Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

Cisco

300-835

Automating Cisco Collaboration Solutions (CLAUTO)

QUESTION 144
All of your department's IP phones are connected to a switch that does not support PoE. The IP phones have all been manually configured with IP addressing information. Another administrator power cycles the switch without warning. No calls are in progress. Which of the following is most likely to occur? (Select the best answer.)

A. The IP phones will power down until the switch restarts.
B. The IP phones will not be affected by the power cycle.
C. The IP phones will disappear from the UCM configuration.
D. The IP phones will reset but retain IP configuration information.

Answer: D

Explanation

Explanation:
Most likely, the IP phones will reset but retain IP configuration information when the administrator power cycles the switch because, in this scenario, the IP addressing information has been manually configured on each IP phone. When an IP phone is disconnected from Cisco Unified Communications Manager (UCM), the phone will automatically reset in an attempt to reestablish communication. Therefore, if an IP phone suddenly resets or is continuously attempting to register with UCM, it is important to first verify the phone's connectivity to the network switch.
The IP phones will not disappear from the UCM configuration. You can verify that an IP phone exists in the UCM by clicking Device > Phone > Find in UCM Administration and searching for the particular IP phone's Media Access Control (MAC) address. The IP phone will no longer be registered with UCM when it loses connectivity. However, the IP phone's record in the UCM configuration will remain there.
The IP phones will not power down until the switch restarts, because the switch in this scenario does not support Power over Ethernet (PoE). Therefore, the IP phones in this scenario must be connected to individual power supplies in order to obtain power.
The IP phones will be affected by the power cycle. In addition to registration problems, IP configuration problems, and Trivial File Transfer Protocol (TFTP) configuration problems, IP phones that are powered directly from a switch by using PoE will not be able to receive power until the switch has restarted.

Reference:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cuipph/7905g_7912g/5_0/sip/english/administration/guide/5_0/LowPtrb.html#wp1092158

QUESTION 145
You want to test a new dial plan before you deploy the plan in a UCM environment.
Which of the following tools should you use? (Select the best answer.)

A. CAR
B. DNA
C. RIS
D. RTMT

Answer: B

Explanation

Explanation:
You should use the Cisco Unified Communications Manager (UCM) Dialed Number Analyzer (DNA) to test a new dial plan before you deploy the plan in a UCM environment. You can also use DNA to test a dial plan after deployment. DNA initially displays results in a new browser window. However, you can export data from DNA in the form of an Extensible Markup Language (XML) file.
A dial plan is a set of rules, or route plan, that determines how calls reach their destinations. A Voice over IP (VoIP) dial plan enables a company to route calls between geographically dispersed sites while keeping the calls onnetwork. Onnetwork calls are calls routed over a single network, such as an IP data network. By contrast, offnetwork calls are calls that are routed through multiple telephony networks, such as those routed over the public switched telephone network (PSTN).
DNA and verification of the calling search space are both ways to troubleshoot error recordings when attempting to make offnetwork calls.
You should not use Cisco Unified RealTime Monitoring Tool (RTMT). RTMT is a clientside application that enables an administrator to monitor devices on a Cisco VoIP network in real time by using Secure Hypertext Transfer Protocol (HTTPS). RTMT uses HTTPS to connect to VoIP devices and gather information, such as device status and performance statistics, in real time. The data that is gathered by RTMT can then be used to pinpoint problems on the VoIP network or to monitor performance thresholds.
You should not use the Cisco Realtime Information Server (RIS). The RIS maintains device registration statuses, performance counter information, and information about critical alarms in real time. Similar to DNA, the Cisco RIS Data Collector, which transmits data to the RIS, runs as a UCM service. If you notice that UCMregistered devices are not showing up in the UCM Administration pages, you should try restarting the Cisco RIS Data Collector service.
You should not use the Cisco Call Detail Records (CDR) Reporting and Analysis (CAR) tool. CAR is used to generate CDR reports, Quality of Service (QoS) reports, traffic reports, and billing reports. Reference:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/dna/9_0_1/CUCM_BK_C7C05BE8_00_cucm-dialed-number-analyzer-90/CUCM_BK_C7C05BE8_00_cucm-dialed-number-analyzer-guide_chapter_01.html#CUCM_TP_D4E3DA13_00

QUESTION 146
You issue the no ip source-address 172.16.0.1 command in telephony service configuration mode on a CME router.
Which of the following is true? (Select the best answer.)

A. The CME router will no longer receive credential services messages.
B. The CME router will receive IP phone messages through an alternate port.
C. The CME router will no longer receive messages from IP phones.
D. The CME router will receive messages from IP phones by using IPv6.

Answer: C

Explanation

Explanation:
The Cisco Unified Communications Manager Express (CME) router will no longer receive messages from IP phones if you issue the no ip sourceaddress 172.16.0.1 command in telephony service configuration mode. The syntax of the ip sourceaddress command is ip sourceaddress {ipv4address | ipv6address},

where ipv4address is the IP version 4 (IPv4) address on which you want the router to receive IP phone messages. Issuing the no form of this command disables the CME router's ability to receive messages from IP phones.
The CME router will not receive IP phone messages through an alternate port. To configure the CME router to receive IP phones through an alternate port, you should issue the ip sourceaddress command with the port keyword. However, the port keyword applies only to Skinny Client Control Protocol (SCCP) phones and operates only on an IPv4 address. For example, issuing the ip sourceaddress 172.16.0.1 port 2400 command in telephony service configuration mode configures the CME router to receive IP phone messages on 172.16.0.1 on Transmission Control Protocol (TCP) port 2400. If the portkeyword is not specified, the CME router receives the IP phone messages on TCP port 2000.
The CME router will not receive messages from IP phones by using IPv6. In order to configure the CME router to receive messages from IP phones by using IPv6, you should issue the ip sourceaddress command with an IPv6 address instead of an IPv4 address. You can also configure the source address to operate in dualstack mode by issuing the secondary keyword followed by an IPv4 address. For example, the ip sourceaddress 2001:DB8:A::1 secondary 172.16.0.1 command configures the CME router to receive IP phone messages at either the IPv6 address of 2001:DB8:A::1 or the IPv4 address of 172.16.0.1.
You cannot configure whether the CME router will receive credential services messages from telephony service configuration mode. Issuing the ip sourceaddressipaddresscommand in credentials configuration mode configures the CME router to receive credential services messages from a particular IP address. Issuing the no form of this command in credentials configuration mode disables that ability.
Reference:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/command/reference/cme_cr/cme_i1ht.html#wp3725679205

QUESTION 147
You issue the showrunning config command on a CME router and receive the following partial output:

```
dial-peer voice 1 voip
 destination-pattern .......
 session target ipv4:192.168.0.1
!
dial-peer voice 2 voip
 destination-pattern 302....
 session target ipv4:192.168.0.2
!
dial-peer voice 3 voip
 destination-pattern 3021234
 session target ipv4:192.168.0.3
!
dial-peer voice 4 voip
 destination-pattern 302
 session target ipv4:192.168.0.4
```

A caller dials 3021234.
Which of the following dial peers will the router use? (Select the best answer.)

A. 1

B. 2
C. 3
D. 4

Answer: D

Explanation

Explanation:
The Cisco Unified Communications Manager Express (CME) router will use dial peer 4 to route the voice data when a caller dials 3021234. When a caller dials 3021234, the router collects the digits as the caller dials them. The router compares the dialed digits against dial peer destination patterns on a digitbydigit basis. Because dial peer 4 most specifically matches the dialed string 302, the router will immediately process the call by using dial peer 4 as soon as the caller completes the 302 sequence of characters.
If multiple dial peers explicitly match the destination pattern, the most specific match for the pattern will be used. For example, if dial peer 4 were removed from this scenario, a caller dialing 3021234 would immediately match all three of the remaining dial peers. Dial peer 3, because it explicitly defines the dialed string, would be the most specific match. Dial peer 1, because its destination pattern contains seven wildcards, would be the least specific match.
The router will not use dial peer 3 to route the voice data when a caller dials 3021234. Although dial peer 3 is the most specific destination pattern match for the entire string of dialed digits, the router will process the most specific match on a digitbydigit basis. Therefore, the router will process the call as soon as dial peer 4 is matched, before the caller has had a chance to complete the full sevendigit string.
The router will not use dial peer 1 or dial peer 2 to route the voice data when a caller dials 3021234. Although the destination pattern configured for dial peer 1 would match any sevendigit dialed string, the destination pattern is not the most specific match for 3021234. Similarly, the destination pattern configured for dial peer 2 would match the dialed string, but it is a less specific match than dial peer 4, because four of the seven digits in the dial peer 2 destinationpattern command are wildcards.
Reference:
https://www.cisco.com/c/en/us/support/docs/voice/call-routing-dial-plans/14074-in-dial-peer-match.html#topic9

QUESTION 148
Which of the following are not Cisco Unity Connection features that you can modify in the Phone section of the User Templates Basics page? (Select 3 choices.)

A. CoS
B. partition
C. search space
D. voice mail password
E. web application password
F. time zone

Answer: DEF

Explanation

Explanation:
You cannot modify the Cisco Unity Connection time zone feature in the Phone section of the User Templates Basics page. If your company's Cisco Unity Connection implementation must support users in different time zones, you can create a unique user template for each time zone. Within each template, you can configure the time zone in the Location section of the User Templates Basics page. You can also adjust the system default language in this section.
In addition, you can modify neither the voice mail password nor the web application password in the Phone section of a Cisco Unity Connection User Templates Basics page. Cisco Unity Connection users have two passwords: the voice mail system password that is issued by using the telephone user interface (TUI) and the web application password that is issued by using Cisco Unity Connection's webbased graphical user interface (GUI). The voice mail password is a personal identification number (PIN) that enables a user to access his or her voice mailbox in Cisco Unity Connection. The web application password is an alphanumeric password that enables a user to access and modify specific Cisco Unified Communications settings by using a browser.
To access the Voice Mail Password Settings section of a user template, you should click Templates > User Templates in Cisco Unity Connection and select Voice Mail from the Choose Password dropdown menu. To access the Web Application Password Settings section of a user template, you should click Templates > User Templates in Cisco Unity Connection, then select Web Application from the Choose Password dropdown menu.
You can modify Class of Service (CoS) features in the Phone section of a Cisco Unity Connection User Templates Basics page. CoS settings enable an administrator to apply a specific set of privileges to Cisco Unity Connection users. In addition, you can modify partition features and search space features in the Phone section of a Cisco Unity Connection user template. A partition is a logical grouping of Voice over IP(VoIP) route patterns and directory numbers (dns). A search space is an ordered list of partitions that a device is allowed to search for patterns that match a dialed number.

Reference:

QUESTION 149
You are configuring digest authentication so that the identity of SIP phones can be challenged by the UCM to which they are connected. After configuring an appropriate security profile, you apply the profile to each SIP phone on the network. After creating a digest user in the UCM Administration End User window, you notice that a Cisco 7961G IP phone is not able to authenticate with UCM. Which of the following should you do? (Select 2 choices.)

A. Associate the digest user with the SIP phone in UCM Administration.
B. Configure the SIP realm on a SIP trunk.
C. Reset the phone.
D. Specify digest credentials in the Application User Configuration window.
E. Upload the configuration file to the TFTP server.

Answer: AC

Explanation

Explanation:
You should associate the digest user with the Session Initiation Protocol (SIP) phone in Cisco Unified Communications Manager (UCM) Administration and then reset the Cisco 7961G IP phone in order to enable the phone to use digest authentication to verify its identity with the UCM to which it is connected.

The digest credentials for most Cisco IP phones are stored in the phone's configuration file, which is downloaded from a Trivial File Transfer Protocol (TFTP) server when the phone is started or reset. On Cisco 7940G and 7960G SIP IP phones, the digest credentials must be manually entered from the IP phone.

Digest credentials consist of a unique user ID, password, and digest realm. UCM generates a Message Digest 5 (MD5) hash from these values and a random number. A checksum is generated from the hash. The user name and checksum are then stored in the UCM database in an encrypted format.
To enable UCM to authenticate a SIP phone, you should first configure a security profile for SIP phones and verify that the Enable Digest Authentication check box has been selected. Next, you should apply the security profile to the SIP phones that you want to be authenticated. After the security profile has been created and applied, you should configure a digest user in the UCM Administration End User window, where you specify the digest user ID and password that you want the SIP phone to use to authenticate. Finally, you must associate the digest user with the SIP phone that you want to be authenticated and reset that SIP phone so that it downloads its new configuration. The new configuration contains the digest credentials.
You do not need to upload the SIP phone configuration file to the TFTP server. UCM updates the configuration file so that it can be downloaded from the TFTP server by the IP phones. However, for security reasons, you might want to ensure that TFTP traffic between the server and the IP phones is encrypted. Otherwise, the digest credentials will be included in a configuration file that is sent across the network as clear text.
You do not need to specify digest credentials in the Application User Configurationwindow. The Application User Configuration window can be used to specify digest credentials for SIP applications that you want to authenticate with UCM.
There is nothing in this scenario to indicate that you should configure the SIP realm on a SIP trunk. You would need to configure a SIP realm if you were receiving digest authentication challenges over a SIP trunk. Reference:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/9_0_1/secugd/CUCM_BK_CCB00C40_00_cucm-security-guide-90/CUCM_BK_CCB00C40_00_cucm-security-guide_chapter_01100.html#CUCM_TK_S2044B79_00
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/9_0_1/secugd/CUCM_BK_CCB00C40_00_cucm-security-guide-90/CUCM_BK_CCB00C40_00_cucm-security-guide_chapter_01.html#CUCM_RF_D4C84CE2_00

QUESTION 150
You are unable to create a new user from UCM Administration.
Which of the following is most likely the cause of the problem? (Select the best answer.)

A. The Telephone Number field is empty.
B. An IP phone has not been associated with the account you are creating.
C. The Cisco Unity User check box has not been selected.
D. Users have been synchronized from LDAP.

Answer: D

Explanation

Explanation:
Of the available choices, most likely you are unable to create a new user from Cisco Unified Communications Manager (UCM) Administration because users have been synchronized from Lightweight Directory Access Protocol (LDAP). New users can be directly created from UCM Administration only if LDAP server synchronization is disabled. You can determine whether LDAP synchronization is enabled by navigating to System > LDAP > LDAP System in UCM Administration.

If users are not able to view telephone numbers in the corporate directory, you should verify that the Telephone Number field is not empty. Users are capable of searching UCM directory information from IP phones or applications. However, in order for users to see that information, the appropriate fields must be filled in for each UCM user in UCM Administration or in the LDAP directory from which UCM obtains the information.

If the UCM user you created was not also created in Cisco Unity Connection, you should verify that the Cisco Unity User check box was selected for that user in UCM Administration. When you create a user in UCM Administration, you can simultaneously create a Cisco Unity Connection account for that user by selecting the Cisco Unity Usercheck box in UCM Administration. However, you will still need to edit the newly created Cisco Unity Connection user account in Cisco Unity Connection to complete the configuration.
It is not likely that you cannot create a user in UCM Administration if an IP phone has not been associated with the account. You cannot associate a device with an end user unless the end user account has already been created. Reference:
https://www.cisco.com/c/en/us/obsolete/unified-communications/cisco-unified-communications-manager-version-7.1.html#wp1059267

QUESTION 151
You want to delete 100 unassigned dns from the UCM database.
Which of the following sets of steps could you use? (Select 2 choices.)

A. Use Bulk Administration > Phones > Delete Phones > Delete Unassigned DN to find and remove the dns.
B. Use Call Routing > Route Plan Report to find and remove the dns.
C. Use Call Routing > Directory Number to find and remove the dns.
D. Use Device > Phone > Directory Number Configuration to find and remove the dns.
E. Use Device > Phone > Device Information to find and remove the dns.

Answer: AB

Explanation

Explanation:
You could use either Bulk Administration > Phones > Delete Phones > Delete Unassigned DN or Call Routing > Route Plan Report to find and remove 100 unassigned directory numbers (dns) from the Cisco Unified Communications Manager (UCM) database. An unassigned dn is a dn that is not associated with a specific device, such as an IP phone, but that can still be used to forward calls to voice mail or to another dn that is associated with a device. For UCM to load and use an unassigned dn, the Activecheck box must be selected for the dn. The Active check box is only displayed for unassigned dns.

The UCM Bulk Administration > Phones > Delete Phones > Delete Unassigned DNwindow automatically searches for and displays a list of unassigned dns in the UCM database. Once the list of unassigned dns is complete, you should select the Run Immediately radio button and then click Submit to immediately delete the unassigned dns from the UCM database.
To find 100 dns by using Call Routing > Route Plan Report, you should choose Unassigned DN from the Find dropdown menu and then click the Find button. Once the list of unassigned dns is complete, you can select the check box beside each dn that you want to delete and then click the Delete Selected button to immediately delete the unassigned dns from the UCM database. Alternatively, you can remove all unassigned dns at once by clicking the Delete All Found Items button instead of the Delete Selectedbutton.
Problems with unassigned dns can cause an IP phone that is attempting to autoregister with UCM to display the following error:
Registration Rejected: Error DBConfig
Therefore, you should remove unassigned dns from the autoregistration configuration if this error occurs.
You cannot use Device > Phone > Directory Number Configuration to find and remove 100 unassigned dns from the UCM database. The Directory Number Configuration window in UCM is for adding dns to an IP phone, updating dn associations with an IP phone, and removing dns from an IP phone. Although you can add new dns to the UCM database by using the Directory Number Configuration window, you cannot remove a dn from the UCM database by using that window.

You can also use the Directory Number Configuration window to reassign dns that have been removed. The Route Plan Report can also be used to accomplish this task.
You cannot use Call Routing > Directory Number to find and remove 100 unassigned dns from the UCM database. However, similar to Device > Phone > Directory Number Configuration, you can use Call Routing> Directory Number to add a dn to the UCM database or to update information about the dn in the UCM database. You can also add a dn to a phone immediately after you add the phone to UCM by clicking the Line [1] -Add a new DN link or the Line [2] -Add a new DN link in the Association Information area, which is displayed on the left side of the Phone Configuration window in UCM.
You cannot use Device > Phone > Device Information to find and remove 100 unassigned dns from the UCM database. However, you can use this option to configure the IP phone Media Access Control (MAC) address, security profile, device pool, phone button template, location, privacy settings, and mobility mode.
Reference:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/bat/8_0_2/bat-802-cm/t03delph.html#wp1355300
https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/71440-ccm4x-unassigneddns.html#maintask1

QUESTION 152
Which of the following terms defines a value that represents voice quality in a network depending on codec and region? (Select the best answer.)

A. Jitter
B. QoS
C. MOS
D. R-Factor

Answer: C

Explanation

Explanation:
Of the available choices, the term Mean Opinion Score (MOS) defines a value that represents voice quality in a network depending on codec and region. MOSs are calculated scores that are mitigated by voice quality hindrances, such as latency and jitter. In addition, MOS scales are not standard across codecs and regions. Therefore, the MOS scale for one codec might not be applicable to another codec. Devices such as the Cisco Network Analysis Module (NAM) monitor active Realtime Transport Protocol (RTP) streams in order to gather the statistical data to compute the MOS.

An R-Factor is also a value that represents voice quality in a network. However, the way R-Factor measurements are calculated is the same across all codecs and regions. Therefore, R-Factor measurements might be a simpler means of evaluating an enterprise that spans regions or deploys a number of different codecs.
Quality of Service (QoS) is a Voice over IP (VoIP) technique that ensures call quality and integrity by mitigating delay and dropped packets, which can interrupt the flow of a VoIP call. Typical QoS techniques include buffer management and the use of multiple transmission queues to separate types of multimedia packets. Because voice traffic is sent in real time, quality is critical.
Jitter is a variation in delay that can cause packets to arrive out of sequence or at a different rate than they were sent. As a result, the end user might experience choppiness in the audio connection. Thus shorter packet roundtrip times contribute to better voice quality. Reference:
https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/branch-routers-series-network-analysis-module-nme-nam/white_paper_c11-520524.html
QUESTION 153

You are the administrator for a small VoIP network connected to an ITSP in the United States. The topology consists of one voice router, a UCM, and three PoEcapable switches. All of the IP phones are receiving power. However, none of the IP phones on the network are registering with UCM.
In which of the following fault domains should you begin troubleshooting? (Select the best answer.)

A. the IP phones
B. the cables connecting the IP phones to the switches
C. the network switches that are connected to the IP phones
D. the UCM configuration

Answer: D

Explanation

Explanation
Because none of the IP phones on the network are registering with Cisco Unified Communications Manager (UCM), you should begin troubleshooting at the UCM configuration. Licensing problems or other configuration issues could be preventing IP phones from registering with UCM. You might also begin troubleshooting at the voice router instead of the UCM if all the IP phones on the network are able to register with UCM but are not able to make calls beyond the router.
You would not begin troubleshooting at the IP phones, because all the IP phones are affected. If only one user were experiencing the problem, you could begin troubleshooting the IP phone fault domain.
You would not begin the troubleshooting process by examining the cables connecting the IP phones to the switch. You might check the cable connecting the IP phone to the switch or the switch port to which the cable is connected if a single IP phone were a Power over Ethernet (PoE) device that was not receiving power from the switch, or if Cisco Unified Communications Manager (UCM) reported that the device is of an unknown type. You might also check the network cable and switch port if the device were powered by a power supply but unable to register and download a configuration.
It is not likely that you would begin troubleshooting the network switches, because all users are affected by the problem. You might begin troubleshooting the problem at the network switches if an entire department within an organization were reporting a problem or if only the users connected to a given switch were experiencing a problem.
Reference:
https://www.cisco.com/c/en/us/obsolete/unified-communications/cisco-unified-communications-manager-version-7.1.html#wp1111505

QUESTION 154
You administer a UCM network of 500 IP phones

You need to add 50 new IP phones to your company's UCM network before the end of the workday. Which of the following does Cisco recommend you do? (Select the best answer.)

A. Add a second UCM server to the cluster.
B. Add the phones by using the BAT.
C. Enable auto-registration in UCM.
D. Provision the IP phones manually in UCM.

Answer: C

Explanation

Explanation:
Cisco recommends that you enable auto-registration in Cisco Unified Communications Manager (UCM) to add fewer than 100 new IP phones to a UCM network. There are three ways to add IP phones to a UCM database: by configuring auto-registration, by using the Bulk Administration Tool (BAT), and by manually provisioning the IP phones in the UCM administrative graphical user interface (GUI). Both auto-registration and the BAT provide a means of adding many phones to the database simultaneously. However, Cisco does not recommend using the BAT if you need to add fewer than 100 IP phones.

Auto-registration enables UCM to automatically add new IP phones to the UCM database as the IP phones are connected to the network. When a new IP phone is connected to the network, UCM will automatically assign an unused directory number (dn) to the IP phone from a pool of available dn numbers.

Auto-registration is a security risk because rogue devices can be connected to the network and registered with UCM by using auto-registration. In addition, you could accidentally register a valid IP phone with a dn from the wrong dn pool if you leave auto-registration enabled after you have completed an auto-registration process. Therefore, Cisco recommends that you enable auto-registration only for short periods of time, such as when you need to add fewer than 100 IP phones to the network. In this scenario, you want to add 50 new IP phones to your company's UCM network before the end of the workday. Because of the time limitation and the small number of IP phones, enabling auto-registration would require the least amount of administrative effort.

You do not need to provision the IP phones manually in UCM. Although you can manually add an IP phone to a UCM database, adding 50 new IP phones by using manual provisioning would require more administrative effort than by using auto-registration or the BAT. When you are manually provisioning an IP phone in UCM, you must fill in the MAC Address field, the Device Pool field, the Phone Button Template field, and the Device Security Profile field. In this scenario, you want to add 50 new IP phones to your company's UCM network before the end of the workday. Because of the time limitation and the number of IP phones, enabling autoregistration would require the least amount of administrative effort. Therefore, you should not manually provision the IP phones. You do not need to add a second UCM server to the cluster. UCM supports a maximum of 7,500 devices as a standalone server and a maximum of 30,000 IP phones per UCM cluster. In this scenario, you administer a network of 500 IP phones. In addition, you are adding only 50 new IP phones, which brings the total number of IP phones to 550.

You do not need to add the phones by using the BAT. The BAT enables a UCM administrator to add or modify multiple IP phones at once. However, Cisco recommends that you use the BAT to add 100 or more new IP phones to a UCM network. In this scenario, using the BAT would require more administrative effort than using auto-registration because the BAT requires you to provide Media Access Control (MAC) addresses for the IP phones that are being added. Autoregistration does not require you to provide MAC addresses.

Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/8_0_2/ccmsys/accm-802-cm/a02autor.html#wp1020237

SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

***Actual Exam Questions**: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

***Exam Dumps**: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

***Practice Tests**: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

***Guaranteed Success**: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

***Updated Content:** Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

***Technical Support**: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*