a.k.a dumpsqueen.com

Implementing Cisco Collaboration Core Technologies (350-801 CLCOR)

Cisco 350-801

Version Demo

Total Demo Questions: 65

Total Premium Questions: 658

Buy Premium PDF

Topic Break Down

Topic	No. of Questions
Topic 1, Infrastructure and Design	83
Topic 2, Protocols, Codecs, and Endpoints	77
Topic 3, Cisco IOS XE Gateway and Media Resources	110
Topic 4, Call Control	208
Topic 5, Quality of Service	92
Topic 6, Collaboration Applications	88
Total	658

QUESTION NO: 1

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: A D

Explanation:

Cisco Unified Communications Manager Self-Provisioning requires the end user to have a primary extension and to be associated with a user profile that contains an appropriate universal device template. The primary extension identifies the directory number that CUCM should use for the user when the device is provisioned. It therefore provides the calling identity and line association required as part of the automated device configuration. The universal device template in the user profile supplies the standardized device settings that CUCM applies when it creates the phone, such as the device pool and other configuration defaults. These two items allow CUCM to build a consistent, policy-based device configuration for the authenticated user without requiring an administrator to manually add and configure the phone first. Cisco documents the primary extension and a user profile with a universal device template as the relevant end-user configuration for Self-Provisioning. See the Cisco Unified Communications Manager System Configuration Guide and Cisco's Unified Communications Manager configuration guides.

QUESTION NO: 2

What will Differserv provide?

A. traffic classification

B. scheduling technique

C. service differentiation

D. queuing mechanism

ANSWER: C

Explanation:

DiffServ provides **service differentiation** by enabling a network to treat packets differently according to the quality-of-service policy assigned to their traffic class. At the edge of a DiffServ domain, traffic can be classified and marked with a Differentiated Services Code Point (DSCP). Network devices then use that marking to apply the per-hop behavior associated with the desired service level, such as preferential forwarding for delay-sensitive voice traffic or a lower-priority forwarding treatment for less critical traffic. The essential outcome is differentiated handling across the network rather than a single, identical forwarding treatment for all packets. This scalable model supports distinct service characteristics for different application needs while avoiding the need for each router to maintain per-flow state. Cisco describes DiffServ as a QoS architecture that classifies and marks traffic so that network nodes can apply defined forwarding behaviors. The IETF DiffServ architecture likewise defines differentiated services through scalable classification and per-hop behaviors. See Cisco’s DiffServ QoS documentation and RFC 2475.

QUESTION NO: 3

An engineer must create a route pattern for a SIP trunk with the pattern named Unity_Con_SIP_Trunk and a voicemail pilot number 8000/ < None > in Cisco Unity Connection. Which value must the engineer enter for the Gateway/Route List field?

A. Option A

B. Option B

C. Option C

D. Unity_Con_SIP_Trunk

ANSWER: D

Explanation:

Unity_Con_SIP_Trunk must be selected in the Gateway/Route List field. In Cisco Unified Communications Manager, a route pattern maps a dialed number to the outbound call-routing destination that should receive that call. Because 8000 is the voicemail pilot and Unity Connection is reached through the SIP trunk named **Unity_Con_SIP_Trunk**, associating that trunk with the route pattern directs calls placed to 8000 to Unity Connection. The route pattern provides the dial-plan match, while the selected SIP trunk supplies the signaling path to the Unity Connection server. The voicemail pilot configuration in Unity Connection must correspond to the number that CUCM routes over this trunk so that calls arriving from CUCM are recognized as calls to the configured voicemail pilot. This arrangement is a standard CUCM-to-Unity Connection SIP integration design: CUCM routes the pilot number through the Unity Connection SIP trunk, and Unity Connection answers the call as voicemail traffic. Cisco's Unity Connection integration documentation is available in the Cisco Unity Connection installation and configuration guides; CUCM dial-plan and route-pattern administration is documented in the Cisco Unified Communications Manager Administration Guide.

QUESTION NO: 4

Which two access layer switches provide support to provide high-quality voice and take advantage of the full voice feature set. 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. Use 802.1Q trunking and 802.1p for proper treatment of Layer 2 CoS packet marking on ports with phones connected.

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

D. 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.

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

ANSWER: A B

Explanation:

High-quality voice at the campus access layer depends on the switch being able to identify voice traffic at the IP-phone connection, establish an appropriate trust boundary, and place delay-sensitive RTP packets into an expedited egress treatment. "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" describes these essential access-switch QoS capabilities. Multiple hardware egress queues allow voice to receive priority scheduling during congestion, while classification, policing, and trust-boundary functions prevent an attached endpoint from improperly marking arbitrary traffic as voice.

"Use 802.1Q trunking and 802.1p for proper treatment of Layer 2 CoS packet marking on ports with phones connected" is also required for the full IP-phone feature set. An IP phone commonly uses an 802.1Q voice VLAN on its switch port and marks voice frames with Layer 2 Class of Service values using 802.1p. The access switch can then trust, preserve, or remark those markings and map them to the appropriate internal QoS queue. Cisco's QoS design guidance describes prioritizing real-time RTP and defining trust boundaries at the access edge; its campus design guidance also covers voice VLAN and access-layer QoS deployment. See Cisco QoS SRND and Cisco Campus Design Zone.

QUESTION NO: 5 - (DRAG DROP)

Drag and drop the steps from the left into order on the right to activate self-provisioning services in Cisco UCM.

Configure CTI route point.	Step 1
Configure a self-provisioning system.	Step 2
Assign a directory number to the CTI route point.	Step 3
Enable auto-registration.	Step 4
Configure an application user.	Step 5
Activate self-provisioning services.	Step 6

ANSWER:

Configure CTI route point.	Activate self-provisioning services.
Configure a self-provisioning system.	Configure CTI route point.
Assign a directory number to the CTI route point.	Assign a directory number to the CTI route point.
Enable auto-registration.	Configure an application user.
Configure an application user.	Configure a self-provisioning system.
Activate self-provisioning services.	Enable auto-registration.

Explanation:

Cisco UCM self-provisioning is configured in a dependency-based order. Start by activating self-provisioning services. This makes the Cisco Unified Communications Manager components required for the self-provisioning IVR available before any configuration attempts to use them. The service activation stage is the foundation for the remaining setup.

Next, configure the CTI route point. The CTI route point is the logical endpoint through which calls reach the self-provisioning IVR application. Once that endpoint exists, assign a directory number to the CTI route point. The directory number gives users a dialable number that reaches the route point and therefore the provisioning workflow.

After the call path is in place, configure an application user. The self-provisioning service uses this account and its associated permissions to interact with Cisco UCM and carry out provisioning-related actions. Then configure a self-provisioning system, which ties the self-provisioning behavior and required service settings together for the deployment.

Enable auto-registration only after the supporting service, CTI destination, dialable directory number, user identity, and self-provisioning system have been configured. At that point, phones that auto-register have a fully prepared self-provisioning environment available to them. Cisco documentation for the UCM administrative configuration and service setup is available in the Cisco Unified Communications Manager Administration Guide, and Cisco's self-provisioning feature overview is available in the Cisco Unified Communications Manager Feature Configuration Guide.

QUESTION NO: 6

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

A. customer interaction management services

B. secure business-to-business communications

C. secure firewall traversal for remote devices

D. Survivable Remote Site Telephony functionality

ANSWER: B C

Explanation:

Cisco Expressway provides **secure business-to-business communications** through its B2B calling capabilities. Expressway supports standards-based SIP communications between organizations while helping protect internal collaboration resources. It enables controlled calling between external business partners and an organization's Cisco Unified Communications environment, including policy-based routing and interoperability functions needed for federation-style communications.

Cisco Expressway also provides **secure firewall traversal for remote devices** through Mobile and Remote Access. In a typical deployment, Expressway-E is placed at the network edge and Expressway-C is deployed internally. Together, they establish secure traversal for remote Cisco collaboration endpoints and clients without requiring those endpoints to connect through a traditional VPN. This allows supported devices to register to collaboration services and use calling, messaging, presence, and related services while outside the corporate network. Cisco describes Expressway as providing secure remote access and business-to-business collaboration connectivity; see the Cisco Expressway product page and the Cisco documentation portal.

QUESTION NO: 7

A Cisco IP Phone 7841 that is registered to a Cisco Unified Communications Manager with default configuration receives a call setup message. Which codec is negotiated when the SDP offer includes this line of text?

M=audio 498181 RTP/AVP 0 8 97

A. G.711ulaw

B. iLBC

C. G.711alaw

D. G.722

ANSWER: A

Explanation:

G.711ulaw is negotiated. In an SDP media description using the RTP/AVP profile, the numeric values following the transport protocol are RTP payload type numbers. Payload type `0` is statically assigned to PCMU, which is G.711 μ-law audio at 8 kHz. This payload type does not require a separate `a=rtpmap` attribute because its codec mapping is defined by the RTP Audio/Video Profile. The offer lists payload type 0 first, and a Cisco Unified Communications Manager deployment using its default configuration can negotiate G.711 μ-law when it is available in the offer and is supported by the endpoint. Cisco Unified IP Phone 7841 endpoints support G.711 μ-law audio, so the phone and Cisco Unified Communications Manager can establish the RTP stream using that codec. The UDP port value in the media line identifies the offered RTP receiving port; it does not affect codec identification. The offered payload list also contains other values, but payload type 0 unambiguously identifies the selected G.711 μ-law codec in this default call scenario. The static RTP payload-type assignment is defined in RFC 3551. Cisco Unified IP Phone 7800 Series administration documentation is available from Cisco.

QUESTION NO: 8

Which two dial-peer configuration criteria can Cisco IOS XE use to match an inbound VoIP call? (Choose two.)

A. incoming called-number

B. incoming uri

C. destination-pattern

D. translation-profile outgoing

E. session target

ANSWER: A B

Explanation:

incoming called-number is a supported inbound dial-peer matching criterion. It compares the called number received on the inbound call leg against the configured dial-peer pattern and allows the gateway to select the appropriate inbound dial peer.

incoming uri is also a supported inbound matching criterion for SIP calls. It allows Cisco IOS XE to select an inbound dial peer by matching SIP URI information, such as the request URI, To header, From header, or Via header, depending on the configured URI class and match direction.

A destination pattern is normally used for outbound dial-peer selection after the gateway has identified an inbound dial peer and must route the call toward its destination. See the Cisco IOS XE Dial Peer Configuration Guide.

QUESTION NO: 9

```
INVITE sip:1@10.10.10.219;user=phone SIP/2.0
Via: SIP/2.0/TCP 10.10.10.84:50083;branch=z9hG4bK471df613
From: "1234 - My Phone" <sip:1234@10.10.10.219>;tag=381c1aba7a78002c558eda31-12b8af63
To: <sip:1@10.10.10.219>
Call-ID: 381c1aba-7a78000d-4ca6894a-41dd3e0f@10.10.10.84
Max-Forwards: 70
CSeq: 101 INVITE
Contact: <sip:1234@10.10.10.84:50083;transport=tcp>
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO
Allow-Events: kpml,dialog
Content-Type: application/sdp
Content-Length: 658

v=0
o=Cisco-SIPUA 26529 0 IN IP4 10.10.10.84
s=SIP Call
b=AS:4064
t=0 0
m=audio 32136 RTP/AVP 114 9 124 113 115 0 8 116 18
c=IN IP4 10.10.10.84
b=TIAS:64000
a=rtpmap:114 opus/48000/2
a=fmtp:114
maxplaybackrate=16000;sprop-maxcapturerate=16000;maxaveragebitrate=64000;stereo=0;sprop-
stereo=0;usedtx=0
a=rtpmap:9 G722/8000
a=rtpmap:124 ISAC/16000
a=rtpmap:113 AMR-WB/16000
a=fmtp:113 octet-align=0,mode-change-capability=2
a=rtpmap:115 AMR-WB/16000
a=fmtp:115 octet-align=1,mode-change-capability=2
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:116 iLBC/8000
a=fmtp:116 mode=20
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=yes
a=sendrecv
```

Refer to the exhibit. When a UC Administrator is troubleshooting DTMF negotiated by this SIP INVITE, which two messages should be examined next to further troubleshoot the issue? (Choose two.)

A. REGISTER

B. UPDATE

C. PRACK

D. NOTIFY

E. SUBSCRIBE

ANSWER: B C

Explanation:

UPDATE and **PRACK** should be reviewed because both SIP methods can participate in SDP offer/answer exchanges after the initial INVITE and can therefore establish or modify the negotiated DTMF media parameters. DTMF carried in-band as RTP events is negotiated through SDP attributes such as `a=rtpmap` for `telephone-event`, along with the applicable payload type, clock rate, and media direction. A subsequent SDP exchange must be checked to confirm that the initially offered telephone-event capability remains accepted and that its payload mapping is consistent in both signaling directions.

An UPDATE request can carry an SDP offer or answer without changing the dialog state, which makes it important when a call leg performs early or mid-dialog media negotiation. PRACK is especially relevant when reliable provisional responses are used: a reliable provisional response may contain an SDP offer, and PRACK can contain the corresponding SDP answer. Examining SDP bodies in these messages verifies the final offer/answer state used for DTMF and helps identify changes to RTP-event negotiation before the call reaches its connected state. The SIP offer/answer procedures are defined in RFC 3264; RTP telephone-event signaling for DTMF is specified in RFC 4733.

QUESTION NO: 10

An administrator is configuring a new Cisco UCM with PSTN capabilities. Due to bandwidth constraints, audio compression is used on the codec. DTMF must work as expected because the customer is calling many call centers where the users must select options in the call. Where is DTMF out-of-band in a CCM 12.5 with SIP-based gateway configured?

A. in the DTMF setting under SIP profile on the Cisco Unified Border Element

B. in the dial peer on the Cisco IOS router

C. in regions on the Cisco UCM where the appropriate codec to use is set

D. in DTMF settings in the audio codec preference list under regions in the Cisco UCM

ANSWER: B

Explanation:

DTMF out-of-band relay is configured on the Cisco IOS gateway's VoIP dial peer, using the `dtmf-relay` command. For SIP interworking, a common configuration is `dtmf-relay rtp-nte`, which uses RFC 2833/RFC 4733 named telephone events. Rather than relying on the compressed voice media stream to carry tones audibly, the gateway sends DTMF as separately identifiable RTP events. This preserves reliable IVR and call-center menu navigation when a compressed codec is negotiated, because the far-end application receives the intended digit events independently of the codec's audio encoding behavior.

The command is applied in the dial-peer voice configuration that handles the VoIP call leg, allowing the gateway to relay DTMF appropriately between the SIP side and the connected PSTN or VoIP call leg. The relay choice must be compatible with the DTMF method negotiated or configured for the SIP connection, but the gateway dial peer is the IOS configuration location for this DTMF relay behavior. Cisco documents DTMF relay as a VoIP dial-peer capability in its Cisco IOS Voice Command Reference; RFC named telephone events are defined in RFC 4733.

QUESTION NO: 11

An engineer with troubleshoots poor voice quality on multiple calls. After looking at packet captures, the engineer notices high levels of jitter. Which two areas does the engineer check to prevent jitter?

(Choose two.)

A. The network meets bandwidth requirements.

B. MTP is enabled on the SIP trunk to Cisco Unified Border Element.

C. Cisco UBE manages voice traffic, not data traffic.

D. All devices use wired connections instead of wireless connections.

E. Voice packets are classified and marked.

ANSWER: A E

Explanation:

Checking that the network meets bandwidth requirements is essential because voice jitter commonly results when links or device queues become congested. Real-time voice packets must be transmitted at a consistent rate; sufficient capacity on every relevant path, including access links and WAN links, reduces queue buildup and variable packet delay. Capacity planning must account for concurrent calls and for other traffic that shares the path, rather than considering voice bandwidth in isolation.

Checking that voice packets are classified and marked is equally important because classification identifies voice as real-time traffic and marking communicates its forwarding treatment across the network. Cisco QoS designs commonly mark voice media with the expedited-forwarding per-hop behavior and then use that classification to place voice into an appropriately prioritized low-latency queue. This allows network devices to protect delay-sensitive media during periods of contention and provides the consistent forwarding needed to minimize jitter. Cisco's voice-quality guidance emphasizes adequate bandwidth together with end-to-end QoS classification, marking, and priority handling for voice traffic. See Cisco: Troubleshoot QoS for Voice and Cisco: Low Latency Queueing Configuration Guide.

QUESTION NO: 12

An engineer is deploying Webex app on Microsoft Windows computers. The engineer wants to ensure that the end users do not receive pop-IQ dialogues %'hen they start the application 'Much two actions ensure the end users are not promted to accept the end-user license (Choose two)

A. Set the DELETEUSERDATA=r installation argument

B. Set the "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CiscoCollabHost\Eula_disable" registry value.

C. Set the "HKEY_LOCAL_MACHINE\SOFTWARE\CiscoCollabHost\Eula_disable" registry value.

D. Set the DEFAULT^'THEMEs-Dark"" installation argument

E. Set the "/quiet installation argument

ANSWER: B C

Explanation:

Set the `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CiscoCollabHost\Eula_disable` registry value and set the `HKEY_LOCAL_MACHINE\SOFTWARE\CiscoCollabHost\Eula_disable` registry value. These machine-level Webex registry settings suppress the End User License Agreement prompt, allowing Webex App to start without requiring each individual Windows user to acknowledge the license dialog. The two locations address the relevant Windows registry views used by the application, including the WOW6432Node location for 32-bit registry access on 64-bit Windows and the standard software location. Deploying both settings is therefore appropriate for a managed enterprise endpoint environment and ensures consistent behavior regardless of which applicable registry view Webex uses. An administrator can deliver these values through an endpoint-management platform, Group Policy preferences, or as part of a standard device-build process before users launch Webex. This is distinct from installation controls: the needed configuration persists as a system-level Webex setting and specifically governs presentation of the EULA at application startup. Cisco documents Windows deployment and enterprise configuration considerations for Webex App in its Webex App mass deployment guide. For broader administrative deployment guidance, see the Webex App administration documentation.

QUESTION NO: 13

An organization deploys Cisco Expressway Mobile and Remote Access for users outside the enterprise network. Which two public DNS records are required for client discovery? (Choose two.)

A. _collab-edge._tls SRV record for the enterprise domain

B. A or AAAA record for the Expressway-E FQDN

C. _cisco-uds._tcp SRV record in public DNS

D. _cuplogin._tcp SRV record in public DNS

E. PTR record for the Cisco UCM publisher

ANSWER: A B

Explanation:

The **_collab-edge._tls** SRV record is required for Mobile and Remote Access service discovery. Remote clients query this record for the user domain to identify the externally reachable Expressway-E service and the TLS port used for the connection.

An **A or AAAA record for the Expressway-E FQDN** is also required. The target specified in the SRV record must resolve to a public IP address that remote clients can reach on the internet. The Expressway-E certificate must contain the appropriate names used by the remote-access deployment.

The internal _cisco-uds._tcp record is used for on-premises Unified CM service discovery and is not the external MRA discovery record. See the Cisco Expressway Mobile and Remote Access Deployment Guide.

QUESTION NO: 14

An engineer configures a SIP trunk for MWI between a Cisco UCM cluster and Cisco Unity Connection. The Cisco UCM cluster fails to receive the SIP notify messages. Which two SIP trunk settings resolve this issue? (Choose two.)

A. transmit security status

B. accept unsolicited notification

C. allow charging header

D. accept out-of-band notification

E. accept out-of-dialog refer

ANSWER: B E

Explanation:

The required SIP trunk security-profile settings are **accept unsolicited notification** and **accept out-of-dialog refer**. Message-waiting indication uses SIP NOTIFY signaling sent from Cisco Unity Connection toward Cisco Unified Communications Manager. These MWI NOTIFY messages can be unsolicited—that is, they are not necessarily associated with a subscription dialog previously established by Unified CM. Enabling **accept unsolicited notification** permits Unified CM to accept and process those incoming MWI NOTIFY requests instead of rejecting them because no matching subscription dialog exists.

Cisco Unity Connection SIP integrations also require **accept out-of-dialog refer** in the Unified CM SIP trunk security profile. This allows Unified CM to accept SIP REFER requests that are sent outside an existing SIP dialog, supporting the signaling behavior used by the Unity Connection integration. Configuring both settings on the security profile assigned to the trunk enables the required signaling exchange and allows Unity Connection to update message-waiting status for Unified CM users. Cisco documents these SIP trunk security-profile requirements in its Unity Connection integration guidance and Unified CM configuration documentation: Cisco Unity Connection Integration Guide and Cisco Unified CM installation and configuration guides.

QUESTION NO: 15

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:

Change the phone security profile. In Cisco Unified Communications Manager, the phone security profile assigned to a SIP endpoint controls security-related signaling behavior, including the SIP transport settings applicable to the device. For an endpoint intended to signal with UDP, its assigned phone security profile must be configured with UDP as the appropriate transport type and must be compatible with the endpoint's own SIP transport configuration. After updating or selecting the appropriate profile, apply the change to the device and reset or restart the endpoint so that it registers and places calls using the revised signaling parameters. This is particularly important for third-party SIP devices, because a transport mismatch between Cisco UCM and the endpoint can prevent successful SIP registration or call setup. Cisco documents phone security profiles as the location for configuring security and transport characteristics for SIP devices; administrators should verify that the profile assigned to the phone matches the required UDP signaling design. See the Cisco Unified CM Administration Guide and Cisco's Unified Communications Manager documentation.

QUESTION NO: 16

When a phone is registered over Mobile and Remote Access, where does it register?

A. Cisco Unified Presence Server

B. Expressway-E

C. Cisco Unified Communications Manager

D. Expressway-C

ANSWER: C

Explanation:

A phone using Mobile and Remote Access registers with Cisco Unified Communications Manager. Mobile and Remote Access provides secure, VPN-less access for Cisco collaboration endpoints that are outside the enterprise network, but it does not change the call-control system to which the endpoint is registered. The endpoint's SIP signaling traverses the Expressway pair: Expressway-E provides the secure internet-facing edge service and proxies the connection to Expressway-C, which provides the trusted-side connection toward the collaboration deployment. Cisco Unified Communications Manager remains the system that authenticates and controls the phone registration, applies the device configuration, associates the device with an end user, supplies directory and dialing information, and provides call-processing services. Consequently, administrators configure the remote-capable endpoint as a Cisco Unified Communications Manager device in the same fundamental way as an internally connected endpoint; MRA is the secure access path to that call-control service. Cisco describes MRA as enabling remote endpoints to register to Cisco Unified Communications Manager through the Expressway deployment. See Cisco's Unified Communications Manager System Configuration Guide and the Cisco Expressway installation and configuration guides.

QUESTION NO: 17

An engineer configures local roule group names to simplify a dial plan. Where does the engineer set the route groups according to the local route group names that are configured?

A. route list

B. device pool

C. CSS

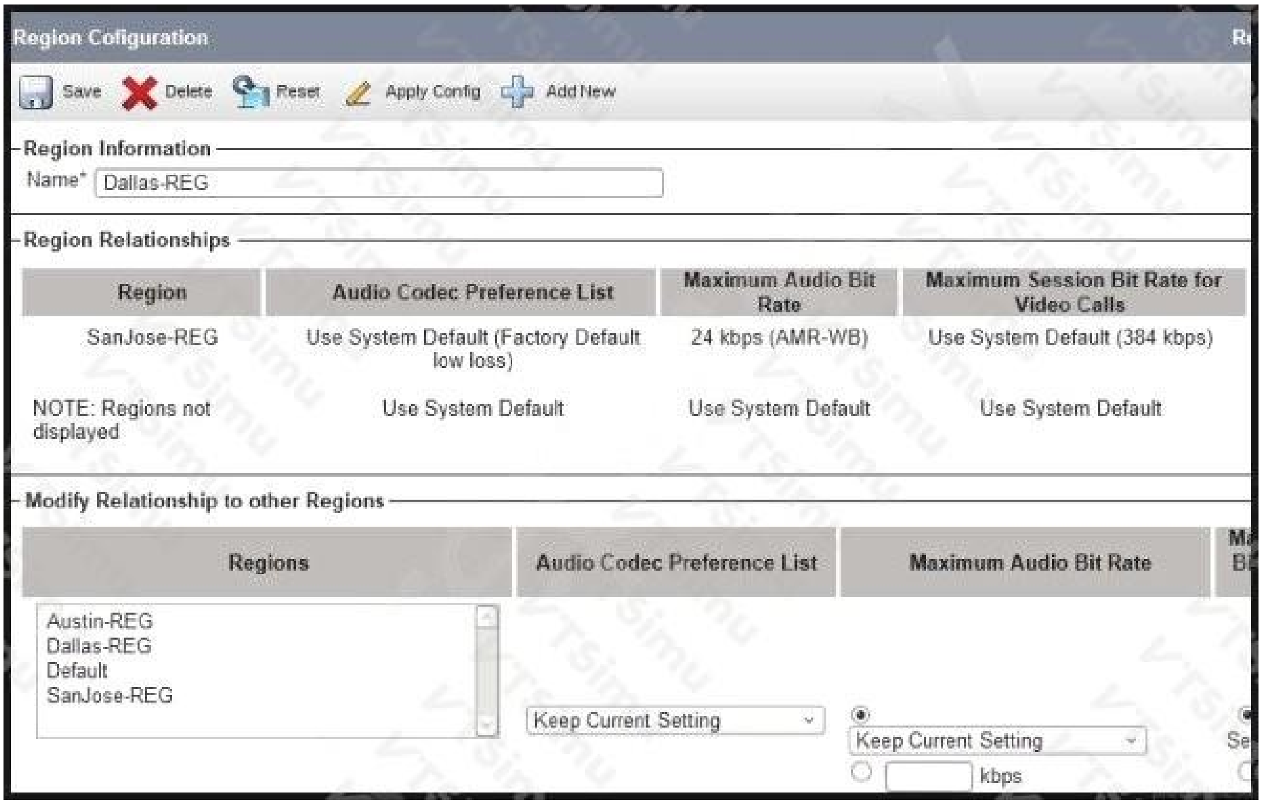
D. route pattern

ANSWER: B

Explanation:

The correct setting location is the **device pool**. In Cisco Unified Communications Manager, a Local Route Group is a logical placeholder used in a route list. Rather than permanently associating a route list with one specific route group, the Local Route Group enables the same dial-plan logic to select a route group based on the originating device's configured device pool. This design makes the dial plan more scalable and reusable across sites. For example, a route pattern can direct calls to a route list that contains the Local Route Group; CUCM then examines the calling device's device pool and uses the route group assigned as that device pool's Local Route Group. Administrators configure this association in the device pool configuration, where the Local Route Group field identifies the route group that represents the site's preferred PSTN gateway or trunk resources. This approach supports centralized route-pattern administration while preserving site-specific egress selection, including appropriate local gateway use and survivability design. Cisco's collaboration design guidance describes Local Route Groups as a mechanism for applying localized gateway selection through device pools and route lists. See the [Cisco Collaboration System Design Guide] and the [Cisco Unified CM Administration Guide].

QUESTION NO: 18



Refer to the exhibit. Which codec should an engineer select for a call made between "Dallas-REG" & "Austin-REG"?

A. G.729

B. G.711

C. MP4A-LATM

D. OPUS

ANSWER: A

Explanation:

G.729 is the appropriate codec for the call between Dallas-REG and Austin-REG because Cisco Unified Communications Manager uses the configured interregion audio bandwidth relationship to determine the codec for calls crossing regions. In a typical WAN-connected regional design, the interregion bandwidth allocation shown for these two regions is intended to accommodate a compressed G.729 audio stream rather than uncompressed G.711 audio. G.729 uses an 8-kbps audio payload and is commonly selected to conserve WAN bandwidth; the actual bandwidth consumed on the link is higher after RTP, UDP, IP, and Layer 2 overhead are included. CUCM evaluates the maximum audio bandwidth configured between the source and destination regions during call setup and negotiates a codec that fits that policy. If endpoints have different codec capabilities, CUCM can insert a transcoder when necessary, but the regional bandwidth policy remains the basis for the selected audio codec. This behavior enables administrators to provide high-quality G.711 within a LAN region while preserving constrained WAN capacity between geographically separate sites. Cisco documents region configuration and codec selection in its Collaboration System SRND and describes codec bandwidth requirements in the Codec Bandwidth Consumption guidance.

QUESTION NO: 19

SIP proxies have operations defined in RFC 3261 and supporting extensions. Though no IETF RFC completely defines how SBCs must function. SBCs evolved over the years.

Which two operations demonstrate the high-level differences between SBCs and SIP proxies? (Choose two.)

A. Stateful proxies are context-aware and can terminate communication sessions by themselves

B. SIP proxies add a Via header and optionally a Record-Route header, and the rest of the headers are left untouched

C. SBCs can modify headers such as To, From, Contact, and Call-ID. It can introduce new headers into the SIP message

D. SBCs are capable of interworking completely different protocols to set up, modify, and tear down communication sessions. It includes SIP, H.323,and MGCP protocols

E. SIP proxies are SDP-aware and can change the SDP bodies

ANSWER: B C D

Explanation:

SIP proxies add a Via header and optionally a Record-Route header, and the rest of the headers are left untouched is a high-level description of normal proxy behavior. RFC 3261 defines proxy processing around forwarding SIP requests while adding a Via value to preserve the return path and loop-detection information. A proxy can also add Record-Route when it must remain on the signaling path for subsequent dialog requests. This forwarding-oriented role contrasts with an SBC's more comprehensive, session-border role.

SBCs can modify headers such as To, From, Contact, and Call-ID. It can introduce new headers into the SIP message because an SBC commonly operates as a back-to-back user agent, creating separate call legs on each side of the border. This permits SIP normalization, topology hiding, address manipulation, and policy enforcement. SBCs are capable of interworking completely different protocols to set up, modify, and tear down communication sessions. It includes SIP, H.323, and MGCP protocols because SBC implementations can provide signaling interworking and media/session control at network boundaries. Cisco describes CUBE as a border element that performs interworking between voice technologies, while RFC 3261 defines the core SIP proxy functions. See RFC 3261, Section 16.6 and Cisco Unified Border Element overview.

QUESTION NO: 20

The IP phones al 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# copy running-config startup-config

B. Switch(config)# no lldp run

C. Switch# configure terminal

D. Switch(conlicj)# interface GigabitEthernet1/0/1

E. Switch(config># no lldp transmit

ANSWER: B C

Explanation:

`Switch# configure terminal` is required to enter global configuration mode, which is the configuration context from which LLDP is enabled or disabled globally on Cisco IOS and IOS XE switches. Once the switch is in that mode, `Switch(config)# no lldp run` disables the LLDP agent globally. Because LLDP operation is globally disabled, the switch stops transmitting and processing LLDP on its interfaces, accomplishing the requirement to remove LLDP across all ports rather than changing ports individually. CDP is a separate Cisco discovery protocol and is not disabled by the global LLDP command, so CDP remains available provided that CDP has been enabled on the switch and relevant interfaces. This is appropriate as a temporary operational change because LLDP can later be restored globally with `lldp run`. Cisco's LAN switching documentation describes LLDP as a globally controlled discovery protocol and documents use of the global LLDP configuration commands: Cisco IOS XE LAN Switching Configuration Guide. Cisco also documents CDP and LLDP as distinct device-discovery protocols: Cisco IOS Technologies.

QUESTION NO: 21

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

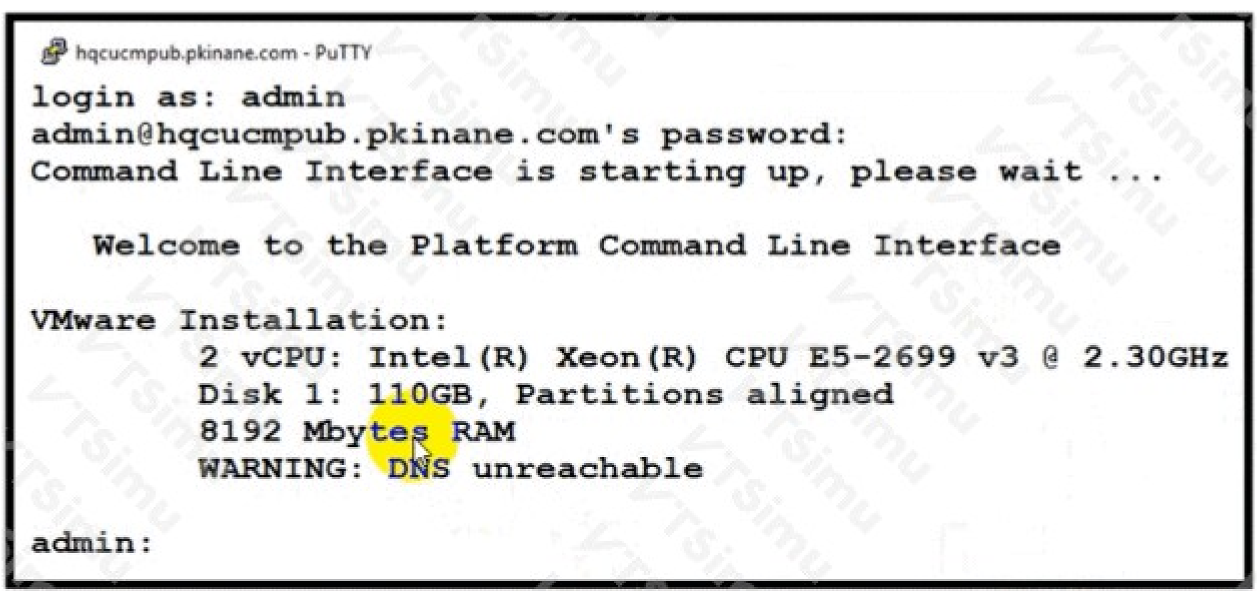
ANSWER: B

Explanation:

Cisco Unified Communications Manager uses DNS resolution for a SIP trunk when the trunk's destination is configured as a fully qualified domain name rather than as a literal IP address. This permits the SIP trunk to identify its remote SIP peer by a stable DNS name, while DNS supplies the corresponding IP address used to establish SIP signaling. DNS-based addressing is particularly useful when the remote service's IP address can change, when resiliency is provided through DNS records, or when interoperability design calls for domain-based SIP routing.

For SIP, DNS lookup behavior can include standard host-record resolution and, where applicable, SIP-specific DNS procedures that use NAPTR and SRV records to locate the appropriate SIP service and transport. The Cisco Unified CM DNS configuration must point to reachable DNS servers capable of resolving the configured destination FQDN. Cisco Unified CM then uses that resolved address when routing signaling through the SIP trunk. This approach aligns with the SIP DNS procedures defined in RFC 3263 and Cisco Unified CM system-configuration guidance for DNS and SIP connectivity in the Cisco Unified CM System Configuration Guide.

QUESTION NO: 22



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. utils ntp status

B. show cdp neighbor

C. show version active

D. utils diagnose test

E. utils diagnose module validate_network

ANSWER: D E

Explanation:

`utils diagnose test` is correct because it initiates the Unified Communications Manager diagnostic test suite. The suite checks required platform and network services, including name-resolution-related connectivity checks. When DNS is configured and the diagnostic process performs its hostname-resolution checks, the CUCM node sends DNS queries that can be observed in an active packet capture.

`utils diagnose module validate_network` is also correct because it runs the network-validation diagnostic module specifically. This module validates network dependencies needed by the CUCM server, including DNS reachability and resolution. Running it causes CUCM to query the configured DNS servers while it validates the node's network configuration, thereby generating the DNS packets required by the capture exercise. These commands are useful during troubleshooting because they produce controlled, server-originated DNS activity rather than requiring an external endpoint to create a lookup.

Cisco documents the available CUCM CLI diagnostic commands and their purpose in the Cisco Unified Communications Manager CLI Reference Guide. CUCM DNS configuration and operational guidance are also available in Cisco's Unified Communications Manager support documentation.

QUESTION NO: 23

Which two features will access layer switches provide support providing high-quality voice and taking advantage of the full voice feature set? (Choose two.)

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

B. 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.

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

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

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

ANSWER: B E

Explanation:

Access-layer switches are responsible for connecting IP phones and for applying the immediate Layer 2 and egress QoS treatment that protects real-time media as it enters the campus. "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." is correct because an access switch can define whether markings received from a phone are trusted, classify traffic when needed, and place latency-sensitive RTP voice traffic into a strict-priority egress queue. This minimizes serialization and congestion delay for voice frames. Cisco describes the trust boundary and priority treatment as central components of an end-to-end QoS design: Cisco QoS congestion-management overview.

“Use 802.1Q trunking and 802.1p for proper treatment of Layer 2 CoS packet marking on ports with phones connected.” is also correct. An IP phone access port commonly carries a data VLAN for the attached workstation and a voice VLAN for the phone. 802.1Q tagging identifies the voice VLAN, while the 802.1p CoS field carries Layer 2 priority marking so the switch can preserve and act on voice QoS markings. Cisco documents voice-VLAN operation and QoS handling for IP phone ports in its Voice VLAN configuration guide.

QUESTION NO: 24

An administrator integrates Cisco Unity Connection with Cisco UCM and must route unanswered calls to user mailboxes. Which two Cisco UCM objects are required? (Choose two.)

A. voicemail pilot

B. voicemail profile

C. hunt pilot

D. translation pattern

E. CTI route point

ANSWER: A B

Explanation:

A **voicemail pilot** identifies the directory number that Cisco Unified Communications Manager uses to reach the voicemail system. For a Unity Connection integration, the pilot is normally configured to route to the Unity Connection voice ports through the appropriate route pattern, SIP trunk, or other call-routing configuration.

A **voicemail profile** associates the voicemail pilot with Cisco UCM directory numbers. When a call is forwarded to voicemail from a line that uses the profile, Cisco UCM uses the associated voicemail pilot to route the call to Unity Connection. The voicemail profile is assigned to the relevant directory number configuration.

QUESTION NO: 25

An engineer configures a Cisco UCM SIP trunk to use TLS and enables X.509 Subject Name validation. Which two conditions are required for Cisco UCM to validate the remote SIP peer certificate? (Choose two.)

A. The remote certificate subject name matches the configured X.509 Subject Name.

B. The issuing CA certificate is uploaded to the CallManager-trust store.

C. The SIP trunk is assigned a route pattern.

D. The SIP profile has SIP OPTIONS Ping enabled.

E. The remote certificate is uploaded to the ITLRecovery certificate store.

ANSWER: A B

Explanation:

The remote certificate subject name must **match the configured X.509 Subject Name** on the SIP trunk security profile. This value identifies the expected certificate identity for the remote SIP peer and is compared with the remote certificate subject name.

The certificate chain must also be trusted by Cisco UCM. The issuing certificate authority certificate must be present in the **CallManager-trust** store so that Unified CM can validate the certificate presented by the remote SIP entity.

A SIP profile controls SIP operational behavior, but it does not establish certificate trust. Likewise, a route pattern determines dial-plan routing and is not used during TLS certificate validation. See the [Cisco Unified Communications Manager Security Guide].

QUESTION NO: 26

Where does an administrator establish the trust boundary on a LAN?

A. core router

B. voice VLAN

C. access switch

D. distribution switch

ANSWER: C

Explanation:

The access switch is the appropriate place to establish the LAN trust boundary because it is the access-layer device directly connected to endpoint devices such as Cisco IP phones and user PCs. A trust boundary should be positioned as close to the traffic source as practical, allowing the network to decide whether it will accept endpoint QoS markings or overwrite them with policy-defined values before traffic enters the rest of the campus. On a phone-facing access port, the switch can trust the phone's Layer 2 CoS marking for voice traffic while treating traffic arriving from an attached PC as untrusted. This prevents users or unmanaged endpoints from assigning elevated priority to their own traffic and ensures that voice packets receive consistent classification and treatment as they move through the distribution and core layers. Establishing this policy at the access switch therefore protects QoS resources and provides a controlled, scalable point for classification, marking, and policing at the network edge. Cisco's QoS guidance describes defining trust boundaries at the network edge and trusting markings only from known, trusted devices. See [Cisco IOS QoS Trust Configuration Guide] and [Cisco Campus Network Design Zone].

QUESTION NO: 27

What is the major difference between the two possible Cisco IM and Presence high-availability modes?

A. Balanced mode provides user load balancing and user failover in the event of an outage. Active/standby mode provides an always on standby node in the event of an outage, and it also provides load balancing.

B. Balanced mode provides user load balancing and user failover only for manually generated failovers. Active/standby mode provides an unconfigured standby node in the event of an outage, but it does not provide load balancing.

C. Balanced mode provides user load balancing and user failover in the event of an outage. Active/standby mode provides an always on standby node in the event of an outage, but it does not provide load balancing.

D. Balanced mode does not provide user load balancing, but it provides user failover in the event of an outage. Active/standby mode provides an always on standby node in the event of an outage, but it does not provide load balancing.

ANSWER: C

Explanation:

Balanced mode provides user load balancing and user failover in the event of an outage. Active/standby mode provides an always on standby node in the event of an outage, but it does not provide load balancing. This accurately describes the two high-availability deployment modes for Cisco IM and Presence Service. In balanced mode, the nodes in a redundancy group actively serve users at the same time. Users are distributed between the available nodes, which uses the capacity of both servers during normal operation. If a node becomes unavailable, its assigned users can fail over to the remaining node, preserving IM and presence availability while the failed node is recovered.

Active/standby mode instead designates one node as the active service node and retains the paired node as a synchronized standby. The standby node is maintained and ready to assume service following an active-node failure, but it does not concurrently process the normal user workload. Consequently, this model emphasizes a dedicated failover role rather than balancing users across both nodes. The distinction is therefore whether both nodes actively share user traffic under normal conditions: balanced mode does, while active/standby mode does not. Cisco configuration and deployment documentation for IM and Presence Service is available through the Cisco IM and Presence Service installation and configuration guides and the Cisco IM and Presence Service product documentation.

QUESTION NO: 28

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

E. restart of the Cisco Unified Communications Manager server

ANSWER: E

Explanation:

A restart of the Cisco Unified Communications Manager server is required after setting a new primary DNS server through the Cisco UCM CLI. The DNS server address is a system-level network setting, and CUCM applies the updated resolver configuration during server startup. Consequently, restarting only an individual application service is not sufficient to ensure that all CUCM processes and the underlying operating system use the new primary DNS information consistently.

In practice, DNS is especially important for CUCM clustering, certificate validation, service discovery, and hostname resolution. Before performing the restart, confirm that the new DNS server can resolve the required CUCM hostnames and that the change is coordinated with any cluster maintenance window. Cisco's CUCM documentation for DNS-related server configuration states that a server restart is needed for DNS changes to become effective. Cisco also provides guidance on CUCM server definition and DNS changes in its support documentation.

References: Cisco: Change CUCM Server Definition from IP Address to FQDN and Cisco Unified Communications Manager CLI Reference Guide.

QUESTION NO: 29

What is the purpose of a DNS CNAME record?

A. to provide system information about a host

B. to define an alias hostname

C. to map a hostname to an IP address

D. to map an IP address to a domain name

ANSWER: B

Explanation:

The purpose of a DNS CNAME record is **to define an alias hostname**. A CNAME, or Canonical Name, record makes one DNS name an alias of another canonical hostname. When a client looks up the alias, DNS resolves it by following the CNAME to its target name and then obtaining the target's address records, such as IPv4 or IPv6 address records. This is useful when multiple service names should refer to the same underlying host, or when an alias should remain stable even if the target host's addressing changes. For example, `www.example.com` can be configured as a CNAME pointing to a provider-assigned hostname, allowing the provider to manage the target addresses without requiring changes to the alias record. The DNS standards define a CNAME RR as specifying the canonical or primary name for an alias, and Cisco Collaboration deployments commonly depend on correct DNS naming and resolution for services, endpoints, and integrations. See RFC 1034, Domain Names—Concepts and Facilities and Cisco Collaboration System Solution Reference Network Designs.

QUESTION NO: 30

In an eleven-class queuing model following realtime, best effort, and scavenger queuing rules, what recommended percentage of bandwidth must be allocated for interactive video?

A. 10%

B. 12%

C. 15%

D. 20%

ANSWER: C

Explanation:

15% is the recommended bandwidth allocation for interactive video in the referenced eleven-class Cisco QoS queuing model. Interactive video is delay- and loss-sensitive, but it is generally handled as a guaranteed-bandwidth data class rather than being placed in the strict real-time priority queue used for voice bearer traffic. Reserving 15% gives the class a defined share during congestion, helping preserve video quality, reduce loss, and maintain acceptable interactivity without allowing video traffic to consume capacity needed by other business-critical applications.

The eleven-class model uses differentiated treatment across real-time, best-effort, and scavenger traffic categories. Within that design, classification and marking identify interactive video so that the scheduler can provide its configured bandwidth guarantee when the outbound interface is congested. The percentage is therefore a QoS design recommendation for the class, not a statement that interactive video always consumes that amount of bandwidth. Actual capacity planning must still account for codec bit rates, call volume, overhead, and WAN-link speed. Cisco QoS guidance and queuing concepts are described in the Cisco IOS XE QoS documentation and Cisco's Deploying QoS for Voice reference.

QUESTION NO: 31

What are two access management mechanisms in Cisco Webex Control Hub? (Choose two.)

A. multifactor authentication

B. Active Directory synchronization

C. attribute-based access control

D. single sign-on with Google

E. Client ID/Client Secret

ANSWER: A B

Explanation:

multifactor authentication and **Active Directory synchronization** are access-management mechanisms relevant to a Webex Control Hub organization. Multifactor authentication strengthens identity verification by requiring an additional factor beyond a password. In a Control Hub deployment, this is commonly enforced through the organization's identity provider when single sign-on is configured, allowing the organization to apply its established authentication and MFA policies before users access Webex services. This supports centralized, policy-based protection of user and administrator access.

Active Directory synchronization provides centralized identity lifecycle management. Using Cisco Directory Connector, an organization can synchronize users and selected directory attributes from an on-premises Active Directory deployment to the Webex common identity store. This helps ensure that Webex accounts reflect the organization's authoritative directory, including creating and updating user identities as directory information changes. It reduces manual account administration and supports consistent access provisioning for collaboration services. Cisco documents directory synchronization with Directory Connector at Directory Connector Deployment Guide; Cisco's identity-integration guidance, including organization authentication through an identity provider, is available at Configure single sign-on in Control Hub.

QUESTION NO: 32

When a call is delivered to a gateway, the calling and called party number must be adapted to the PSTN service requirements of the trunk group. If a call is destined locally, the + sign and the explicit country code must be replaced with a national prefix. For the same city or region, the local area code must be replaced by a local prefix as applicable. Assuming that a Cisco UCM has a SIP trunk to a New York gateway (area code 917), which two combinations of solutions localize the calling and called party for a New York phone user? (Choose two.)

A. Configure the gateway to translate the calling number and apply it to the dial peer. Combine it with a translation profile for called numbers.
!
voice translation-rule 1 rule 1 /^1917/ // rule 2 /^ [+]1917/ // !
voice translation-profile strip+1 translate calling 1
!

B. Configure two calling party transformation patterns:
\+1917.CCCCCC, strip pre-dot, numbering type: subscriber
\+!, strip pre-dot, numbering type: national

C. Configure two called party transformation patterns:
\+1917.XXXXXXX, strip pre-dot, numbering type: subscriber \+1.!, strip pre-dot, numbering type: national

D. Configure the gateway to translate called numbers and apply it to the dial peer. Combine it with a translation profile for calling numbers.
!
voice translation-rule 1 rule 1 /^1917!/ // rule 2 /^[+]1917!/ //
!
voice translation-profile strip+1 translate called 1
!

E. Configure two calling party transformation patterns:
\+1917.XXXXXXX, strip pre-dot, numbering type: subscriber
\+1.!, strip pre-dot, numbering type: national

ANSWER: C E

Explanation:

The correct solutions are the called-party transformation patterns and the calling-party transformation patterns that each distinguish New York local numbers from other North American national numbers. The pattern `\+1917.XXXXXXX` identifies an E.164 number for the local New York area code. Using *strip pre-dot* removes the `+1917` portion and retains the seven-digit subscriber number, which is the appropriate local presentation for calls within that area. Setting the numbering type to subscriber also accurately describes the resulting number format. The `\+1.!` pattern handles other NANP destinations or callers by removing only `+1`, leaving the area code and subscriber number in national format; its numbering type is therefore national. Both transformations are required because Cisco Unified Communications Manager independently normalizes and transforms called-party and calling-party information on outbound routing. Applying equivalent logic to each party ensures that the PSTN gateway receives a locally valid destination number and a properly localized calling number. Cisco dial-plan guidance recommends maintaining globalized E.164 format internally and applying localized transformations at the egress point: Cisco Collaboration SRND—Dial Plan. Cisco also documents calling and called party transformation behavior in the Cisco Unified CM Administration Guide.

QUESTION NO: 33

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: C D

Explanation:

CLI connectivity to a Cisco IP Phone 7800 Series is provided through Secure Shell, so Cisco Unified Communications Manager must both permit the SSH service and supply usable SSH credentials to the phone. Enabling SSH Access in the phone's Product Specific Configuration Layout instructs the phone to enable its SSH server after it receives and applies its configuration from Cisco UCM. The engineer must also set a username and password in the Secure Shell Information fields. Those credentials are required when establishing the SSH session to the phone CLI. Because the phone is already reachable by ICMP and HTTP and successfully registered, basic IP connectivity and phone registration are present; the remaining configuration needed is specifically the SSH service enablement and its authentication details. After the changes are saved and applied, the phone may need to obtain its updated configuration, such as through a reset, before the CLI can be accessed with the configured SSH credentials. Cisco's Cisco IP Phone 7800 Series administration documentation is available from the Cisco 7800 Series maintenance and administration guides. Cisco also documents phone configuration administration in the Cisco IP Phone 7800 Series Administration Guide for Cisco Unified Communications Manager.

QUESTION NO: 34

How does Cisco Unity Connection determine which call routing rule to use when more than one rule could apply to an incoming call?

A. It uses the first matching rule in the configured order.

B. It uses the matching rule with the longest called number.

C. It uses the rule that was most recently modified.

D. It applies all matching rules in sequence.

ANSWER: A

Explanation:

Cisco Unity Connection evaluates call routing rules in the configured order and uses the first rule whose conditions match the call. Administrators can therefore place more-specific rules above broader rules to ensure that calls from particular numbers, schedules, or dialed numbers receive the intended treatment.

After a matching rule is selected, Unity Connection applies the configured call handler, directory handler, conversation, or other routing action associated with that rule. Rules lower in the list are not evaluated after a match is found.

QUESTION NO: 35

Endpoint A is attempting to call endpoint

B. Endpoint A only supports G.711ulaw with a packetization rate of 20 ms, and endpoint B supports packetization rate of 30 ms for G.711ulaw. Which two media resources are allocated to normalize packetization rates through transrating? (Choose two.)

A. software transcoder on Cisco UCM

B. hardware transcoder on Cisco IOS Software

C. software MTP on Cisco IOS Software

D. software MTP on Cisco UCM

E. hardware MTP on Cisco IOS Software

ANSWER: D E

Explanation:

Transrating is required when endpoints use the same codec but use different packetization periods, as in this G.711 μ-law call using 20-ms and 30-ms packets. A Media Termination Point performs the needed RTP stream termination and repacketization, allowing Cisco Unified Communications Manager to present each endpoint with media in its supported packetization interval. The Cisco Unified CM software MTP supports G.711 media and can provide this packetization-rate normalization. A Cisco IOS hardware MTP, which uses DSP resources on the IOS gateway or media-resource platform, also provides MTP services for RTP stream handling and transrating. In both cases, the codec remains G.711 μ-law; the media resource normalizes the packet timing and packet size rather than changing the codec. Cisco documents MTPs as media resources that terminate and re-originate RTP streams, including for packetization-period incompatibilities, while hardware MTP capacity is delivered through DSP-based IOS media resources. See Cisco's Collaboration SRND media-resources guidance and the Cisco Unified Communications Manager documentation portal.

QUESTION NO: 36

Which recommendation is the best practice for marking video and voice media in a Cisco Unified Communications network?

A. Voice Cos 5 (IP Precedence 6, PHB AF41, or DSCP 16) Video Cos 4 (IP Precedence 5, PHB EF, or DSCP 32)

B. Voice Cos 6 (IP Precedence 4, PHB AF41, or DSCP 24) Video Cos 5 (IP Precedence 4, PHB EF, or DSCP 34)

C. Voice Cos 5 (IP Precedence 2, PHB EF, or DSCP 48)
Video Cos 4 (IP Precedence 4, PHB AF41, or DSCP 46)

D. Voice Cos 5 (IP Precedence 5, PHB EF, or DSCP 46)
Video Cos 4 (IP Precedence 4, PHB AF41, or DSCP 34)

ANSWER: D

Explanation:

Voice Cos 5 (IP Precedence 5, PHB EF, or DSCP 46)
Video Cos 4 (IP Precedence 4, PHB AF41, or DSCP 34)

This marking scheme follows Cisco's differentiated QoS model for real-time collaboration media. Voice bearer traffic is highly sensitive to delay, jitter, and loss, so it is marked with Expedited Forwarding (EF), represented by DSCP 46. EF maps to IP Precedence 5 and Layer 2 Class of Service (CoS) 5, allowing network devices to identify voice media for low-latency treatment. Video media also needs preferential handling, but Cisco recommends a separate assured-forwarding class rather than placing it in the strict-priority voice class. Interactive video is marked AF41, represented by DSCP 34, which maps to IP Precedence 4 and CoS 4. This classification preserves distinct queues and policies for voice and video, helping protect voice quality while providing video with appropriate bandwidth, loss handling, and congestion treatment. The markings should be trusted or set consistently at the network edge and carried end-to-end through switches, routers, WAN links, and policy boundaries. Cisco documents these voice and video media marking recommendations in its collaboration and QoS design guidance: Cisco Collaboration SRND and Cisco QoS SRND.

QUESTION NO: 37

Which Cisco unity Connection handler plays a greeting at announces the option to dial a user extension by default?

A. the operator call handler

B. the Interview handler

C. the Goodbye call handler

D. the Directory handler

ANSWER: A

Explanation:

The operator call handler is correct. Cisco Unity Connection includes this predefined system call handler to provide callers with an operator-assistance path. Its default greeting is designed to tell callers that they can dial a user extension directly or remain on the line to be transferred to the operator. This behavior supports a common auto-attendant workflow: callers who know an extension can enter it immediately, while callers who need assistance can wait for the configured operator transfer. The handler can be customized in Unity Connection Administration, including its greeting, extension-dialing behavior, transfer destination, schedules, and transfer rules; however, the question asks for the default behavior of the predefined handler. The default operator call handler therefore matches both required elements: it plays a greeting and announces the direct-extension dialing option. Cisco's Unity Connection administration documentation describes the built-in call handlers and the configuration of caller input and transfer behavior, while Cisco's product documentation index provides version-specific administration guides. See Cisco Unity Connection Administration Guide and Cisco Unity Connection configuration guides.

QUESTION NO: 38

An engineer is asked to implement on-net/off-net call classification in Cisco UCM. Which two components are required to implement this configuration? (Choose two.)

A. CTI route point

B. SIP route patterns

C. route group

D. route pattern

E. SIP trunk

ANSWER: D E

Explanation:

route pattern and **SIP trunk**
are required because Cisco Unified Communications Manager applies on-net or off-net classification as part of call routing and then sends the call to the selected SIP-based egress connection. The route pattern is the dial-plan object that matches the dialed number and provides the route configuration, including the Call Classification setting. Setting that value to OnNet or OffNet identifies how Unified CM should treat the call for routing features and policies that rely on whether a destination is internal to the enterprise dial plan or external.

A SIP trunk provides the signaling path to the next SIP entity, such as a service provider, CUBE, gateway, or another call-control system. After the route pattern is matched, Unified CM can select the SIP trunk as the route destination, allowing the classified call to leave Unified CM using SIP. This pairing makes the classification actionable: the route pattern establishes the call's classification, while the SIP trunk supplies the SIP egress connectivity used for the routed call. Cisco documents route patterns as core route-plan objects and SIP trunks as the device type used for SIP call routing. See the Cisco Unified CM System Configuration Guide and the Cisco Unified Communications Manager documentation.

QUESTION NO: 39

Which two approaches are taken to implement CAC within Cisco UCM in full-mesh topology? (Choose two.)

A. physical location

B. Audio Codec Preference List

C. location-based CAC

D. RSVP-enabled locations

E. device pool

ANSWER: C D

Explanation:

Cisco Unified Communications Manager supports two principal call-admission-control approaches for controlling WAN bandwidth in a full-mesh deployment: location-based CAC and RSVP-enabled locations. Location-based CAC uses configured audio and video bandwidth values for Locations and Location Links. When Unified CM processes a call between locations, it evaluates the available interlocation bandwidth and admits the call only when sufficient bandwidth remains. This provides a centralized, configuration-driven method of limiting real-time media usage across WAN links.

RSVP-enabled locations extend CAC by using Resource Reservation Protocol signaling to request and reserve bandwidth through RSVP-capable network devices for an individual call. Unified CM can use the RSVP reservation outcome when deciding whether the call's media path can be admitted. This approach is particularly useful when the network infrastructure supports RSVP and the deployment requires call-by-call bandwidth reservation rather than relying solely on administratively configured bandwidth values. Cisco documents both Locations-based CAC and RSVP-based CAC as Unified CM bandwidth-management mechanisms. See Cisco's Unified CM System Configuration Guide and its Feature Configuration Guide.

QUESTION NO: 40

What are the QoS requirements for voice and video calls over an a Cisco MPLS VPN?

A. less than or equal to 150 ms of one-way latency

B. less than or equal to 60 ms jitter

C. less than or equal to 300 ms of one-way latency

D. less than or equal to 10 percent packet loss

ANSWER: A

Explanation:

"less than or equal to 150 ms of one-way latency" is correct because interactive real-time media is highly sensitive to end-to-end delay. Cisco uses 150 ms as the recommended maximum one-way delay target for voice traffic, based on ITU-T guidance, because delays at or below this level generally preserve natural conversational interaction. The one-way measurement is important: it represents the delay experienced by media traveling from a talker or camera source to the receiving endpoint, including serialization, propagation, processing, and queuing delay across the MPLS VPN path. QoS policy on the WAN should therefore prioritize real-time RTP media into an appropriately provisioned low-latency treatment so congestion does not introduce excessive queueing delay. The same latency target is relevant to interactive video, where timely delivery of audio and video is necessary to maintain a usable call experience. Cisco's enterprise QoS design guidance identifies one-way delay of 150 ms or less as the recommended performance objective for real-time traffic. See Cisco's Enterprise QoS Solution Reference Network Design and the ITU-T G.114 transmission-time recommendation.

QUESTION NO: 41

In the cisco expressway solution, which two features does mobile and Remote access provide? (Choose two)

A. VPN-based enterprise access for a subset of Cisco Unified IP Phone models

B. secure reverse proxy firewall traversal connectivity

C. the ability 10 register third-party SIP or H 323 devices on Cisco UCM without requiring VPN

D. the ability of Cisco IP Phones to access the enterprise through VPN connection

E. the ability for remote users and their devices to access and consume enterprise collaboration applications and services

ANSWER: B E

Explanation:

Cisco Expressway Mobile and Remote Access provides **secure reverse proxy firewall traversal connectivity** by using the Expressway-C/Expressway-E architecture. Expressway-E is placed at the network edge and securely brokers signaling and media-related access between internet-based clients or supported endpoints and the internal collaboration environment, while avoiding direct exposure of internal Unified Communications services. This architecture enables authenticated, encrypted remote connectivity through the perimeter firewall.

It also provides **the ability for remote users and their devices to access and consume enterprise collaboration applications and services**. For example, users outside the corporate network can use supported Cisco collaboration clients and endpoints to register to Unified CM and use services such as calling, messaging, presence, voicemail, and meetings, subject to the organization's configured services and licensing. A key purpose of MRA is to extend these enterprise collaboration capabilities to external networks without requiring the user to first establish a traditional VPN tunnel. Cisco documents MRA as a secure remote-access solution for collaboration users and supported devices through Expressway.

References: Cisco Expressway Configuration Guide; Cisco Expressway installation and configuration guides.

QUESTION NO: 42

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

A. real-time alarm browse

B. multicluster support

C. call quality monitoring

D. email notifications

E. customizable events

ANSWER: B C

Explanation:

In Cisco Prime Collaboration Assurance's licensing model, **multicluster support** is an Advanced-license capability because it extends Assurance management beyond a single Cisco Unified Communications Manager cluster. This capability is intended for larger or distributed collaboration deployments where centralized visibility across multiple clusters is needed. **Call quality monitoring** is also an Advanced-license capability. It provides the quality-focused monitoring and troubleshooting functions needed to assess call-media performance, identify degraded voice or video experience, and investigate quality issues using call-related data. These functions go beyond the foundational fault and performance-management functions supplied with the Standard tier. Cisco's Prime Collaboration Assurance documentation distinguishes the Standard and Advanced feature sets and describes how licensing controls the available Assurance monitoring capabilities. Review the Cisco Prime Collaboration Assurance Guide and the Cisco Prime Collaboration product documentation for the product's licensing and feature context.

QUESTION NO: 43

An engineer must deploy the Cisco Webex app to a Virtual Desktop Infrastructure (VDI) environment and support full-featured meetings. Which action must the engineer take to meet these requirements?

A. Configure the VDI thin client and install the Webex app

B. From Control Hub. configure VDI optimization for the Webex app

C. Install three separate VDI plugins on the VDI thin client

D. Install two separate VDI plugins on the VDI thin client

ANSWER: D

Explanation:

Install two separate VDI plugins on the VDI thin client. A Webex App VDI deployment consists of the Webex App installed on the hosted virtual desktop and supporting plugin software installed locally on the user's thin client. The local plugin establishes the optimized media path between the endpoint and Webex services, preventing real-time audio, video, and screen-sharing media from being unnecessarily processed through the virtual desktop.

For full-featured meetings, the thin client needs both the Webex App VDI plugin and the Webex Meetings VDI plugin. The Webex App VDI plugin provides optimization for Webex App functionality, while the Meetings VDI plugin enables the VDI-specific media optimization needed for Webex meetings features. Installing both components ensures that meeting media is handled by the local endpoint while the virtual desktop continues to provide the application interface and signaling context. Cisco documents the VDI architecture, required client-side plugin installation, and the additional Meetings plugin requirement for full meeting functionality in its Webex App for VDI deployment guide and Webex Meetings VDI documentation.

QUESTION NO: 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: B E

Explanation:

Cisco Expressway Mobile and Remote Access is designed to extend on-premises Cisco collaboration services securely to users and supported endpoints that are outside the corporate network. The feature described as *secure reverse proxy firewall traversal connectivity* is provided by the Expressway-C and Expressway-E pair: Expressway-E is deployed at the network edge and provides a secure traversal path through the firewall, while Expressway-C integrates that remote access path with internal Unified Communications services. This architecture allows remote connections without exposing internal collaboration servers directly to the public Internet.

The feature described as *the ability for remote users and their devices to access and consume enterprise collaboration applications and services* is also central to MRA. Supported clients and endpoints can use services such as Cisco Unified Communications Manager calling, instant messaging and presence, voicemail, directory access, and conferencing while away from the enterprise network. MRA uses secure signaling and media mechanisms and is intended to avoid the operational burden of requiring a traditional VPN for supported collaboration access. Cisco documents MRA as an edge solution for remote access to collaboration services and describes its secure firewall-traversal role in the Cisco Collaboration Edge CVD and the Cisco Expressway MRA Deployment Guide.

QUESTION NO: 45

A customer reports that the load balancing solution is not working (or two Cisco Unified Border Element routers. The (cube1.abc.com) router should take 60% of the calls, and the (cube2 abc.com) router should take 40% of the calls. Assuming all DNS A records are present, which two SRV configurations would provide the desired outcome? (Choose two.)

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

ANSWER: B C

Explanation:

The two selected SRV configurations provide the required distribution because both Cisco Unified Border Element targets are in the same SRV priority group and their SRV weights produce a 60:40 ratio. DNS SRV priority controls failover preference: a client uses target records with the lowest numerical priority first. When multiple usable records have that same priority, the client uses their relative weights to select a target. Therefore, a weight ratio of 60 to 40 produces an expected distribution of approximately 60 percent of calls to `cube1.abc.com` and 40 percent to `cube2.abc.com`. An equivalent proportional ratio, such as 3 to 2, produces the same expected 60/40 result because SRV weights are relative rather than absolute. This behavior supports load sharing while retaining the ability to use a separate, higher-priority-number SRV group for backup service if needed. DNS A records remain necessary so each selected SRV target hostname can be resolved to its address. The SRV priority and weighted-selection behavior is defined in RFC 2782. Cisco's CUBE documentation also covers DNS-based destination resolution and dial-peer behavior in the Cisco Unified Border Element Configuration Guide.

QUESTION NO: 46

An engineer configures a SIP trunk for MWI between a Cisco UCM cluster and Cisco Unity Connection. The Cisco UCM cluster fails to receive the SIP notify messages. Which two SIP trunk settings resolve this issue? (Choose two.)

A. accept out-of-dialog refer

B. accept out-of-band notification

C. transmit security status

D. allow changing header

E. accept unsolicited notification

ANSWER: A E

Explanation:

For a Cisco Unity Connection SIP integration, the SIP trunk security profile on Cisco Unified Communications Manager must allow the signaling behaviors used by Unity Connection. Enabling **accept unsolicited notification** permits Unified CM to receive NOTIFY requests that are not associated with a previously established SIP subscription dialog. This is essential for Unity Connection message-waiting indication delivery: Unity Connection sends SIP NOTIFY messages to update the MWI state for a user's associated phone or directory number, and Unified CM must be configured to accept those notifications.

Enabling **accept out-of-dialog refer** permits Unity Connection to send REFER signaling outside an existing SIP dialog when required by the integration. Cisco's Unity Connection SIP integration guidance identifies both settings as required selections in the SIP trunk security profile used between Unified CM and Unity Connection. Applying these settings to the security profile assigned to the Unity Connection SIP trunk allows the cluster to accept the relevant inbound SIP signaling and process Unity Connection MWI updates. See Cisco's Unity Connection SIP integration documentation and the Cisco Unified CM System Configuration Guide.

QUESTION NO: 47

An administrator is developing an 8-class QoS baseline model. The CS3 standards-based marking recommendation is used for which type of class?

A. Scavenger

B. best effort

C. voice

D. call signaling

ANSWER: D

Explanation:

The correct class is **call signaling**. In Cisco's QoS Baseline model, call-signaling traffic is marked with Class Selector 3 (CS3), whose Differentiated Services Code Point value is 24. Call signaling includes the control-plane messages that establish, maintain, modify, and tear down voice or video calls, such as SIP signaling. Marking this traffic CS3 provides a consistent, standards-based identifier that network devices can use to classify it and apply an appropriate assured-forwarding treatment. This is important because timely signaling delivery is necessary for reliable call setup and ongoing call control; signaling must be protected from congestion, although it does not have the same low-latency forwarding requirements as the media stream itself. Cisco's enterprise QoS guidance maps the call-signaling class to CS3 as part of the recommended multi-class QoS policy design. The DSCP Class Selector code-point definition also establishes that CS3 corresponds to a precedence value of 3, making it suitable for this prioritized control traffic classification. See Cisco's Enterprise QoS Solution Reference Network Design and the IETF Differentiated Services Field RFC.

QUESTION NO: 48

Which protocols does Cisco IM and Presence use to authenticate Jabber?

A. XMPP

B. SOAP

C. TCP

D. LDAP

E. QBE

ANSWER: A B

Explanation:

Cisco Jabber authentication with the Cisco IM and Presence Service uses both XMPP and SOAP. XMPP is the core client-to-presence protocol used by Jabber to establish its instant-messaging and presence session with the IM and Presence Service. After the client is authenticated, this XMPP session carries presence information, instant messages, contact-list-related data, and other real-time collaboration signaling.

SOAP is also used by Jabber for service interactions associated with authentication and client configuration. In Cisco Collaboration deployments, Jabber communicates with Cisco Unified Communications Manager and IM and Presence web services over HTTPS using SOAP-based requests. These exchanges support the client sign-in workflow and retrieval of the service and configuration information needed to connect to the collaboration environment. Therefore, both protocols are relevant to the Jabber authentication process: XMPP provides the authenticated IM and presence session, while SOAP supports the associated authentication and service/configuration exchanges. Cisco's Jabber documentation and collaboration product documentation describe Jabber as an XMPP-based IM and presence client that integrates with Cisco Unified Communications Manager and IM and Presence services through web-service interfaces. See the Cisco Jabber product page and Cisco's Unified Communications Manager configuration guides.

QUESTION NO: 49

There is a saturated link that has traffic shaping configured. How is incoming traffic processed?

A. Traffic is compressed so that the traffic fits within the bandwidth of the link.

B. Excess traffic is queued, and then dropped after the timer expires.

C. Excess traffic is queued for later transmission.

D. Excess traffic is dropped.

ANSWER: C

Explanation:

Traffic shaping is a congestion-management mechanism that regulates the rate at which traffic is transmitted onto a link. When packets arrive faster than the configured shaping rate permits, the device does not immediately discard the excess solely because it exceeds that rate. Instead, it places the excess packets into a shaping queue and schedules them for transmission when sufficient bandwidth is available under the configured rate. This smooths bursts and helps ensure that the egress traffic rate conforms to the service level or bandwidth contract. Therefore, *Excess traffic is queued for later transmission.* is correct. Shaping is normally applied in the outbound direction, because a device can control when it sends packets but cannot directly control the rate at which packets arrive from a neighboring device. Queued traffic can ultimately be dropped if the queue reaches its configured capacity, but this is a buffer-exhaustion condition rather than the normal shaping behavior. Cisco describes shaping as buffering traffic that exceeds the configured rate and releasing it later at the desired rate. See Cisco's Traffic Policing and Traffic Shaping Comparison and the Cisco IOS Traffic Shaping documentation.

QUESTION NO: 50

An administrator configures the voicemail feature in a Cisco collaboration deployment. The user mailboxes must be configured when the Cisco Unity Connection server is configured. Which action accomplishes this task?

A. Configure an SCCP integration with Cisco UCM.

B. Configure a SIP integration with Cisco UCM to sync users.

C. Configure an AXL server to access the Cisco UCM users.

D. Configure an active directory to sync the users who will have a voicemail box.

ANSWER: C

Explanation:

Configure an AXL server to access the Cisco UCM users. Cisco Unity Connection integrates with Cisco Unified Communications Manager to import and synchronize user information through the Administrative XML Layer (AXL) API. During the integration configuration, the administrator identifies the Unified CM server and supplies credentials for an account with the required AXL permissions. Unity Connection can then query Unified CM for end-user data and synchronize the selected users into its own database. The imported users can be assigned a voicemail user template, which supplies mailbox-related settings such as the class of service, greeting behavior, and mailbox policies. This approach centrally uses the Unified CM user population while allowing Unity Connection to create and manage the associated voicemail accounts. AXL is Cisco Unified CM's programmatic administrative interface and is specifically used by integrated applications, including Unity Connection, to retrieve and synchronize configuration data. Cisco documents the AXL API and its role in Unified CM administration at Cisco Unified Communications Manager AXL API. Cisco Unity Connection deployment and integration documentation is available from the Cisco Unity Connection Installation and Configuration Guides.

QUESTION NO: 51

An engineer is integrating Unity Connection with Cisco UCM. Which two actions must be configured so that recording and playback from the IP phones works at all times, including peak traffic hours? (Choose two.)

A. Increase the number of voice ports.

B. If it's a Unity Connection Cluster, ensure that replication is fine and not in split-brain mode.

C. The phone system to which the phones are registered in Unity Connection has the Default Trap Switch check box enabled.

D. Add dedicated dial-out ports with the allow trap connections setting selected.

E. Ensure that you have set up SIP Digest Authentication on the SIP trunk security profile.

ANSWER: A D

Explanation:

Increase the number of voice ports. is required because Unity Connection uses voice ports to process active telephony calls. Telephone recording and playback consume port resources while a caller is interacting with the Unity Connection conversation. The deployment must therefore be sized with enough ports to cover the expected busy-hour call volume, including concurrent message access and recording activity. Adequate port capacity prevents callers from being denied service when utilization rises.

Add dedicated dial-out ports with the allow trap connections setting selected. is also required to provide reliable Telephone Record and Playback (TRAP) functionality. TRAP connections support phone-based recording and playback operations, and dedicating appropriately configured ports ensures those operations have resources available rather than competing entirely with other Unity Connection call-processing demands. Together, capacity planning for voice ports and explicitly enabling TRAP-capable dedicated ports provide consistent phone conversation access during peak traffic periods. Cisco Unity Connection administration and deployment guidance is available in the Cisco Unity Connection Administration Guide and the Unity Connection installation and configuration guide library.

QUESTION NO: 52

Users want their mobile phones to be able to access their Cisco Unity Connection mailboxes with only having to enter their voicemail pin at the login prompt when calling the pilot number. Where should an engineer configure this feature?

A. alternate extensions

B. message settings

C. transfer rules

D. greetings

ANSWER: A

Explanation:

alternate extensions is the correct configuration location. In Cisco Unity Connection, an alternate extension associates an additional telephone number with a user mailbox. An engineer can add each user's mobile-phone number as an alternate extension on that user's account. When the user calls the Unity Connection pilot number from that mobile device, Unity Connection uses the incoming caller ID to identify the associated mailbox. Because the caller is recognized as belonging to that user, the conversation can proceed directly to PIN authentication rather than requiring the caller to first enter an extension or user ID. This supports a practical and secure mobile voicemail-access workflow while retaining PIN-based authentication for mailbox access. The mobile carrier and calling path must present a caller ID that matches the configured alternate extension, including any required dialing-format considerations. Cisco documents alternate extensions as the mechanism for associating additional phone numbers with a Unity Connection user and enabling recognition of calls from those numbers. See Cisco's Unity Connection Administration Guide and the Cisco Unity Connection User Guide resources.

QUESTION NO: 53 - (SIMULATION)

-

Guidelines

-

This is a lab item in which tasks will be performed on virtual devices.

• Refer to the Tasks tab to view the tasks for this lab item.

• Refer to the Topology tab to access the device console(s) and perform the tasks.

• Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.

• All necessary preconfigurations have been applied.

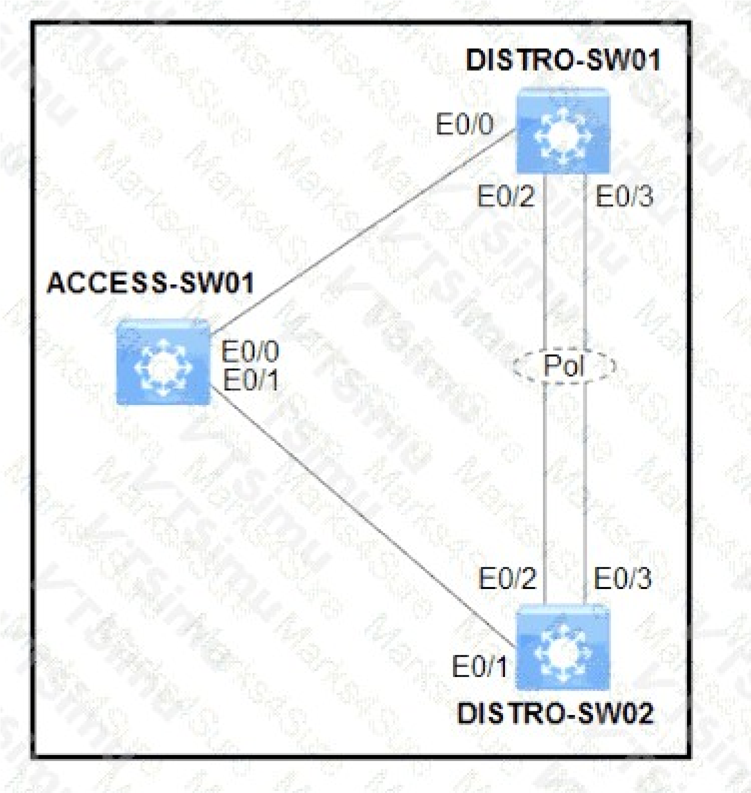
• Do not change the enable password or hostname for any device.

• Save your configurations to NVRAM before moving to the next item.

• Click Next at the bottom of the screen to submit this lab and move to the next question.

• When Next is clicked, the lab closes and cannot be reopened.

Topology



Tasks

-

The operations team started configuring network devices for a new site.

Complete the configurations to achieve these goals:

1. Ensure that port channel Po1 between DISTRO-SW01 and DISTRO-SW02 is operational using the LACP protocol. Configuration changes for this task must be made on DISTRO-SW01.

2. Ensure that traffic on VLAN 10 is carried as untagged traffic between DISTRO-SW01 and DISTRO-SW02.

3. Complete the Rapid-PVST+ configuration on DISTRO-SW2 by ensuring it it the secondary root switch for all VLANs in the range of 1 to 1005.

DISTRO-SW01

```
DISTRO-SW01>
DISTRO-SW01>
DISTRO-SW01>en
DISTRO-SW01#config t
Enter configuration commands, one per line. End with CNTL/Z.
DISTRO-SW01(config)# in
DISTRO-SW01(config)# interface e0/0
DISTRO-SW01(config-if)#no cha
DISTRO-SW01(config-if)#no channel-g
DISTRO-SW01(config-if)#no channel-group 1
DISTRO-SW01(config-if)#no channel-group 1 mo
DISTRO-SW01(config-if)#no channel-group 1 mode pas
DISTRO-SW01(config-if)#no channel-group 1 mode passive
DISTRO-SW01(config-if)#
* Jul 10 20:07:53.469: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0,
changed state to up
DISTRO-SW01(config-if)#
DISTRO-SW01(config-if)#exit
DISTRO-SW01(config)#
DISTRO-SW01(config)# in
DISTRO-SW01(config)# interface ran
DISTRO-SW01(config) # interface range e
DISTRO-SW01(config)# interface range ethernet 0/2-3
DISTRO-SW01(config-if-range)#ch
DISTRO-SW01(config-if-range)#channel-gr
DISTRO-SW01(config-if-range)#channel-group 1
DISTRO-SW01(config-if-range)#channel-group 1 mo
DISTRO-SW01(config-if-range)#channel-group 1 mode ac
DISTRO-SW01(config-if-range)#channel-group 1 mode active
DISTRO-SW01(config-if-range)#
* Jul 10 20:08:25.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2,
changed state to up
* Jul 10 20:08:25.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3,
changed state to up
DISTRO-SW01(config-if-range)#exit
DISTRO-SW01(config)#
* Jul 10 20:08:31.447: %LINK-3-UPDOWN: Interface Port-channel, changed state to up
* Jul 10 20:08:32.451: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3,
changed state to up
DISTRO-SW01(config)#
DISTRO-SW01(config)#exit
DISTRO-SW01#
* Jul 10 20:08:39.212: %SYS-5-CONFIG_I: Configured from console by console
DISTRO-SW01#sh eth
DISTRO-SW01#sh etherc
DISTRO-SW01#sh etherchannel s
DISTRO-SW01#sh etherchannel summary
```

```
DISTRO-SW01#sh etherchannel s
DISTRO-SW01#sh etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregate

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

      A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group   Port-channel  Protocol  Ports
------+-------------+---------+----------
1     Po1(SU)        LACP      Et0/2(P)  Et0/3(P)
```

```
DISTRO-SW01#
DISTRO-SW01# config t
Enter configuration commands, one per line. End with CNTL/Z.
DISTRO-SW01(config)#inte
DISTRO-SW01(config)#interface po
DISTRO-SW01(config)#interface port-
DISTRO-SW01(config)#interface port-channel 1
DISTRO-SW01(config-if)#sw
DISTRO-SW01(config-if)#switchport tr
DISTRO-SW01(config-if)#switchport trunk na
DISTRO-SW01(config-if)#switchport trunk native vl
DISTRO-SW01(config-if)#switchport trunk native vlan 10
DISTRO-SW01(config-if)#
* Jul 10 20:09:27.352: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on Ethernet0/3 (10), with DISTRO-SW02 Ethernet0/3 (1).
DISTRO-SW01(config-if)#
* Jul 10 20:09:27.857: %SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent
peer vlan id 1 on Port-channel1 VLAN10.
* Jul 10 20:09:27.857: %SPANTREE-2-BLOCK_PVID_PEER: Blocking Port-channel1 on
VLAN0001. Inconsistent peer vlan.
* Jul 10 20:09:27.857: %SPANTREE-2-BLOCK_PVID_LOCAL: Blocking Port-channel1 on
VLAN0010. Inconsistent local vlan.
DISTRO-SW01(config-if)#
```

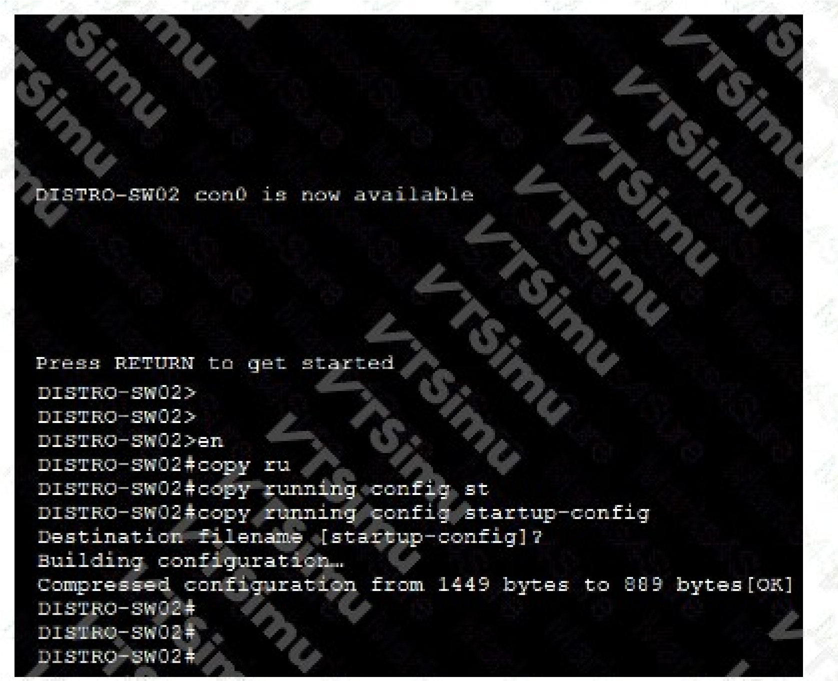
```
* Jul 10 20:09:27.857: %SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan
id 1 on Port-channel1 VLAN10.
* Jul 10 20:09:27.857: %SPANTREE-2-BLOCK_PVID_PEER: Blocking Port-channel1 on VLAN0001.
Inconsistent peer vlan.
* Jul 10 20:09:27.857: %SPANTREE-2-BLOCK_PVID_LOCAL: Blocking Port-channel1 on VLAN0010.
Inconsistent local vlan.
DISTRO-SW01(config-if)#
* Jul 10 20:09:30.710: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on Ethernet0/2 (10), with DISTRO-SW02 Ethernet0/2 (1).
DISTRO-SW01(config-if)#
* Jul 10 20:10:03.864: %SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking Port-channel on
VLAN0001. Port consistently restored
* Jul 10 20:10:03.864: %SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking Port-channel on
VLAN0010. Port consistently restored
DISTRO-SW01(config-if)#
DISTRO-SW01(config-if)#exit
DISTRO-SW01(config)#
DISTRO-SW01(config)#exit
DISTRO-SW01#co
DISTRO-SW01#co
* Jul 10 20:10:35.644: %SYS-5-CONFIG_I: Configured from console by console
DISTRO-SW01#copy ru
DISTRO-SW01#copy running-config st
DISTRO-SW01#copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
Compressed configuration from 1447 bytes to 886 bytes[OK]
DISTRO-SW01#
DISTRO-SW01#
```

DISTRO-SW02

-

```
DISTRO-SW02>
* Jul 10 20:08:25.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2,
changed state to up
* Jul 10 20:08:25.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3,
changed state to up
DISTRO-SW02>
* Jul 10 20:08:31.447: %LINK-3-UPDOWN: Interface Port-channel, changed state to up
* Jul 10 20:08:32.448: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel,
changed state to up
DISTRO-SW02>
* Jul 10 20:09:27.848: %SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer
vlan id 10 on Port-channel1 VLAN1.
* Jul 10 20:09:27.848: %SPANTREE-2-BLOCK_PVID_PEER: Blocking Port-channel1 on VLAN0010.
Inconsistent peer vlan.
* Jul 10 20:09:27.857: %SPANTREE-2-BLOCK_PVID_LOCAL: Blocking Port-channel1 on VLAN0001.
Inconsistent local vlan.
DISTRO-SW02>
* Jul 10 20:09:31.330: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on Ethernet0/3 (1), with DISTRO-SW01 Ethernet 0/3 (10).
```

```
DISTRO-SW02>en
DISTRO-SW02#config t
Enter configuration commands, one per line, End with CNTL/Z.
DISTRO-SW02(config)#
DISTRO-SW02(config)#inter
DISTRO-SW02(config)#interface por
DISTRO-SW02(config)#interface port-ch
DISTRO-SW02(config)#interface port-channel 1
DISTRO-SW02(config)#interface port-channel 1
DISTRO-SW02(config-if)#sw
DISTRO-SW02(config-if)#switchport tr
DISTRO-SW02(config-if)#switchport trunk na
DISTRO-SW02(config-if)#switchport trunk native vl
DISTRO-SW02(config-if)#switchport trunk native vlan 10
DISTRO-SW02(config-if)#exit
DISTRO-SW02(config)#
DISTRO-SW02(config)#sp
DISTRO-SW02(config)#spanning-tree vl
DISTRO-SW02(config)#spanning-tree vlan 1-
* Jul 10 20:10:04.934: %SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking
Port-channel1 on VLAN0010. Port consistently restored.
* Jul 10 20:10:04.934: %SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking
Port-channel1 on VLAN0001. Port consistently restored.
DISTRO-SW02(config)#spanning-tree vlan 1-1005 ro
DISTRO-SW02(config)#spanning-tree vlan 1-1005 root se
DISTRO-SW02(config)#spanning-tree vlan 1-1005 root secondary
DISTRO-SW02(config)#exit
```



ANSWER: See the explanation for the answer

Explanation:

Configure the EtherChannel using the two inter-distribution links (E0/2 and E0/3), not E0/0. E0/0 connects toward the access switch, so remove its incorrect EtherChannel membership if present.

DISTRO-SW01

```
enable
configure terminal
interface ethernet0/0
 no channel-group 1 mode passive
exit
interface range ethernet0/2 - 3
 channel-group 1 mode active
exit
interface port-channel 1
 switchport trunk native vlan 10
end
copy running-config startup-config
```

The `mode active` setting makes Port-channel 1 use LACP. Setting VLAN 10 as the native VLAN causes VLAN 10 frames to traverse this trunk untagged.

DISTRO-SW02

```
enable
configure terminal
interface port-channel 1
 switchport trunk native vlan 10
exit
spanning-tree mode rapid-pvst
spanning-tree vlan 1-1005 root secondary
end
copy running-config startup-config
```

Configure the native VLAN on both ends of the port channel; otherwise STP blocks the channel because of a native-VLAN/PVID inconsistency. The root-secondary command makes DISTRO-SW02 the Rapid-PVST+ secondary root for every VLAN from 1 through 1005.

Optional validation:

```
show etherchannel summary
show interfaces trunk
show spanning-tree vlan 1 root
```

`show etherchannel summary` should show Po1 using `LACP`, with E0/2 and E0/3 bundled (`P`).

QUESTION NO: 54

Which two actions must be taken to provision a new device using the self-provisioning? (Choose two.)

A. Enable the self-provisioning IVR in the Cisco UCM.

B. Import the user profile to the corporate LDAP directory.

C. Link the appropriate universal device template to the user profile.

D. Ensure the user has a directory URI and a primary extension.

E. Link the appropriate service profile to the provisioning template.

ANSWER: A C

Explanation:

Cisco Unified Communications Manager self-provisioning relies on the Self-Provisioning IVR application and a Universal Device Template (UDT). Administrators must enable and configure the self-provisioning IVR in Cisco UCM so that eligible users can call the configured IVR pilot, authenticate with their user credentials and PIN, and initiate the automated device-provisioning workflow. The IVR is the user-facing mechanism that collects the provisioning request and triggers CUCM to create the device configuration.

Administrators must also link the appropriate universal device template to the user profile. The UDT supplies the standardized device settings CUCM applies when it creates the new phone, including the device pool, phone button template, calling search space, and other phone-specific defaults. Associating that UDT with the user profile ensures that CUCM can select the intended configuration when the user completes the IVR workflow. The user profile is then assigned to the applicable end users as part of the overall setup. Cisco documents self-provisioning configuration and the role of the IVR and UDT in its CUCM System Configuration Guide. Cisco's System Configuration Guide for Release 14 also describes the relevant user-management and provisioning configuration model.

QUESTION NO: 55

How does traffic policing respond to violations?

A. Excess traffic is queued.

B. All traffic is treated equally.

C. Excess traffic is dropped.

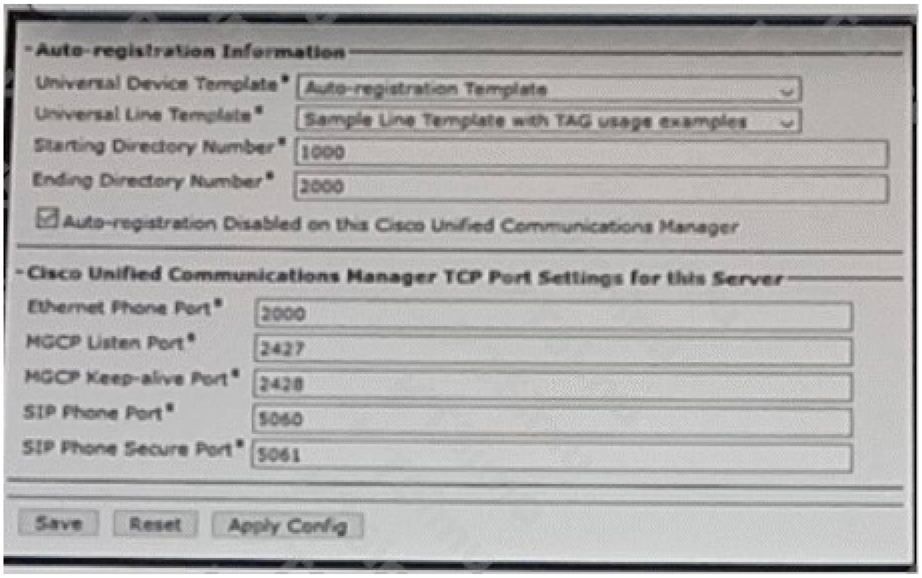
D. Excess traffic is retransmitted.

ANSWER: C

Explanation:

Traffic policing enforces a configured traffic-rate limit by measuring packets against a rate threshold, typically using a token-bucket mechanism. When traffic conforms to the configured rate, packets are forwarded normally. When packets exceed the configured policing parameters, the usual policing action is to drop the excess packets. This provides an immediate enforcement mechanism that prevents a flow from consuming bandwidth beyond its contracted or configured allowance. Cisco QoS policing can also be configured to mark packets differently based on whether they conform, exceed, or violate defined limits; however, when the question asks how policing responds to violations in the standard sense, dropping excess traffic is the expected behavior. Unlike traffic shaping, policing does not buffer excess packets to smooth the sending rate over time. It acts directly on packets at the point where the policy is applied, making it useful for enforcing service policies at network boundaries and protecting resources from traffic that exceeds an agreed rate. Cisco's comparison of policing and shaping describes policing as dropping packets that exceed the defined rate, whereas shaping delays packets by queuing them. See Cisco's Policing and Shaping Overview and the Cisco IOS XE QoS Policing and Shaping documentation.

QUESTION NO: 56



Refer to the exhibit. Which action must an engineer take to implement self-provisioning on a primary communications manager server?

A. Select a different Universal Line Template.

B. Change the SIP Phone Secure Port.

C. Uncheck the auto-registration Disabled checkbox.

D. Select a different Universal Device Template.

ANSWER: C

Explanation:

Uncheck the auto-registration Disabled checkbox. Cisco Unified Communications Manager self-provisioning depends on auto-registration so that an unconfigured phone can register with the specified Cisco Unified CM node. After registration, CUCM uses the self-provisioning configuration, including the selected Universal Device Template and Universal Line Template, to create and associate the device and line information for the user. When the Auto-registration Disabled setting remains selected, the server does not accept auto-registration requests, preventing a new phone from entering the self-provisioning workflow regardless of which universal templates are selected. The primary communications manager must therefore allow auto-registration before it can serve as the self-provisioning node. In a production deployment, the engineer should also ensure that the appropriate self-provisioning parameters and universal templates are already configured, then limit or disable auto-registration again when the controlled provisioning window is complete, consistent with the organization's endpoint-security practices. Cisco documents that self-provisioning uses auto-registration and that the Auto-registration Disabled parameter controls whether auto-registration is permitted on a CUCM node. See Cisco's System Configuration Guide and the Cisco Unified Communications Manager configuration guides.

QUESTION NO: 57

The security department will audit an IT department to ensure that the proper guidelines are being followed. The reports of the call detail records show unauthorized access to PSTN. Which two actions should an administrator check to prevent the unauthorized use of the telephony system? (Choose two.)

A. Ensure that ad hoc conference calls are dropped if an external user is add.

B. Call forward settings (ALL/Busy/No Answer) are restricted to internal extensions in the network

C. Add an additional firewall between the Cisco UCM server and the Expressway Core server.

D. For extension mobility, logged-out CSS is restricted to internal extensions and emergencies.

E. Forced authorization code is used to recognize a dialing extension and authorize an international call.

ANSWER: B E

Explanation:

Call forward settings (ALL/Busy/No Answer) are restricted to internal extensions in the network is correct because call forwarding can otherwise provide a path for toll fraud: a caller reaches an internal device and has the call forwarded to an external PSTN destination. Limiting forward destinations to on-net directory numbers prevents the Unified CM call-forward feature from becoming an unauthorized off-net relay. The restriction should be enforced through the applicable calling search spaces and partitions so that users cannot forward to route patterns or other PSTN-reachable destinations.

Forced authorization code is used to recognize a dialing extension and authorize an international call is also correct because Forced Authorization Codes require a caller to enter an approved code before Unified CM completes a call to a protected destination class, such as international PSTN routes. This creates an authorization control for expensive call types and permits the organization to track use through call records and authorization-code reporting. Administrators commonly apply FAC requirements to route patterns or translation patterns that reach restricted PSTN destinations. Cisco documents call-routing controls, including authorization and calling-search-space design, in its Unified Communications Manager documentation; Cisco's collaboration security guidance also emphasizes restricting calling privileges to mitigate toll-fraud exposure.

QUESTION NO: 58

Which call routing pattern is used for phone numbers that are in the E.164 format?

A. /+.! Route Pattern

B. \+.! Route pattern

C. \+.! Translation Pattern

D. \+1.[2-9]XX[2-9]XXXXXXX called Party Transformation Pattern

ANSWER: B

Explanation:

The **\+.! Route pattern** is used to route calls dialed in E.164 format in Cisco Unified Communications Manager. E.164 addressing represents a fully qualified, globally routable telephone number, beginning with a plus sign followed by a country code and the remaining destination digits. In a CUCM route pattern, the backslash escapes the plus sign so that CUCM treats it as the literal leading "+" in the dialed number. The period matches a digit, and the exclamation mark supports a variable-length sequence of subsequent digits. Consequently, **\+.!** matches globalized dial strings such as +12125551212 and allows CUCM to select the appropriate route list, route group, gateway, or SIP trunk for the destination. This is a common design for normalized dial plans because CUCM can retain the complete E.164 number through call routing and then apply any required digit transformation only at the egress point. Cisco documents route patterns as the dial-plan elements that match dialed digits and direct calls, including the use of pattern syntax and wildcards. See the Cisco Unified CM Administration Guide and Cisco's Unified Communications Manager configuration guides.

QUESTION NO: 59

A company has an excessive number of call transfers to local and long-distance PSTN from Cisco Unity Connection voicemail. Which action in the Cisco Unity Connection restriction table resolves this issue?

A. Block PSTN patterns on Default Transfer, Default Outdial, and Default System Transfer.

B. Implement password complexity on voicemail boxes to prevent accounts from being compromised.

C. Create a custom restriction table *********** and block it.

D. Create a custom restriction table ??????????? and block it.

ANSWER: A

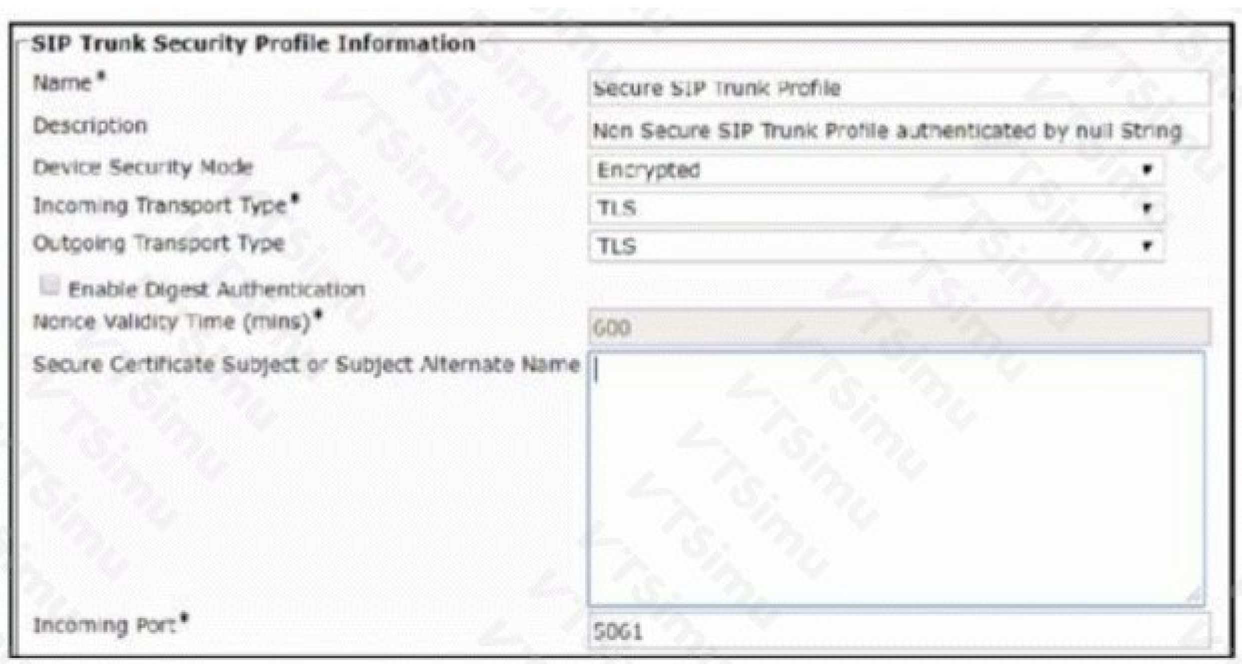
Explanation:

Block PSTN patterns on Default Transfer, Default Outdial, and Default System Transfer. Cisco Unity Connection uses restriction tables to control the dial strings that callers, subscribers, and system features can use when transferring or placing calls through Connection. Applying PSTN-blocking patterns to all three relevant default tables provides coverage for the primary ways Unity Connection can initiate an external call: a caller-directed transfer, an outdial operation, and a system-initiated transfer. This is important because restricting only one call path would leave other voicemail-related transfer mechanisms able to reach local or long-distance PSTN destinations.

The blocked patterns should match the organization’s external dialing plan, including any required PSTN access prefix and applicable local or long-distance number formats. Administrators can then retain explicitly required internal transfer patterns while preventing Unity Connection from being used to generate unauthorized or excessive PSTN transfers. Cisco documents restriction tables as the mechanism for limiting call-transfer and outdial destinations, and the Unity Connection administration documentation provides the applicable configuration guidance. See the Cisco Unity Connection configuration guides and the Cisco Unity Connection documentation resources.

QUESTION NO: 60

Refer to the exhibit.



An administrator configures a secure SIP trunk on Cisco UCM.

Which value is needed in the secure certificate subject or subject alternate name field to accomplish this task?

A. The fully qualified domain name of the remote device that is configured on the SIP trunk.

B. The common name of the Cisco UCM CallManager certificate.

C. The full qualified domain name of all Cisco UCM nodes that run the CallManager service.

D. The common name of the remote device certificates.

ANSWER: A

Explanation:

The fully qualified domain name of the remote device that is configured on the SIP trunk is required. For a secure SIP trunk, Cisco Unified Communications Manager validates the identity presented by the remote SIP peer during the TLS handshake. The identity entered for the trunk must match an identity carried by the peer certificate, either in its X.509 Subject field or in a Subject Alternative Name extension. In normal deployments, that identity is the peer's fully qualified domain name, such as `cubesbc.example.com`, because the SIP trunk is configured to reach that named remote system and the certificate is issued for that DNS identity.

This match binds the TLS connection to the intended SIP-trunk peer and allows Cisco UCM to verify that the endpoint presenting the certificate is the configured remote device. The remote device's certificate therefore must contain the same FQDN in its Subject or SAN, and the corresponding trusted issuing certificate chain must be available to Cisco UCM. Cisco documents SIP trunk TLS certificate identity validation and the required subject-name matching behavior in its Cisco Unified Communications Manager Security Guide and Cisco Unified Communications Manager configuration guides.

QUESTION NO: 61

Which behavior occurs when Cisco UCM has a CallManager group that consists of two subscribers?

A. Endpoints attempt to register with both subscribers in a load-balanced method.

B. Endpoints attempt to register with the bottom subscriber in the list.

C. Endpoints attempt to register with the top subscriber in the list.

D. If a subscriber is rebooted, endpoints deregister until the rebooted system is back in service.

ANSWER: C

Explanation:

Endpoints attempt to register with the top subscriber in the list. A Cisco Unified Communications Manager CallManager group is an ordered, prioritized list of up to three Unified CM servers that provides call-processing redundancy for assigned devices. The server displayed at the top of the group is the primary CallManager in the group and has the highest priority. When an endpoint using that device pool starts or needs to reestablish registration, it first attempts to register with this highest-priority subscriber. If that subscriber is unavailable, the endpoint proceeds through the remaining servers in the configured priority order, enabling failover without requiring the endpoint to remain unregistered until the preferred server returns. This behavior is driven by the CallManager group associated with the device pool assigned to the endpoint; the group is not a load-balancing mechanism for simultaneous registration across its listed subscribers. The ordered design lets an administrator define the normal call-processing server while retaining predictable backup registration behavior during a server failure or maintenance event. Cisco documents CallManager groups as prioritized server lists used by devices for registration and failover. See the Cisco Unified CM System Configuration Guide and the Cisco Unified CM Solution Reference Network Design guide.

QUESTION NO: 62

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

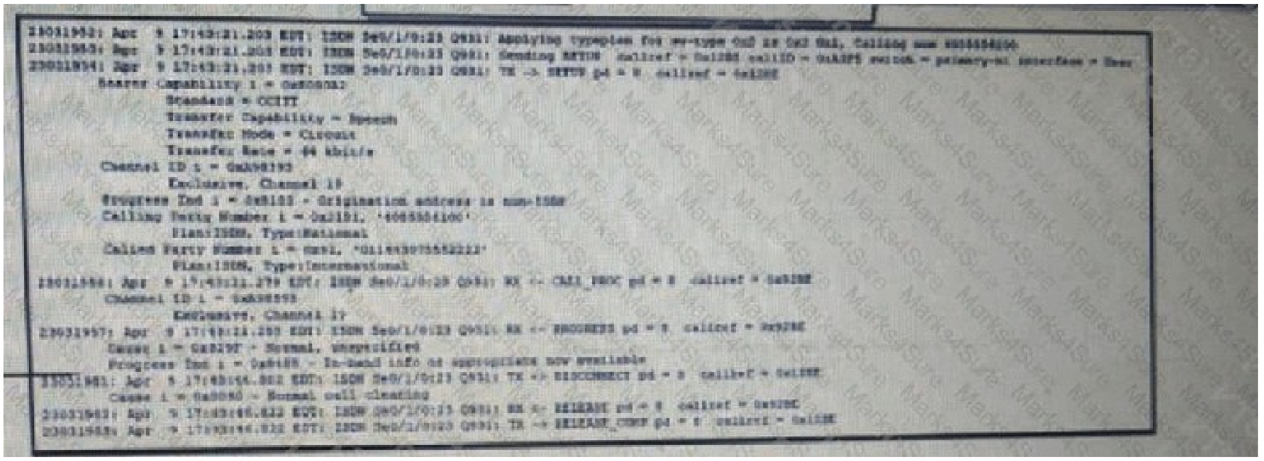
Explanation:

Confirm the phone load name in the phone configuration. A DX80 registered to Cisco Unified Communications Manager is provisioned by CUCM, which can specify the firmware load that the endpoint must run. Although an administrator can install a newer software image directly through the endpoint web interface, that local version does not override the load designated by CUCM. When the DX80 subsequently registers, restarts, or performs its scheduled provisioning check, it compares its installed image with the Phone Load Name configured for the device. If CUCM specifies the earlier load, the endpoint downloads and activates that assigned version, producing the apparent rollback observed the next morning.

The administrator should therefore review the DX80 device configuration in CUCM and ensure that the Phone Load Name is either set to the intended supported DX80 software load or left to inherit the appropriate current default device load. After the correct firmware is installed and selected in CUCM, the endpoint can be reset so it registers with—and remains on—the intended version. This aligns endpoint-side upgrades with the centrally managed firmware policy and prevents CUCM provisioning from restoring an older image. Cisco's CUCM configuration documentation is available in the [Cisco Unified Communications Manager configuration guides](); endpoint administration resources are available in the [Cisco Webex DX80 documentation]().

QUESTION NO: 63

Refer to the exhibit.



A call to an international number has failed. Which action corrects this problem?

A. Assign a transcoder to the MRGL of the gateway.

B. Strip the leading 011 from the called party number

C. Add the bearer-cap speech command to the voice port.

D. Add the isdn switch-type primart-dms100 command to the serial interface.

ANSWER: B

Explanation:

Strip the leading 011 from the called party number is correct because 011 is the North American international access code used by a caller to indicate an international destination. The PSTN-facing gateway or service-provider trunk must receive the digits in the format its dial plan expects. Where the provider expects the country code and national number rather than the enterprise access prefix, forwarding 011 causes the called number to be interpreted incorrectly and the call fails. Applying digit manipulation to remove the leading 011 produces the normalized outgoing number, beginning with the country code, while preserving all destination digits needed for international routing. In Cisco Unified Communications Manager, this can be implemented through route-pattern digit manipulation, such as a discard-digits instruction, or through an appropriate translation pattern, depending on the dial-plan design. Cisco recommends using route patterns and digit transformations to normalize numbers before they are sent to a gateway or trunk. See Cisco's route pattern administration documentation and its dial-plan transformation guidance.

QUESTION NO: 64

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: C E

Explanation:

The required SRV records are `_sip._udp.abc.com 60 IN SRV 1 60 5060 cube1.abc.com` and `_sip._udp.abc.com 60 IN SRV 1 40 5060 cube2.abc.com`. An SRV resource record uses the fields priority, weight, port, and target after the record type. To distribute calls between two targets rather than use one strictly as a backup, both CUBE targets must have the same priority. A DNS client selects only among targets with the lowest available priority; therefore, assigning priority `1` to both routers places them in the same load-sharing group.

Within that equal-priority group, the weight values determine the relative probability of selection. Weights of 60 for `cube1.abc.com` and 40 for `cube2.abc.com` provide a 60:40 selection ratio over a sufficiently large number of calls. Both records specify UDP SIP service through `_sip._udp` and use port 5060, the standard SIP UDP port. The target hostnames resolve through the assumed DNS A records. The SRV priority and weighted-selection behavior is defined in RFC 2782; SIP's use of SRV records is described in RFC 3263.

QUESTION NO: 65

A network administrator with ID0123456789 has determined that a WAN link between two Cisco UCM clusters supports only 1 Mbps of bandwidth for voice traffic. How many calls does this link support if G.711 as the audio codec is used?

A. 12

B. 13

C. 15

D. 16

ANSWER: A

Explanation:

12 is correct because Cisco Unified Communications Manager bandwidth management allocates approximately 80 kbps of WAN bandwidth per G.711 audio call. Although the G.711 codec payload itself is 64 kbps, a voice call also carries RTP, UDP, IP, and Layer 2 framing overhead. Cisco's call-admission-control calculation therefore uses 80 kbps as the standard bandwidth requirement for a G.711 call on an IP WAN link.

A 1 Mbps voice allocation represents 1,000 kbps of available bandwidth. Dividing 1,000 kbps by 80 kbps per call gives 12.5 calls. Because a partial call cannot be admitted and bandwidth controls must avoid exceeding the configured allocation, the supported capacity is rounded down to 12 simultaneous calls. Those calls consume 960 kbps, leaving 40 kbps unused. This calculation is important when configuring locations or other CAC mechanisms between clusters: the allocation should protect the WAN from oversubscription while ensuring that calls admitted across the link receive the bandwidth required for acceptable G.711 voice quality. Cisco documents the G.711 bandwidth value and IP telephony bandwidth considerations in its Understanding Bandwidth Consumption guidance and its Cisco Unified Communications Manager System Configuration Guide.