with Subscriber 1, but the call fails. Cisco Unified Border Element then retries the same call with
Subscriber 2, and the call proceeds normally. Which action resolves the issue?

A. Verify that the Run On All Active Unified CM Nodes checkbox is enabled.

B. Verify that the correct calling search space is selected for the Inbound Calls section. C. Verify that the Significant Digits field for Inbound Calls is set to All.

D. Verify that the PSTN Access checkbox is enabled.

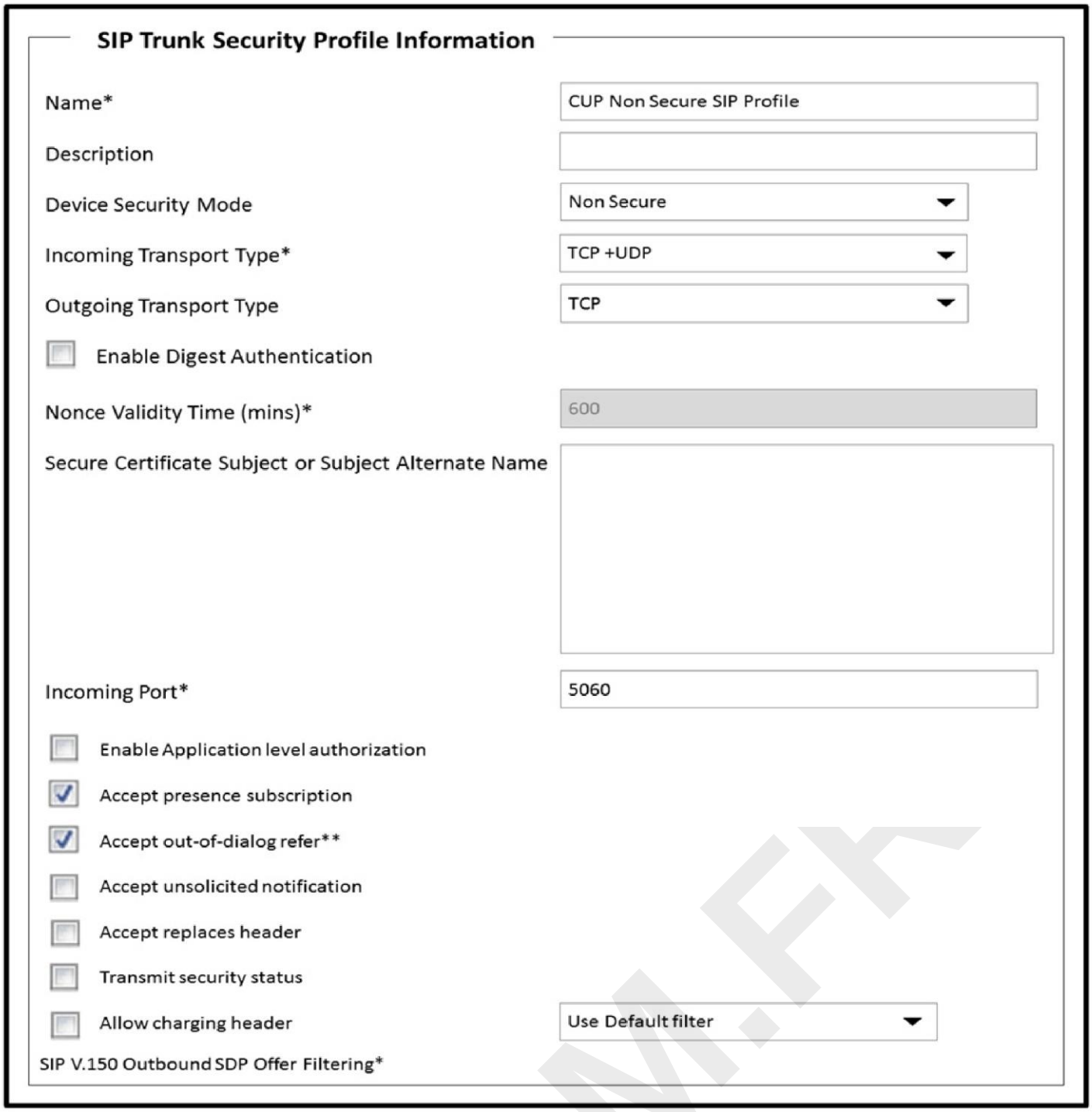
Answer: A

Explanation:

503 - Service Unavailable - The server's SIP service is temporarily unavailable.If CSS is missing it would not find a proper DN, and will return <404 - not found<Since there is no answer of several Trunks, it only explains one trunk and >Run On All Unified CM Nodes< should put in concern

Question: 72

Refer to the exhibit.



A collaboration engineer is configuring the Cisco UCM IM and Presence Service. Which two steps complete the configuration of the SIP trunk security profile?
(Choose two.)

A. Check the box to accept replaces header.
B. Check the box to allow charging header.
C. Check the box to enable application-level authorization.
D. Check the box to transmit security status.
E. Check the box to accept unsolicited notification.

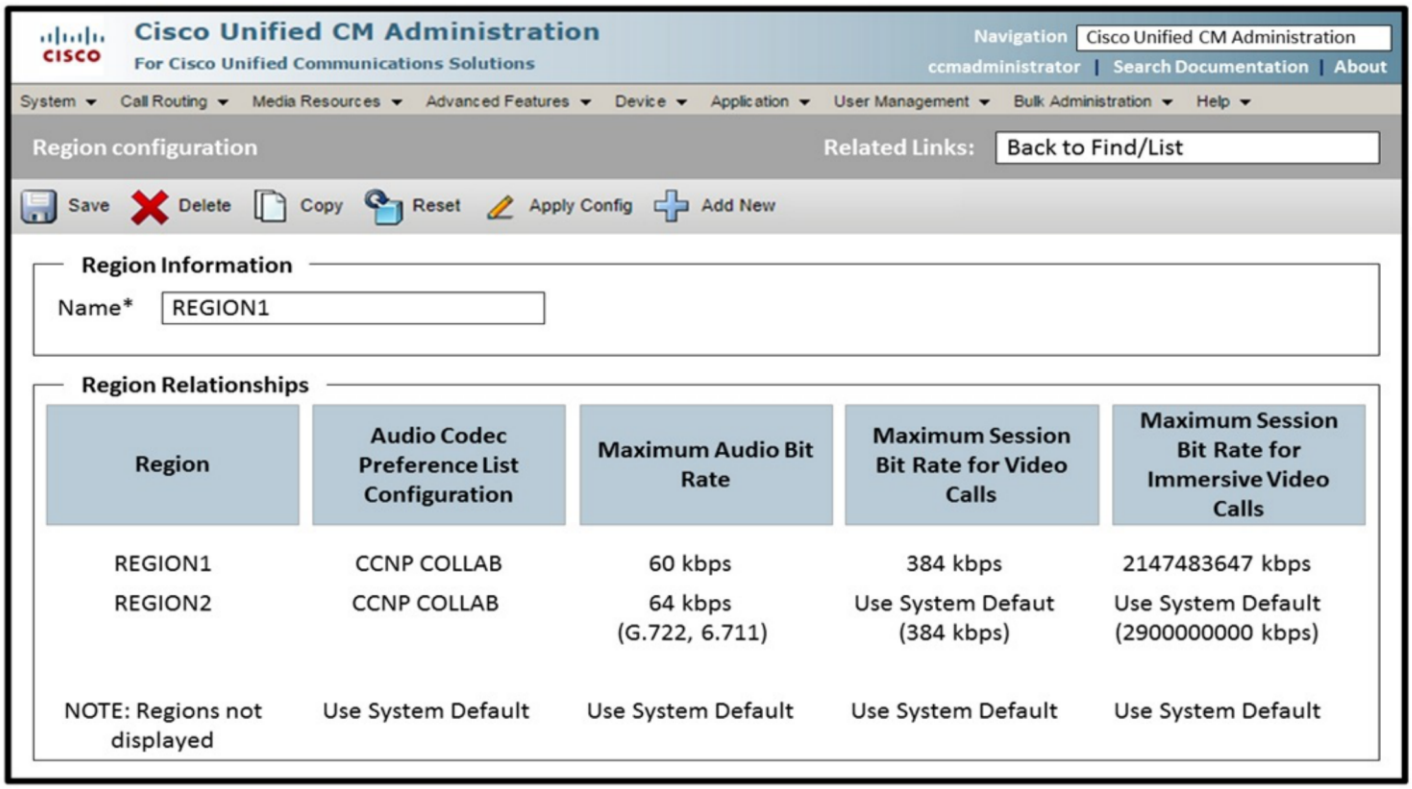
Answer: AE

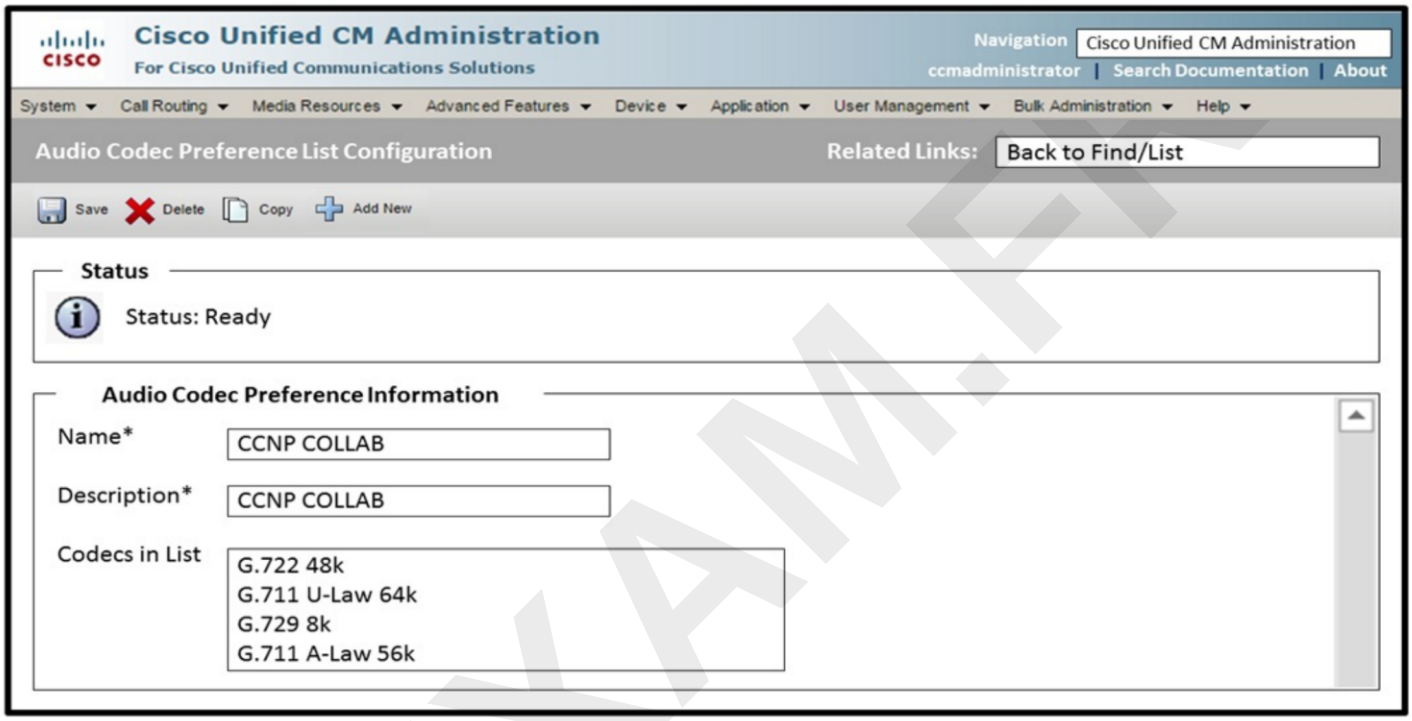
Explanation:

Reference:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/12_0_1/cup0_b_config-admin-guide-imp-1201/ cup0_b_config-admin-guide-imp-1201_chapter_0100.html

Question: 73

Refer to the exhibit.





An engineer is troubleshooting this video conference issue:

➪ A video call between a Cisco 9971 in Region1 and another Cisco 9971 in Region1 works.

➪ As soon as the Cisco 9971 in Region1 conferences in a Cisco 8945 in Region2, the Region1 endpoint cannot see the Region2 endpoint video.

What is the cause of this issue?

A. Cisco 8945 does not have a camera connected.

B. Maximum Audio Bit Rate must be increased.

C. Maximum Session Bit Rate for Video Calls is too low.

D. Maximum Session Bit Rate for Immersive Video Calls is too low.

Answer: C

Explanation:

This is one of those "trick" questions that really does not have a clear answer and is more in "reading between the lines," in typical Cisco exam fashion.Answer A: This cannot be right because that would be an assumption. 8945s have built-in video/camera.Answer B: The codecs in the list and max bitrate show no issue, so this is not it.Answer C: This is the best choice based on the information provided. The section in the question of "when the 9971 CONFERENCES IN the 8945..." indicating that the 8945 is being added to an already in-progress video call, totaling three or more video streams. This would mean 384kbps is definitely way too low.Answer D: This is wrong because neither of these devices are immersive (not SX, DX, MX, IX, etc., aka Telepresence).

Question: 74

If a phone needs to register with cucm1.cisco.com, which network service assists with the phone registration process?

A. SMTP
B. ICMP
C. DNS
D. SNMP

Answer: C

Explanation:

The correct answer is C, DNS (Domain Name System). Phones register with Cisco Unified Communications Manager (CUCM) by referencing a hostname (e.g., cucm1.cisco.com), not an IP address directly. DNS is the fundamental network service that translates human-readable domain names into the IP addresses computers need to communicate. When a phone tries to register with CUCM using the specified hostname, it first queries a DNS server. The DNS server responds with the IP address associated with cucm1.cisco.com. The phone then uses this IP address to establish a connection with the CUCM server and complete the registration process.

SMTP (Simple Mail Transfer Protocol) is used for email transmission, ICMP (Internet Control Message Protocol) is used for network diagnostics, and SNMP (Simple Network Management Protocol) is used for device monitoring; none of these directly assist in resolving hostnames to IP addresses. Therefore, DNS is the crucial service that enables the phone to find and connect to its designated CUCM server. Without DNS, the phone would not know the IP address of cucm1.cisco.com, and therefore registration would fail.

Authoritative Links for further research:

Cisco Unified Communications Manager (CUCM) documentation:
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html (Search for documentation related to phone registration and DNS configuration within CUCM)
DNS Explained:https://www.cloudflare.com/learning/dns/what-is-dns/
RFC 1035 - Domain Names - Implementation and Specification:
https://datatracker.ietf.org/doc/html/rfc1035

Question: 75

Which type of input is required when configuring a third-party SIP phone?

A. digest user
B. serial number

C. manufacturer
D. authorization code

Answer: A

Explanation:

The correct answer is **A. digest user**. When configuring a third-party SIP (Session Initiation Protocol) phone to work with a Cisco Unified Communications Manager (CUCM) or other SIP-based communication system, the device typically authenticates itself using SIP digest authentication. This authentication method employs a username (digest user) and a password, which are hashed to protect the credentials during transmission. The digest user is the unique identifier assigned to the phone within the CUCM.

Serial numbers (B) are usually used for inventory and tracking, but not for the actual registration and authentication of the device with the CUCM. The manufacturer (C) is relevant for firmware and phone profile selection, but not for authentication. Similarly, authorization codes (D) might be used for other purposes, like feature activation, but are not part of the core SIP authentication process.

In SIP digest authentication, the client (the phone) presents a hashed version of its password to the server (CUCM). The server, knowing the user's original password, performs a similar hashing process. If the two resulting hashes match, the server authenticates the client. This method is favored over simpler authentication schemes because it helps prevent password theft over the network.

Therefore, the crucial input for authenticating and registering a third-party SIP phone is the **digest user**, along with the associated password. This user is created in CUCM (or the equivalent system) and linked to the specific phone.

For further research, you can refer to these authoritative links:

Cisco Collaboration System documentation on SIP endpoints: Search the Cisco documentation portal for articles on "configuring SIP phones," specifically looking for "digest user" and authentication.
(https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html)
RFC 3261 - SIP (Session Initiation Protocol): This is the fundamental document that outlines how SIP works, including authentication mechanisms. (https://datatracker.ietf.org/doc/html/rfc3261)
Cisco CLCOR Exam Topics: Review the official Cisco CLCOR exam topics document to identify specific areas related to SIP and third-party endpoints. (https://learningnetwork.cisco.com/s/clcor-exam-topics)

Question: 76

An administrator configures Cisco UCM to use UDP for SIP signaling and finds that an endpoint cannot make calls. Which action resolves this issue?

A. Change the common phone profile.
B. Change the SIP dial rules.
C. Change the SIP profile.
D. Change the phone security profile.

Answer: D

Explanation:

The correct answer is **D. Change the phone security profile.** Here's why:

Cisco Unified Communications Manager (CUCM) utilizes phone security profiles to define security-related

parameters for endpoints. Crucially, these profiles dictate the transport protocol used for SIP signaling – specifically, whether TCP, TLS, or UDP is employed. When an endpoint cannot make calls while CUCM is configured for UDP, it's likely that the phone's assigned security profile is not configured to allow UDP for signaling.

Changing the common phone profile (A) primarily affects settings like display parameters and softkey templates, not SIP transport protocols. SIP dial rules (B) govern digit manipulation and routing, not transport protocols. While SIP profiles (C) contain overall SIP settings for a CUCM instance, they do not directly control an individual endpoint's signaling protocol.

The phone security profile, on the other hand, explicitly states the desired SIP signaling transport – TCP, TLS, or UDP. The chosen protocol on this profile must match the CUCM configuration and network capabilities. If a security profile is set to TCP or TLS when CUCM is configured for UDP, SIP signaling will fail. Modifying the security profile to allow UDP solves this mismatch, enabling the endpoint to establish SIP sessions
successfully. Therefore, adjusting the phone security profile is the appropriate method to resolve the issue of a phone's inability to make calls using UDP.

Authoritative Links:

Cisco Unified Communications Manager Security Guide:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/12_5_1/cucm_b_security-guide-1251/cucm_b_security-guide-1251_chapter_010.html#task_1933687 - This Cisco document outlines security profiles and their role in SIP signaling transport.

Cisco Collaboration SRND:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/cucm/cucm_b_cisco-collaboration-srnd/cucm_b_cisco-collaboration-srnd_chapter_011.html - The SRND provides detailed information on CUCM configurations, including phone security profile usage.

Question: 77

An engineer implements a new Cisco UCM based telephony system per these requirements:☞ The local Ethernet bandwidth is sized based on the total bandwidth per call.
☞ A G.736 codec is used.
☞ The bit rate is 64 kbps.
☞ The codec sample interval is 10 ms.
☞ The voice payload size is 160 bytes per 20 ms.
What should the size of the Ethernet bandwidth be per call?

A. 31.2 kbps
B. 38.4 kbps
C. 55.2 kbps
D. 87.2 kbps

Answer: D

Explanation:

Okay, let's break down how to calculate the Ethernet bandwidth per call for this Cisco UCM telephony system.

First, we need to understand the core components affecting bandwidth. The G.736 codec with a 64 kbps bit rate represents the raw voice data. However, network overhead adds to this. The question provides information about a payload size of 160 bytes per 20 ms, which means we aren't using G.711 which has an implied payload size.

The problem states the sample interval is 10 ms, and a 20 ms payload size is being used. Since the payload is

160 bytes for 20ms, this is 80 bytes for 10ms. Since there are 1000 ms in a second, this results in 100 * 80 = 8000 bytes per second.8000 bytes * 8 bits = 64000 bits per second, which is 64 kbps, this matches the codec.

Ethernet overhead consists of Layer 2 (Ethernet) and Layer 3 (IP) headers. Typically, this adds about 20 bytes per packet. Also, there's a 12-byte RTP header on each packet of voice data. This results in 20+12 = 32 bytes of overhead. Since there are 50 packets per second, the overhead will be 50 * 32 bytes = 1600 bytes. Multiplying by 8 bits per byte is 12800 bps.

Now we know 64 kbps of voice and 12.8 kbps of overhead totaling 76.8 kbps. Since we use Ethernet, it also includes a minimum interpacket gap of 12 bytes and a 8 byte Preamble. Therefor the Ethernet Overhead is 20 bytes.

We know we need 50 packets a second, so 20 * 50 = 1000 bytes overhead1000 bytes * 8 bits = 8000 bits = 8 kbps.Adding 8kbps to our previous 76.8 kbps total, will result in a total of 84.8 kbps. The only answer close to this is 87.2 kbps.

So the total size will be 64 kbps (voice) + 12.8 kbps (RTP/IP/UDP) + 8 kbps (Ethernet), approximately equal to 87.2 kbps. Therefore, the correct answer is D, 87.2 kbps.

For further research, you can look into:

Cisco's documentation on voice codecs and bandwidth calculations:
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-tech-notes-list.html
Understanding RTP overhead:https://en.wikipedia.org/wiki/Real-time_Transport_Protocol **Ethernet Frame Structure:**https://en.wikipedia.org/wiki/Ethernet_frame

Question: 78

Which two steps are required for bulk configuration transactions on the Cisco UCM database utilizing BAT? (Choose two.)

A. A server template must be created in Cisco UCM.
B. A data file in Extensible Markup Language format by uploaded to Cisco UCM.
C. A data file in Abstract Syntax Notation One format by uploaded to Cisco UCM.
D. A device template must be created in Cisco UCM.
E. A data file in comma-separated values format must be uploaded to Cisco UCM.

Answer: DE

Explanation:

The correct answer is **D and E**. Cisco's Bulk Administration Tool (BAT) relies on a combination of templates and data files for efficient bulk modifications to the Cisco Unified Communications Manager (CUCM) database. First, a **device template (D)** is necessary within CUCM. This template defines the specific configuration parameters for devices like phones, users, or other entities. It acts as a blueprint, ensuring consistency across the bulk additions or modifications. The template specifies which fields to update and how they should be formatted. Secondly, a **data file in comma-separated values (CSV) format (E)** is essential. This file contains the actual data that BAT will use to populate or update the configurations defined in the template. Each row represents a new device or change, while the columns correspond to the template's fields. The CSV format is chosen for its simplicity and ease of use, allowing administrators to manage large amounts of data effectively using spreadsheet software. In summary, BAT needs the device template to know what to configure, and the CSV file to know what data to configure with. Options A, B, and C are incorrect because server templates are not used in BAT transactions, and XML and ASN.1 formats are not supported for data

files. The process involves first creating a Device template to define the configuration settings, and then, a CSV file to input the data associated with these settings.

Further research:

Cisco Bulk Administration Tool (BAT) Documentation: Search for "Cisco BAT documentation" on the Cisco website for the most authoritative information on using BAT, including specific details on creating templates and formatting CSV files. Cisco Official Website (Look for the documentation specific to your CUCM version) **Understanding Device Templates:** Explore the specific details of how to create and use Device Templates within your CUCM environment via Cisco official documentation.
CSV format for BAT: Delve into formatting best practices for BAT CSV import files.

Question: 79

A collaboration engineer troubleshoots issues with a Cisco IP Phone 7800 Series. The IPv4 address of the phone is reachable via ICMP and HTTP, and the phone is registered to Cisco UCM. However, the engineer cannot reach the CLI of the phone. Which two actions in Cisco UCM resolve the issue? (Choose two.)

A. Enable Settings Access under Product Specific Configuration Layout in Cisco UCM.
B. Enable FIPS Mode under Product Specific Configuration Layout in Cisco UCM.
C. Enable SSH Access under Product Specific Configuration Layout in Cisco UCM.
D. Set a username and password under Secure Shell Information in Cisco UCM.
E. Disable Web Access under Product Specific Configuration Layout in Cisco UCM.

Answer: CD

Explanation:

The problem describes a Cisco IP phone that's generally reachable but inaccessible via its command-line interface (CLI). This indicates that basic connectivity and registration to Cisco Unified Communications Manager (UCM) are working, but the specific service needed for CLI access is either disabled or misconfigured. The correct answer is **C and D**.

Option **C**, "Enable SSH Access under Product Specific Configuration Layout in Cisco UCM," is crucial because the Cisco IP Phone 7800 series CLI is accessed via Secure Shell (SSH). By default, SSH access to the phone might be disabled in UCM, and enabling this in the phone's configuration profile in UCM allows SSH connections.

Option **D**, "Set a username and password under Secure Shell Information in Cisco UCM," is equally necessary. SSH requires authentication, so having the appropriate credentials configured within the UCM ensures that the engineer can successfully log in. This username/password combination is used for accessing the phone's CLI, without these the SSH service will not allow connections.

Options A, B, and E are incorrect. Enabling or disabling settings access, changing FIPS mode, and disabling web access do not directly influence the ability to establish an SSH connection and access the phone's CLI.

In essence, SSH access and corresponding credentials are independently controlled within Cisco UCM for security reasons. Both enabling the service and having valid credentials are required to facilitate successful CLI access on the phone. This is a common security practice to prevent unauthorized access to the phone's operational configuration.

Authoritative Links:

Cisco Unified Communications Manager Administration Guide:
https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-

callmanager/products-installation-and-configuration-guides-list.html - Refer to the configuration guides for specific phone models and how they interact with UCM settings.

Cisco IP Phone 7800 Series Documentation:https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-7800-series/products-user-guide-list.html - To understand the phone's capabilities including CLI access methods.

Question: 80

A remote office has a less-than-optimal WAN connection and experiences packet loss, delay, and jitter. Which VoIP codec should be used in this situation?

A. G.711alaw
B. iLBC
C. G.722.1
D. G.729A

Answer: B

Explanation:

The correct answer is **B. iLBC**. iLBC (internet Low Bitrate Codec) is specifically designed for use in situations with less-than-optimal network conditions, like those described with packet loss, delay, and jitter. It offers good voice quality even with significant packet loss, making it suitable for unreliable WAN connections. G.711 (A-law) is a high-bandwidth codec that produces excellent voice quality but is highly susceptible to packet loss and jitter, quickly degrading audio quality under adverse network conditions. G.722.1 is a wideband codec offering good audio, but its higher bandwidth requirements and sensitivity to network impairments make it unsuitable for the provided scenario. G.729A is a low-bandwidth codec that performs reasonably well under poor network conditions but generally doesn't perform as robustly as iLBC, especially in higher packet loss scenarios. iLBC's robust error-concealment mechanisms and moderate bit rate makes it a better choice to deliver acceptable quality under such poor network conditions. Its ability to maintain reasonable audio quality even with packet loss makes it a favorable codec for networks where connectivity is unreliable. iLBC is more computationally intensive than G.729A, however. The tradeoff between network performance and computational overhead must be evaluated before implementing the codec.

For further research on VoIP codecs and network considerations, you can consult the following resources:

Cisco Collaboration System SRND:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/collab12/collaboration_system_1 (Search for "Codecs")
iLBC codec description:https://www.rfc-editor.org/rfc/rfc3951
Understanding Codecs for VoIP:https://www.3cx.com/voip/codecs/