9. CUCM Phones and Users

UNDERLYING SERVICES

Service	Description
NTP (Network Time Protocol)	Timestamps for Call Detail Records (CDR), Call Management Records (CMR) and logs. Publisher CUCM node syncs to NTP; subscribers sync to the publisher. Phones sync to their subscriber node via SCCP (skinny) messages. SIP (Session Initiation Protocol) phones need an NTP, but can get by with the timestamps in SIP OK responses from the subscriber server.
CDP (Cisco Discovery Protocol)	Conveys Voice VLAN ID from the switch to the phone
DHCP (Dynamic Host Configuration Protocol)	Provides phones with IP & Mask, Gateway, DNS server(s), TFTP server(s). Phones can be manually configured, but don't. The CUCM server can provide DHCP, but don't.
PoE (Power over Ethernet)	Powers the phones
TFTP (Trivial File Transfer Protocol)	Phones get config files, firmware. When configuration updated, CUCM creates or modifies a config file for the device and uploads it to the server. Note (p235) "A generic TFTP server will not have the integrated capability that a CUCM TFTP server does and will not correctly fulfill the role."
DNS (Domain Name System)	Avoid reliance on. CUCM cannot provide.

PHONE REGISTRATION

Phone Boot (SIP & SCCP)

- Power from PoE or adapter
- Load local firmware image
- Learn voice VLAN from CDP
- DHCP Request—get IP, Mask, Gateway, TFTP, and potentially more

Then the Path Splits (SCCP vs SIP):

SCCP Phone Registration

- Phone downloads its own configuration from TFTP in file: SEP<MAC>.cnf.xml
- Phone Registers with primary CUCM server mentioned in the file
- CUCM server sends DNs, softkeys, and speed dials in SCCP messages

SIP Phone Registration

- In a secured cluster, the phone gets the Certificate Trust List via TFTP
- Phone downloads SEP<MAC>.cnf.xml from TFTP, just like with SCCP
- Phone downloads any SIP dial rules configured for that phone
- Phone Registers with primary CUCM server mentioned in the file (like SCCP)
- Phone downloads localization files, softkey configs & ringtones from TFTP

Configuration files are created by CUCM and uploaded to the TFTP server when a phone is created or modified.

For SCCP, the SEP<MAC>.cnf.xml file contains an ordered list of CUCM servers with TCP ports that the phone should register with. It also lists the firmware version and service URL for each model of device (phone).

CUCM PRE-PHONE GROUNDWORK

Activate needed services on the Unified Serviceability admin page (http://<ip>/ccmservice). For example: Call Manager, TFTP, and DHCP Monitor.

DHCP—The server ability of CUCM supports only phones, up to 1,000 of them. Multiple subnets supported, but no redundancy and only one DHCP server per cluster, typically on the publisher.

(Admin) System → DHCP → DHCP Server

Click "Add New." Select the server running the DHCP Monitor Service (just activated, above) from the pull-down. Configure desired settings like Primary DNS Server IPv4 Address, PrimaryTFTP, IP Address lease time. These settings are inherited by the subnet config page.

DHCP Subnets—Settings here override those inherited from above.

(Admin) System → DHCP → DHCP Subnet

Click "Add New." Select server from drop-down list. Set subnet address & mask, range start & end, gateway, DNS, TFTP (option 150)

DHCP in IOS—See Chapter 3 notes.

DEVICE POOLS

Device Pool—A template to apply several settings to a group of phones at once and w/o errors.

CUCM Group—Defines an ordered list of up to 3 redundant call-processing servers and an optional SRST (Survivable Remote Site Telephony) reference.

Phones normally send a primary registration msg to the primary server (1st in list), a backup registration msg to the backup server (2nd in list) and nothing to the tertiary server. If the primary fails, the phone sends a primary registration message to the secondary server, registering with it, and sends a backup msg to the tertiary.

Subscriber—A CUCM *server,* not a phone! Subscribers can be in multiple groups, to evenly distribute phones & provide redundancy. Good design ensures that no failure scenario overloads a server.

Region—Assignment (tag) that can a used to control bitrates *per-call* within and between regions, indirectly selecting the codec.

Location—Define max bandwidth used by calls to a location. Usage by each call is tracked and when bandwidth is used up, further calls are dropped (default) or rerouted over the PSTN, depending on AAR config. This is one mechanism for CAC (Call Admission Control).

Date/Time Group—Puts a phone in a time zone & date format group.

Phone NTP Reference—SIP phones need to directly contact an NTP server; SCCP phones get time through SCCP messages. Preferably, the NTP server will be local to the phones.

OTHER DEFAULTS & TEMPLATES

Device Defaults (page)—For all supported endpoint types, lists firmware load, device pool, and phone button template defaults—Used when a new device is registered.

Softkey / Phone Button Template—Softkeys are for features (conferencing, etc.) 7 default softkey templates provided. The 80+ default phone button templates (separate for SIP and SCCP) typically provide two lines and fill the rest with speed-dials.

Profiles—Configures repetitive tasks. Several types and many versions of each type can be created:

- Security Profile—(default unsecured) Can config devices secured, use encrypted TFTP config files, and Certificate Authority Proxy.
- Common Phone Profile—DND settings, VPN, USB ports, video capability, power-save options

ADDING PHONES

Four ways to add phones:

- Manual—Phone configuration page
- Autoregistration—CUCM dynamically configures & adds any phone that connects
- BAT (Bulk Admin Tool)—CUCM provides template .csvs to create multiple phones at once
- TAPS (Autoregister Phone Tool)—An IVR (Interactive Voice Response) server, combined with autoregister and BAT, automates adding thousands of phones at a time
- Self-Provisioning—Similar to TAPS, with IVR and CTI (Computer Telephony Integration) internal to CUCM as of v 10.x Note: CTI refers to things like dialing from an outlook database —mentioned in chapter 2.

MANUAL PHONE CONFIG

(Admin) Device --> Phone; click [add new]

- Model from drop-down
- Choose protocol, SIP or SCCP, if model supports both
- Enter the 5 Required Fields that lack a default: MAC, device pool, phone button template, owner user ID, security profile
- Click "save"; page reloads with button template applied. Now can add specifics in the "Association Information" pane, on the left
- Click "Line [1] - Add New DN"—Opens a new DN Info Page
    - Route Partition (see chap 10)—related to calling privileges or class of control
    - Alerting Name—Name to display on caller's phone when ringing (non-PSTN)
    - Call Forward / Pickup Option Settings—how forward if busy
    - Display—Internal caller ID string to show on another phone we call
    - Line Text Label—Local to the phone—How to label the line button
    - External Phone Number Mask—Changes the CLID (Calling Line ID) to be a full PSTN number instead of an internal DN (extension number) when go out via PSTN

    - Click "save" *twice*. The second save is new in v 9.x and only required if the DN has been changed. Watch top of screen for warning that the config refreshed when the DN changed instead of saving and still needs to be saved with a second attempt.
- In the "related links" drop-down, select "Configure Device (<Phones>)" and click "go"
- Now you're back at the phone page to make further changes or click "save" again
- The page prompts you to click the "Apply Config" Button to reload the phone (restart or reset, depending on what was changed)

Restart vs Reset—In CUCM 8, the "Apply Config" button chooses reset or restart for you.

- Reset reboots both firmware and config of the phone. Important, if you've changed firmware version, locale, SRST, or Communications Manager Group to force the phone to pull a new file from TFTP. From the phone, a reset can be triggered with "Settings" and **#** (keypad)
- Restart unregisters the phone (it immediately reregisters). This is good for refreshing info not passed through the config file—button changes, names, forwarding. Faster because the firmware isn't restarted

Associating a User with a Phone—required if users are to use "user web pages" to configure their phone. A user is associated with the device, which is associated with 1 or more DNs. The three entities are independent—a device and DN won't go away if a user is deleted, etc.

AUTOREGISTRATION

A phone can even receive a DN automatically. Best practice = only when needed. To enable:

- (System --> Enterprise Parameters)—Choose SCCP (default) or SIP protocol for phones that support both. Phones that don't support your choice will autoregister with the other protocol.
- Make sure that at least one CM Group has autoregistration enabled (checkbox)
- Enable Autoregistration on at least one CUCM server within the CM group that has autoreg.
    - *Deselect* the checkbox "Auto-registration Disabled on this Cisco Unified Communications Manager" (default=checked=autoregistration disabled)
    - Set "Starting Directory Number" and "Ending Directory Number." (Both default to 1000.) Setting them to the same value automatically disables autoregistration
    - Select a UDT (Universal Device Template) and ULT (Universal Line Template) (previously configured). These are new in CUCM v9 and can have variables, like #LastName# (click the pencil icon to insert one from a list) for things like button labels that get filled in once a user exists
    - Optionally, set the partition that will be assigned to the phones (good way to limit and control auto-reg phones)
    - click save

BULK ADMIN TOOL

Database inserts, modifications, or deletions can be scheduled & unattended. Can export selected records, modify them, and reinsert for accurate bulk changes. Can be used for almost any aspect of CUCM, including phones, users, forced authorization codes & client matter codes, user device profiles, the region matrix, gateway devices, etc.

Components

- Excel template (downloaded from the CUCM server) provides required fields and formatting for new data being entered. Phone creations require the MAC address of each new phone, but a barcode scanner can quickly input those into a laptop as you walk the room
- Server-side templates allow you to configure data that all records in a given transaction will have in common
- Web page interfaces for preparing and executing operations

Strategy: use autoregister to get all phones working, then modify configs with BAT. You need only be positive of which phone's MAC address is sitting on which desk.

AUTO REGISTER PHONE TOOL

TAPS (Tool for Auto-registered Phone Support) goes one step further. Great for huge deployments, but requires you to have and correctly configure an IP-IVR (Interactive Voice Response) system.

- Build an IP-IVR server and configure it to support TAPS, and integrate the CUCM server with it. Several Cisco applications support IP-IVR, including Unified Contact Center Express
- Prepare a BAT job, specifying a Device Template for all common phone settings and a .csv file with specifics
- Run the BAT job, with the checkbox that automatically substitutes fake "dummy" MAC addresses for the as-yet-unknown real ones. Now CUCM has a bunch of records with correct extension numbers and wrong phone MAC addresses.
- Phones autoregister, receiving a temporary DN, and can place calls.
- Each phone can now call the special IP-IVR pilot number. After authenticating (optional), the user can enter the extension they should have. The IVR automatically captures the MAC of the calling phone and the "correct" extension number keyed in by the user & sends them to CUCM
- CUCM receives the MAC and the extension number. CUCM changes the MAC in the record with the given extension number and restarts the phone. Done.

SELF-PROVISIONING

Conceptually the same as TAPS, except that the IVR is internal to CUCM. It can also use the power of UDT / ULT variables for better customization.

CUCM END USERS

Anyone can use any phone, but the really cool features orbit the idea of a specific "user." The difference between end users and application users is important in CUCM.

End Users—Typically type a user name & password at a web page login screen

Application Users—An application (not a person). It sends authentication as part of a data request. Example: a third-party billing application accessing CDRs (Call Data Records).

End User	Application User
Actual person	Application
Interactive logins	Non-interactive
Assigns user features and rights	Application authorization
In the user directory	Not in user directory
LDAP can be used	No LDAP—authentication must be local

Credential Policy—defines preset passwords, end-user PINs, and "application user" passwords. The Default credential policy uses the application password specified at install is for all of them. Additional policies can specify # of login attempts, minimum password length, password aging & # of previous passwords stored, whether to check for weak passwords.

Strong Password	Strong PIN
3 of 4 character classes { upper, lower, numbers, symbols }	No number more than twice consecutively
Can't use same char more the 3 times consecutively	Can't include mailbox or extension, even in reverse
Can't include alias, username, or extension	Needs 3+ different numbers in it
No consecutive characters	Can't be dial-by-name version of the user name
	No repeated digit patterns or linear keypad sequences

Features that use the End-User login:

- Unified CM Admin web pages
- User Web Pages (Self-Care Portal)
- Serviceability
- OS Admin
- Disaster Recovery System
- Cisco Extension Mobility
- CUCM Assistant
- Directories
- IP Phone Services
- Data Associated with User Accounts

User Account Info Categories (Application User accounts use a subset of this):

- Personal & Organizational Settings (User ID; Name—first, middle, last; Manager UserID, Department, Phone Number, Mail ID)
- Password Info (Password)
- CUCM Config Settings (PIN; SIP Digest Credentials; User Groups and Roles; Associated PC, controlled devices, and DNs; Application and feature parameters—Extension Mobility, Presence Group, CAPF)

User Locale—Controls language on phone & user web page. Locale files are installed on CUCM and are downloaded to specific phones over TFTP

Device Association—Associating an end user account with a device allows the user to customize speed dials, ring preferences, etc. The end user can be associated with IP phones, CIPC (Cisco IP Communicator) and Cisco Extension Mobility profiles.

Because the User Attribute Name in the CUCM database must be unique, you can dial a user by name. CUPS (Cisco Unified Presence Server) tracks a user's availability on voice, video, & chat.

Manual Entry, One at a Time

4 required fields—User ID, Last Name, Presence Group (defaults to Shared Presence Group), Remote Destination Limit (default=4)

In other words, you only need to enter User ID and Last name, the others can default.

Bulk Import Using BAT—Also for removes and updates. Admin uploads a .csv file.

LDAP (Lightweight Directory Access Protocol) Integration—Only works for end users; application users are always and only in the CUCM database. Two ways to integrate; typically you'll do both:

- Synchronization—Populates CUCM with user attributes from LDAP using DirSync. Sync can be once, on demand, or scheduled. Passwords stay in CUCM; to keep the same password everywhere, a user must change it in both LDAP and CUCM. Data from LDAP is read-only in CUCM. CUCM versions 9 and above can maintain local user accounts in addition to the LDAP-sourced accounts. Within LDAP-sourced accounts, much additional data is CUCM-only (associated devices, PIN, extension mobility profile, etc). Synch can be full or incremental. Microsoft Active Directory 2000/2003/2008 can only do full.
- Authentication—Redirects password authentication to the LDAP server. End user passwords aren't replicated in CUCM and can only be changed in LDAP. If LDAP fails, only the CUCM Application Administrator (defined at install) can log in. Passwords are sent to LDAP as an MD5 hash for checking.

	SYNCHRONIZATION	AUTHENTICATION
Purpose	Copies some user attributes to CUCM from LDAP, using DirSync	Redirects password authentication to the LDAP server.
Create / Delete Accts in CUCM?	Local accounts possible in v9 +	Local accounts possible in v9 +
Password Location	Two separate passwords	LDAP Only
Some data only in CUCM?	Yes	Yes

LDAP Sync Specifics

- Whichever LDAP attribute is mapped to the CUCM User ID field must be unique. Verify this before building the sync agreement
- A record won't be replicated to CUCM if the "sn" LDAP attribute (surname / last name) contains no data because it's a required field in CUCM
- If the LDAP attribute that maps to User ID in CUCM collides with an existing Application User, that record will be skipped

LDAP Sync Agreement—Maps fields between LDAP and CUCM. Critically, the CUCM User ID can be sAM Account Name, UID, mail, or TelephoneNumber. Also defines what part of the LDAP directory will be searched for user accounts. (The LDAP directory can have a tree structure with different departments, locations, etc.) CUCM gains access to all branches below that point in the tree; it can't go up or sideways. The agreement specifies when the first sync will happen and a schedule for future updates.

Custom Filter—Allows you to limit which accounts are imported, e.g. only accounts in a specific organizational unit. If the filter is changed, a full LDAP sync is needed for it to take effect.

CONFIGURING LDAP SYNC

After creating an account in LDAP for CUCM with read permissions,

- Activate the Cisco DirSync service

(Serviceability) Tools --> Service Activation

  - Choose the publisher from the server drop-down list
  - Find the Cisco DirSync service, check the box next to it, click save

- Configure the LDAP system in CUCM

(Admin) System --> LDAP --> LDAP System

  - Check the box "Enable Synchronizing from LDAP Server"
  - Choose LDAP server type from drop-down
  - Choose which LDAP attribute maps to the CUCM User ID attribute from drop-down
  - Click Save

- Configure the LDAP directory

(Admin) System --> LDAP --> LDAP Directory

  - Name the sync agreement in the LDAP Configuration Name field
  - Specify the LDAP account that CUCM will use
  - Define the User Search Base, using full LDAP path syntax, e.g. "ou=Users, dc=Pod1, dc=com"
  - Set the sync schedule
  - Map CUCM fields to LDAP fields
  - Specify one to three (redundancy) LDAP server IP addresses & tell it to use SSL for security (configure LDAP for SSL too)

- Configure LDAP Custom Filters [book doesn't mention this until its own section, at the end]

To verify success, do a quick search for end users on CUCM. Under the "LDAP Sync Status" column, users listed as "Active LDAP Synchronized User" are being synced from LDAP; "Enabled Local User" users didn't exist in LDAP.

When a synced user's config page is opened, several fields won't be editable: User ID, Last Name, Middle Name, Telephone Number, Mail ID, Manager ID, and Department.

CONFIGURING LDAP AUTHENTICATION

Normally, LDAP integration will be followed by LDAP authentication to ensure that users, all of whom are synced, needn't maintain two separate passwords.

(Admin) System --> LDAP --> LDAP Authentication

- Check the box "Use LDAP Authentication for End Users"
- Specify the account and password CUCM will use to access LDAP
- Specify the LDAP User Search Base
- Specify one to three (redundancy) LDAP server IP addresses
- Click Save

To verify LDAP authentication is in use, open a user config page and ensure the password field is gone. A user can check by changing their LDAP password and ensuring that CUCM follows. Note that the PIN will still be local to CUCM.

LDAP CUSTOM FILTERS

(Admin) System --> LDAP --> LDAP Custom Filter.

- Click "Add New" & name the filter
- Type the filter statement in parens (). See RFC 4515 for search filter rules. e.g. (sn=M*) will get Milton Macpherson.

MEMORY TECHNIQUE FOR EXAM

Location vs. Region—Alphabetical ordering of "IN" or "OUT" direction of call matches "LOCATION" or "REGION." Location = Bandwidth limit entering site, Region is per call.