16. Troubleshooting CUCM

PHONE REGISTRATION

Check for these problems in order, unless you're some kind of genius.

Problems Local to the Phone

Settings button (on the phone) → Network Configuration

Scroll down to "IP Configuration" and make sure the phone has received an IP address (in the correct subnet), subnet mask, default gateway, and TFTP server address (150)
Scroll down to "DHCP Enabled" to make sure it's set to "yes"

VLAN or Switch Mismatches—make sure the switch has a voice VLAN defined for the port and a separate access VLAN if you've attached a PC to the phone.

DHCP Problems—check that the server is running and hasn't exhausted the address pool. Do a sanity check on the subnets, pools, mask, gateway, and option 150 TFTP address

Settings button (on the phone) → Network Configuration

Ensure the DHCP server entry matches the IP address of the DHCP server.
Check that an IP address in the correct range has been assigned
Check the "TFTP Server 1" address

If the DHCP server is on a remote subnet, check for "ip helper-address <IP>" on the router (sub)interface.

TFTP Problems—the phone asks TFTP for a file called "SEP<mac>.cnf.xml". This file will exist if the phone has been successfully added to CUCM/CME. If the phone hasn't been added, the file will be missing and the phone will ask for "XMLDefault.cnf.xml". If this isn't working:

- Check for the correct TFTP address in the "Network Configuration" list
- Check that TFTP is running at that address

Settings button (on the phone) → Status Messages

Check for messages like "File Not Found:SEP<mac>.cnf.xml" or "TFTP Timeout"

CUCM Registration Problems

Settings → Device Configuration → Unified CM Configuration

Verify the IP address of the CUCM server, and maybe a backup & tertiary server
Check that the Call Manager (CUCM) is running at that IP address
If using autoregistration, make sure it's set up right.

If the phone knows the IP address of its CUCM server, you know it received the TFTP file.

If all else fails, you may have a problem with the phone—out of scope.

DELETING UNASSIGNED DIRECTORY NUMBERS

Routine Maintenance—If you're using the strategy of allowing phone auto registration, then changing each DN to it's "real" value, the old DNs aren't released back into the pool for reuse. Instead they're marked "unassigned" and are invisible unless you specifically look for them.

- Problem: Range of autoregistration DNs exhausted
- Symptom: "Error DB Config" on phone

To release the numbers back to the autoregistration pool for reuse,

System → Route Plan Report

- Set the first filter (left-most field) to "Unassigned DNs" & Click "Find"
- Select all the listed DNs (checkboxes to their left) and click "Delete Selected'

This is also how you would clean up the database after modifying your partitions design. Why? When a DN is assigned to a different partition, it still exists in the old partition, flagged as unassigned. They appear as selectable in lists, but don't function because they're not assigned to any device.

CUCM REPORTS

The Cisco Unified Reporting Tool uses the Cisco Tomcat service and RPCs (Remote Procedure Calls) to pull data from

- RTMT (Real Time Monitoring Tool) counters
- CDR (Call Detail Records) and the CDR Admin & Reporting Database
- CUCM database
- Disk Files—traces and logs
- Prefs settings
- CLI
- RIS (Real-time Information Server)

Ensure that the Tomcat service is running and that HTTPS traffic can flow to & from the servers.

Generating Reports

- Be a member of the CCM Super Users Group (by default only the CUCM application administration account is)
- Choose the unified reporting tool from the top-right drop-down or use the direct URL: https://<IP>/cucreports/
- From the System Reports menu (left pane), choose a report. The system will show the most recent run's output for that report. Check the timestamp for usefulness. An icon at the top right can generate a fresh report. If the report has never run, you'll get a message and a link to generate a new report. A green checkmark icon on the report means it ran successfully
- Other buttons (top-right, beside report title) on the report run page allow you to upload an XML report from your PC to the server, download it to your PC, or run it again.

Report Uses

- Troubleshooting
- Maintenance—configuration or load mismatches, summarize system information
- System Analysis—list phones by type, feature, etc.

CAR TOOL

CAR (Call detail record Analysis and Reporting) Tool—every call and its quality metrics can be logged in flat files on the subscriber server and uploaded to the CDR/CAR database on the publisher at a regular interval that you set. Useful for internal administration, or as input to third-party billing applications.

- CDR (Call Detail Record)
- CMR (Call Management Record)—Call quality metrics; Not loaded by default

Reports can be scheduled to run automatically or manually via the web interface (https://<ip>/car).

Activating CAR

(Serviceability) → Tools → Service Activation

Select the Cisco CAR Web Service and click [Save]

- If you're using an external billing server, also activate the Cisco SOAP (Simple Object Access Protocol) CDROnDemand Service

CDR Service Parameters—set per server

(Admin) → System → Service parameters

- Select a server from the first drop-down
- Select the "Cisco CallManager" service
- Click the [Advanced] button at the top of the page to display all parameters and adjust the following as desired:
    - CDR Enabled Flag—should CDRs be generated (default false). Set on each server
    - CDR Log Calls with Zero Duration Flag—(default false) log calls that didn't connect or lasted less the 1 second. Unsuccessful calls (reorder tone or busy trunk failure) are logged no matter what
    - Call Diagnostics Enabled—(default disabled) whether to generate CMRs. Choices are never, generate only if CDRs are also being generated, and always
    - Display FAC (Forced Authorization Code) in CDR—(default false)
    - Show Line Group Member DN in finalCalledPartyNumber CDR Field—(default false; the Hunt Pilot number is recorded, not the DN) For calls to Call Hunting systems, should the Hunt Pilot number or the DN that picked up the call be recorded in the CDR.
    - Add Incoming Number Prefix to CDR—(default false) Several incoming prefixes are defined in the service parameters. Should the incoming prefix be added to the calling party number in a CDR? "Prefixes added to an inbound call are always recorded in CDRs; this setting controls whether prefixes are added to CDRs if they are added to outbound calls."

CAR Tool Users—3 kinds of users have access to the tool:

- Administrators—Total access. Any user or application can be given admin access to CAR by making them a member of the "Standard CAR Admin Users Group"
- Managers—User, department, and QoS reports. Who's a manager? In CM Admin, if User A is selected in the "Manager User ID" field on user B's configuration page, then user A can run manager reports on user B. Automated reports can be delivered to a manager's e-mail
- Users—Must be a member of the "standard CCM End Users Group." Users can receive billing reports by e-mail for specific date ranges regarding devices associated with their account.

CDR & CMR ARCHITECTURE

CAR Data—Combination of CDRs and CMRs. Several of each can be generated for each call. Collected in a CUCM server's local log & periodically uploaded to the CDR repository node using SFTP. The repository node runs the CDR Repository Manager Service, which can send the files to up to 3 configured locations (typically third party billing servers).

CDR—Generated by CUCM servers processing calls. Contain called & calling numbers, timestamps begin & end, why the call was disconnected.

CMR—latency, jitter, packet loss, amount of data sent during call.

CAR Parameters

- Mail—where to send the reports
- Dial-Plan—configure to match the local calling pattern so CDRs will be interpreted correctly (e.g. 4-digit calls classified as on-net & 7-digit as local.) Default settings are based on the NANP
- Gateways—Gateways in CUCM are automatically added & deleted, but the area codes local to the gateway must be added so the reports can determine which calls are long distance
- COMPANY_NAME—64 char max. Appears in report headers
- CAR Scheduler—what types of records are loaded (raw data pulled from the call processing nodes to the repository node), at what intervals, and for how long.
- Purging—Automatic (default) or manual. Adjust the high & low water marks for starting & stopping the purge based on database disk space utilization. Records are selected for purging based on their age.
- Automatic Report Generation—Can choose reports & whether to email them. Report interval (daily, weekly, monthly) is fixed but start time ca be customized in the scheduler.

Exporting CDR & CMR Records as a .csv file for import into a billing application

(From CAR tool) CDR → Export CDR/CMR

- Set from & to dates
- Under "Select Records," check CDR Records, CMR Records, or both & click "Export File"
- (new window) Choose "CDR Dump" or "CMR Dump" & click "Save As"
- The "Delete File" checkbox purges the downloaded records from the CAR database, controlling its size.

GENERATING CDR REPORTS

Reports and who they're available to:

Report	Description	Admin	MGRs	Users
Bills—Individual	Specified date range, detail or summary format. Can be viewed or e-mailed	X	X	X
Bills—Department	Call & QoS data in detail or summary. Can select specific users or all users that report to the manager	X	X	
Top N by Charge	List of N users in order of call charges over period List of N call destinations by charges over period List of N calls by charge over period	X	X	
Top N by Duration	Users sorted by duration, destinations in order of duration or calls in order of duration	X	X	
Top N by # of Calls	Users or extensions by number of calls	X	X	
CUCM Assistant—Manager Call Usage	Summary or detail information for call completion by Managers using CUC Manager Assistant. Report can list calls the managers made for themselves, calls that assistants handled for the managers, or both	X		
CUCM Assistant—Assistant Call Usage	Can list calls assistants make for themselves, handled for managers, or both	X		
Cisco IP Phone Services	Show selected IP phone services, the number of users subscribed to the services, and the utilization % for each	X		

Example Report Generation—CAR Report Tool https://<ip>/car

User Reports → Top N → By Number of Calls

- The next screen sets parameters, like call types, user types, date range, and N (# of records)
- Click [View Report] (or [Send Report])

SYSTEM REPORTS

Still in the CAR tool, several system reports exist. Acronyms for reference:

- FAC (Forced Authorization Code)
- CMC (Client Matter Code)

Report	Description	Admin	MGRs	Users
QoS—Detail	Detailed QoS statistics for calls handled by CUCM during the date range. Useful for system-wide voice quality monitoring	X		
QoS—Summary	Pie chart format showing QoS ratings for calls of specified classifications and time frame. Includes a summary table for calls per QoS grade	X	X	
QoS—By Gateway	% of calls per selected gateways meeting defined QoS criteria. Can be generated hourly, daily, weekly	X	X	
QoS—By Call Type	% of calls by selected type that meet chosen QoS criteria. Can be generated hourly, daily, weekly	X		
Traffic Summary	Call volume for selected call types and QoS categories for time frame. Useful for # of calls hourly / daily / weekly	X		
Traffic Summary by Extension	Call volume per specified extension(s) and call types during time frame	X		
FAC/CMC—Client Matter Code	Called & calling numbers, duration, and call classification for time period	X		
FAC/CMC—Authorization Code Name	Called & calling numbers, timestamps, duration, and call classification for specified time period by FAC name (includes authorization level)	X		
FAC/CMC—Authorization Level	Called & calling numbers, timestamps, duration, and call classification for specified time period by FAC authorization level (includes FAC name)	X		
Malicious Call Details	Details of calls tracked by the MCID (Malicious Caller Identification) service during time period	X		
Precedence Call Summary	Bar graph—summary of calls that were preempted by the selected MLPP levels for the time period	X		
System Overview	High-level information about the CUCM network	X		
CDR Error	Statistics for errors during CDR data transfer	X		

Device Reports

- Gateway—Detail, Summary, and Utilization reports showing gateway utilization according to various call and gateway criteria.
- Route Patterns and Hunt Groups
    - Route / Line Group Utilization
    - Route Pattern / Hunt Pilot Utilization
    - Hunt Pilot Summary
    - Hunt Pilot Detail
- Conference Bridge—monitor conference resources with Conference Call Detail & Conference Bridge Utilization reports
- Voice Messaging—Estimates the % utilization of voice-message devices

CISCO UNIFIED RTMT

RTMT (Real Time Monitoring Tool)—A client application on an administrative workstation to collect, view, interpret, and monitor the various counters, trace files, and logs generated by CUCM, CUC, and CUP. The application can be downloaded from CUCM, CUC, CUP, and CUCCX (Contact Center Express) servers. The tool is specific to each server product, except for CUCM and CUC, which share the same one. Only one RTMT instance can be installed on a workstation. Connects to the server via HTTPS & monitors system performance, device status, device discovery, CTI applications, and voice-messaging ports.

AMC (cisco Alert Manager Collector service)—allows the RTMT to collect info in realtime.

Services and Servlets that provide RTMT with info & capabilities (all names actually start with "Cisco…"). Auto-Start means that the service starts up automatically after the installation.

SERVICE /SERVLET	DESCRIPTION	AUTO-START
Communications Manager Servlet		X
RIS Data Collector	(Real-time Information Server)—performance, counter statistics, alarms generated, etc.	
Tomcat Stats Servlet	Allows you to monitor the Tomcat perfmon counters using RTMT or the CLI	
Trace Collection Servlet & Service	Together, these support trace collection and allow their viewing via the RTMT client	
Log Partition Monitoring Tool	Monitors disk usage on the log partition.	X
SOAP-Real-Time Service APIs	Enable collection of real-time info for devices and CTI applications.	X
SOAP-Performance Monitoring APIs	Enables performance monitoring counters for various applications through SOAP APIs.	X
RTMT Reporter Servlet	Enables publication of reports for RTMT	X
Serviceability Reporter	Enables publication of reports for RTMT	

Once added to the standard "CCM Admin Users" and standard "RealtimeAndTraceCollection" groups, end users (or application users) can use their normal User ID and password to log into RTMT. The standard "CCM super users" group has sufficient privileges, too.

Administrative capabilities of RTMT include

- Monitor predefined system health objects
- Generate e-mail alerts for objects that exceed defined range
- Collect & view trace files from different services
- View syslog messages
- Configure and monitor performance counters

RTMT Interface—a GUI that includes the following menus and options: [verbatimish]

- File—Save, restore, and delete RTMT profiles, monitor Java Virtual Machine (JVM) info., access the report archive, access the Unified reporting tool, log off, or exit
- Edit—Set up categories for table format views, set polling rates for performance counters and devices, show/hide Quick Launch Channel, and edit trace settings for RTMT
- Window—Close current (or all) RTMT windows
- Application—Administration, serviceability, and application-specific interfaces, depending on which RTMT is in use
- RTMT—contents (submenus) depend on whether you're using the RTMT with a CUCM server of CUC:

Submenu	Description	CUCM	CUC
System	Monitoring of platform health, including CPU and memory and disk utilization. Administrators can set up and monitor various performance counters, alerts, and traces, and access the Trace & Log Central tool and syslog viewer	X	X
Voice / Video	Summary information applicable about the server, search for devices, monitor services	X	
IM and Presence	Summary information applicable to the CUP application	X	
Unity Connection	Port Monitor Tool and view statistics and summaries applicable to CUC		X
Analysis Manager	Display configuration and licensing summaries, and use the Call Path Analysis tool	X	

Monitoring CUCM with RTMT (examples)

- Voice and Video Summary—Graphs for registered phones, calls in progress, and active MGCP gateway ports and channels
- Gateway Activity (per gateway type, not per gateway)—summary of calls in progress for a specific type of gateway (MGCP FXS, FXO, T1, PRI, or H.323). Can also show number of completed calls per gateway type (per server or per cluster)
- Device Search—Table format with one row per device & criteria in columns (can choose which criteria columns to include). Can search based on:
    - Devices—Can search for phones; gateway, H.323, CTI, and voice managing devices; media resources; hunt lists; and SIP trunks
    - Criteria—Can search based on status ([un]registered, rejected, any other status configured in the database), device model. Phones can also be limited by protocol.
- Database Summary—replication status (including replication status for each server in a cluster), # of replicates, # of change notification requests queued in the database and in memory, # of connection clients.
- Call Activity—4 graphs showing Calls completed, attempted, in progress; and total logical partition failures.

  Customization—The "System → Performance" screen can select up to 6 graphs or charts per server

- Alert Central—Chart format view of both predefined and custom-configured alerts.
  Drill Down—Right-click on an alert and choose "Alert Details"
- Remote Browse—can browse through trace files on a server if you don't want to download them using (S)FTP. During debugging, this can be worth the load placed on the server.
  (RTMT) System → Tools → Trace and Log Central → Remote Browse
- Syslog—Choose the node and file (names are based on date/time) to view
  (RTMT) System → Tools → Syslog Viewer

DRS

DRS (Disaster Recovery System)—Scheduled or manual backups of CUCM and CDR/CAR databases, plus its own settings so it doesn't need to be reconfigured after a restore.

- Config—CLI or GUI. Interface via the DRS web page to the master agent. The platform admin account has access by default; others can be added.
  https://<ip>/drf (or the drop-down navigation at the top of the CUCM admin page)
  Yes, it really is drf; the F stands for Framework
- Storage—SFTP only; local tape drive option has been disavowed
- Distributed architecture—Master agent stores system-wide component registration info, maintains the schedule & sends backup tasks to local agents, and stores the backups (writes them to remote SFTP)
- Cannot be used for upgrade/downgrade (requires same version), but might be useful for migration to virtualization (author doesn't mention this)
- Common to all Linux-based UC apps, but which components are backed up varies:

Component	CUCM	CUP	CUC
Platform	X	X	X
License Manager	X	X	X
Trace Collection Tool	X	X	X
Syslog	X	X	X
Relevant Database—CUCM, CUP or CUC	X	X	X
TFTP / MoH Files	X		
CDR / CAR Data	X		
XCP Data		X	
CUP Data		X	
Mailbox Store			X
Greetings			X

Config: Set Up a Backup Device—up to 10 can be created

(DRS) Backup → Backup Device

- Name the backup device being created
- Provide the SFTP server's IP, root path, & login account; click [Save]

Config: Set Up a Scheduled (recurring) Backup—resource intensive; schedule accordingly

Backup → Current Status

- Progress of a backup, with % for each component. Those at 100% have a link to the log file.

Backup → Scheduler

- Click [Add New], name the schedule, and pick a backup device (config'd above)
- Choose what features you want backed up. Options depend on the application:

Application	Features That Can Be Backed Up
CUCM	CCM, CDR_CAR
CUC	CONNECTION_DATABASE, CONNECTION_GREETINGS_VOICENAMES, CONNECTION_MESSAGES_UNITYMBXDB1, CUC
CUP	CUPS, CUP

- Define a backup schedule & enable the job

Backup → Manual Backup

- All the same options except that it just runs immediately

Restore from Backup—this is a replace, not a merge.

Restore → Restore Wizard

- Select a backup device to read from & the correct backup file from the list on that device
- Choose the feature(s) to be restored
- When restoring from an SFTP server, you can select the optional "File Integrity Check" to slow down the restore, the server, and the network.
- Choose which server(s) should be restored. When restoring the publisher, DRS automatically restores the subscribers too.

Restore → Status

- To monitor progress