Cisco Unified Communications Management

Service Description

Table of Contents

1. Introduction

Unified Communications (UC) is an evolving set of technologies that automates and unifies human and device communications in a common context and experience. It optimizes business processes, increases user productivity, and enhances human communications by reducing latency, managing flows, and eliminating device and media dependencies.

In its broadest sense, UC integrates real-time, enterprise, communication services such as instant messaging (chat), presence information, voice (including IP telephony), mobility features (including extension mobility and single number reach), audio, web & video conferencing, fixed-mobile convergence (FMC), desktop sharing, data sharing (including web connected electronic interactive whiteboards), call control and speech recognition with non-real-time communication services such as unified messaging (integrated voicemail, e-mail, SMS and fax). UC is a set of products that provides a consistent unified user-interface and user-experience across multiple devices and media-types.

UC allows an individual to send a message on one medium, and receive the same communication on another medium. For example, one can receive a voicemail message and choose to access it through e-mail or a cell phone. If the sender is online according to the presence information and currently accepts calls, the response can be sent immediately through text chat or video call. Otherwise, it may be sent as a non-real-time message that can be accessed through a variety of media.

Multiple vendors supply UC technologies today. Popular vendors include Cisco, Microsoft, and Avaya. The scope of this document is restricted to Cisco UC and managed services from CDI for Cisco UC.

2. CDI Next Gen Managed Services for Cisco UC

Organizations today rely on UC and Voice-over-IP (VoIP) to deliver vital communications services. CDI Next Gen Services (NGS) for Cisco UC infrastructure is designed to provide clients with a comprehensive suite of 24x7 monitoring, management, maintenance, and administration services for management of both core Cisco UC infrastructure and UC end-users in the enterprise. CDI NGS for UC and VoIP ensures these services meet the availability, reliability, and quality demands of end-users by monitoring and proactively managing each and every UC component in their environment, including and extending into the network infrastructure.

CDI supports two major service levels for UC with its managed services.

	SERVICE LEVELS	
	"CORE"	**"ADVANCED"**
Summary	Management of core UC infrastructure only excluding Phones, End-Users, Agents, & Mailboxes	Management of end-to-end UC infrastructure including Phones, End-Users, Agents, & Mailboxes
Description	For enterprise UC environments, to meet needs of clients, who have invested in skillsets for UC end-user support, but either don't have or don't want to invest in skillsets to manage and support UC core back-end systems & apps for various reasons – cost, skills availability, risk, focus, etc.,	For enterprise UC environments, to meet needs of clients, who either don't have or don't want to invest in skillsets to manage and support end-to-end UC systems (including core UC back-end systems & apps, as well as end-user phones, mailboxes, and agents) for various reasons – cost, skills availability, risk, focus, etc.,
Offering	• CDI provides full management services for all core UC infrastructure – devices, applications (e.g. call manager, call center, unity, etc.,) • CDI will not manage phones, end-users, agents and mailboxes • CDI provides professional services to handle related add-on activities	• CDI provides full management services for all core UC infrastructure – devices, applications (e.g. call manager, call center, unity, etc.,) • CDI will also manage phones, end-users, agents, and mailboxes • CDI provides professional services to handle related add-on activities

Some example use cases supported by CDI for the above service levels include the below:

EXAMPLE USE CASES SUPPORTED	SUPPORTED IN "CORE" SERVICE LEVEL	SUPPORTED IN "ADVANCED" SERVICE LEVEL
Call center down	✓	✓
UCCE in split brain	✓	✓
End-to-end call management for end-users, agents		✓
Some users in UK office not able to call local pizza chain		✓
Choppy voice during monthly sales conference calls for Austin site users		✓
Phones switching back and forth between sub1 and sub2		✓
Phones unregistered for work-from-home users		✓
Analysis of agents logged in; calls in queue		✓
Analysis of top-talkers		✓

Multiple benefits accrue to the client as a result of CDI UC managed services. Some of them include:

- Comprehensive end-to-end solution for UC managed services
- High service levels for UC
- Access to advanced UC skillsets
- Free up of skilled resources to work on more strategic projects
- Service delivery & governance
- Risk management
- Cost control, lower TCO, and improved ROI of end-to-end UC environment

3.UC Service Management Methodology & Scope

3.1. Service Management - Operations

3.1.1. Service Entitlements

Service entitlements for the various UC managed services levels are below

SERVICES ENTITLEMENTS	"CORE" SERVICES	"ADVANCED" SERVICES	CADENCE
SERVICE OPERATIONS FUNCTIONS:			
Alert Monitoring	✓	✓	24x7
Alert Management	✓	✓	24x7
SOP and Runbooks	✓	✓	As needed
Runbook automation	✓	✓	As needed
Incident Management	✓	✓	As needed
RMA coordination for hardware* parts (for Core infrastructure elements, excluding phones)	✓	✓	As needed
Telco vendor management	✓	✓	As needed
Problem Management (for Core infrastructure elements, excluding phones)	✓	✓	As needed
Change Management (for Core infrastructure elements, excluding phones)	✓	✓	As needed
Circuit Management	✓	✓	As needed
Service Requests	✓	✓	As needed
Availability Management	✓	✓	24x7
Service Maps	✓	✓	Onboarding/Changes
SLA Management	✓	✓	24x7
Mailbox Management (End User & Agents)		✓	As needed
Agent Desktop Management (Agents)		✓	As needed
IP Phone Management (End User & Agents)		✓	As needed
RMA coordination for hardware parts (Phones)		✓	As needed
Problem Management (End-Users, Phones)		✓	As needed
Change Management (End Users)		✓	As needed
Remote Access to IP Phones		✓	As needed
MACD Service Requests (End-Users, Phones)		✓	As needed
RELEASE MANAGEMENT FUNCTIONS:			
Patch Management (Minor releases; for Core infrastructure elements, excluding phones)	✓	✓	Monthly
Product Lifecycle Management (for Core infrastructure elements, excluding phones)	✓	✓	Quarterly
Phone firmware upgrades		✓	Quarterly
Product Lifecycle Management (Phones)		✓	Quarterly
CAPACITY MANAGEMENT:			
Performance Management	✓	✓	Monthly
Voice Quality Monitoring (IP SLA)	✓	✓	24x7
Performance Reports	✓	✓	Monthly
BACKUP AND RESTORE FUNCTIONS:			

Configuration Management	✓	✓	Daily
UC Application Backup Management	✓	✓	Daily
Restore of Network Device Configuration	✓	✓	As needed
Restore of Hypervisor, OS, UC Application	✓	✓	As needed
SERVICE OPTIMIZATION FUNCTIONS:			
Health checks	✓	✓	Monthly
Trunk Optimization	Add-on	✓	Quarterly
QoS Optimization	Add-on	✓	Quarterly
ONLINE TOOLS:			
Monitoring Portal	✓	✓	24x7
Performance Reports	✓	✓	24x7
Dashboards	✓	✓	24x7
Customer Portal	✓	✓	24x7
End User Portal		✓	24x7
UC SECURITY MANAGEMENT:			
Voice signal encryption		✓	As needed
Voice traffic encryption		✓	As needed
Voice mail encryption		✓	As needed
CISCO UC APPLICATIONS SUPPORT:			
Cisco VOIP Phone Management		✓	24x7
Cisco Agent Desktop Management		✓	24x7
Cisco Jabber Management		✓	24x7
Cisco WebEx Management		✓	24x7
Cisco Unified Attendant Console Management		✓	24x7
Cisco Web Attendant Management		✓	24x7
Cisco Unified Communications Manager Management	✓	✓	24x7
Cisco Unified Presence Server Management	✓	✓	24x7
Cisco Unified Communications Manager Express Management	✓	✓	24x7
Cisco Unity Connection Management	✓	✓	24x7
Cisco Unity Express Management	✓	✓	24x7
Cisco Unified IM and Presence Management	✓	✓	24x7
Cisco Unified Mobility Management	✓	✓	24x7
Cisco Business Edition Management	✓	✓	24x7
Cisco Expressway Management	✓	✓	24x7
Cisco TDM Gateway Management	✓	✓	24x7
Cisco Voice Gateway Management	✓	✓	24x7
Cisco Unified Border Element Management	✓	✓	24x7
Cisco UCCX Management	✓	✓	24x7
Cisco UCCE Central Controllers (Router/Logger) Management	✓	✓	24x7
Cisco UCCE Peripheral Gateways Management	✓	✓	24x7
Cisco UCCE Administration and Real-time Data Server Management	✓	✓	24x7
Cisco UCCE Historical Data Server and Detail Data Server Management	✓	✓	24x7
Cisco UCCE Routing Functions Management	✓	✓	24x7
Cisco UCCE Pre-Routing and Post-Routing Functions Management	✓	✓	24x7
Cisco UCCE Customer Profile Routing Management	✓	✓	24x7
Cisco UCCE Agent Request API Management		✓	24x7

Cisco UCCE Reporting Management	✓	✓	24x7
Cisco UCCE Universal Queue Management	✓	✓	24x7
Cisco UCCE Remote-Agent Support Management		✓	24x7
Cisco UCCE Unified IP IVR Management	✓	✓	24x7
Cisco UCCE Outbound Dialer Management	✓	✓	24x7
Cisco UCCE Email Interaction Management	✓	✓	24x7
Cisco UCCE Web Interaction Management	✓	✓	24x7
Cisco Unified Customer Voice Portal Management	✓	✓	24x7
Cisco Unified Call Studio Management	✓	✓	24x7
Cisco Finesse Server Management	✓	✓	24x7
Cisco MediaSense Management	✓	✓	24x7

** If client has purchased tech support services from vendor, then CDI will co-ordinate tech support with vendor. Client must have valid maintenance or tech support agreement with vendor for UC and VoIP devices. Expiration of maintenance or technical support agreement places limits on services. Technologies placed in 'End of Life' by vendor will not be supported.*

ADD-ON OPTIONS:
Integration adapters
BC/DR management
Onsite support
Application upgrades (Major releases)
Netflow Analytics
Intelligent Business Operations (trends)

Various entitlements are described in detail below.

3.1.2. Alert Monitoring

CDI alert monitoring function enables the remote detection of system alerts reported by hardware and software components within the UC infrastructure and follows a defined escalation matrix to escalate the alert to the correct party. Scope covers monitoring of alerts whose severity are classified as either "Emergency", "Critical", or "Error" by the product manufacturer.

Basic Health Monitoring For All UC Core Systems & Applications

Monitor Type	Description
System	• Usage of processor, hard disk, virtual memory, and RAM • Status of network interfaces on physical and virtual machines hosting UC applications
Environment	• Status of system fan, system temperature sensor, and system power supply of physical servers hosting UC applications
Application	• Status of all critical services supporting UC applications

Fault Monitoring on Cisco Unified Communications Manager

Monitor Type	Description
CPU Pegging	Monitors percentage of CPU load on a call processing server
Insufficient Hard Disk Space	Monitors percentage of used disk space in log partition
Low Virtual Memory	Monitors if available virtual memory is running low
Fan Down	Monitors that a required fan is operating correctly
Temperature High	Monitors if a temperature sensor's current temperature exceeds relative temperature threshold
Temperature Sensor Down	Monitors if server's temperature is outside of normal operating range and if system should be shut down
Power Supply Down	Monitors if power supply state is down
Service Down	Monitors if one of critical services is not running.

Code Red	Monitors if Cisco Unified Communications Manager has remained in a Code Yellow state for an extended period and cannot recover
Code Yellow State	Monitors if Cisco Unified Communications Manager has initiated call throttling due to an unacceptably high delay in handling incoming calls
CTI Link Down	Monitors if CTI Manager has lost communication with all Cisco Unified Communications Managers in cluster
Physical Disk Down	Monitors if hard drive failure on Cisco Unified Communications Manager
DB Replication Failure	Monitors if failure with replication of Communications Manager database
SDL Link Out Of Service	Monitors if local Cisco Communications Manager has lost communication with remote Communications Manager
HTTP Service Down	Monitors if HTTP service cannot be used to communicate to all Cisco Unified Communications Managers in cluster
Authentication Failed	Monitors if there was an authentication failure for a login attempt
High Analog Port Utilization	Monitors if Gateway port is unavailable or is facing out-of-service issues
Media List Exhausted	Monitors if all available media resources defined in media list are busy
Hardware Failure	Monitors if a hardware failure has occurred in Communications Manager
Number Of Registered Phones Dropped	Monitors count of registered phones in cluster that dropped more than configured percentage between consecutive polls
ICT Call Throttling	Monitors if Cisco Communications Manager has detected a route loop over H323 trunk
Cisco DRF Failure	Monitors if DRF backup or restore process encountered errors
Core Dump File Found	Monitors if server crashed
High Digit Port Utilization	Monitors if one of MGCP gateways has a high port utilization (T1 CAS, T1 PRI, E1 PRI, BRI, and/or E1 CAS)
High Resource Utilization	Monitors if high resource utilization for MTP, MOH, conference, or transcoder resources
CDR Maximum Disk Space Exceeded	Monitors if disk usage of CDR (Call Detail Record) files exceeded maximum allocation
Thread Counter Update Stopped	Monitors if current number of processes or threads have exceeded maximum number of tasks
SOAP Not Reachable	Monitors if a device experienced failures with connectivity of Simple Object Access Protocol (SOAP) while polling
System Version Mismatched	Monitors if there is a mismatch in system version among all servers in cluster
Route List Exhausted	Monitors if all available channels define in route list are busy
Server Unreachable	Monitors if host is not reachable
D Channel Out Of Service	Monitors if MGCP D channel is out of service

Additional Cisco UC monitors and alerts supported by CDI are listed in Section **Error! Reference source not found.** (Appendix). T hese include the following monitors and alerts:

- CUCM alerts - Section **Error! Reference source not found.**
- Unity Connection alerts - Section **Error! Reference source not found.**
- IM & Presence alerts - Section **Error! Reference source not found.**
- UCCE alerts - Section **Error! Reference source not found.**
- UCCX syslog monitors - Section **Error! Reference source not found.**

CDI also monitors the UC infrastructure utilizing standard SNMP data collection, SNMP Trap receiver, Syslog monitoring, syslog, SOAP (*Simple Object Access Protocol)* , AP, Service Provider SIP trunk monitoring, Cisco RTMT (email integration with Vistara), synthetic transaction (IPSLA) monitoring and call logs. The CDI platform also enables CDI staff to securely and remotely access monitored devices to perform standard operating procedures (SOPs) or advanced troubleshooting services.

UCM/UNITY (STANDARD AND EXPRESS), UCCX, PRESENCE
Device Availability: Up/Down
Device Health: (CPU and Memory and Disk Utilization)
Interface Status: Up/Down
Interface Performance: – Utilization, In/Out Traffic Rate
Interface Errors: Error and Discard Rate, CRC and Collision Errors
Critical Services Availability: CallManager Service, Cisco CTI Manager Service, Cisco CTL Provider Service, Cisco Telephony Call Dispatcher, Cisco TFTP Service, SNMP Service, Unity Services, UCCX Services
Call Statistics (active calls, calls completed, calls in progress, Active Ports, Ports in service, Trunk Activity, SIP Activity), FXO/FXS ports
Hardware Monitoring: Disk, Memory Modules, Chassis Temperature

CALL QUALITY (QOS)
Jitter, Latency, Packet Loss, MOS Listening Quality, Severely Concealed Seconds

GATEWAYS
Device Availability: Up/Down
Device Health: (CPU and Memory and Disk Utilization), License Usage
Hardware Monitoring: Disk, Memory Modules, Chassis Temperature
Interface Performance: Utilization, In/Out Traffic Rate
Interface Errors: Error and Discard Rate, CRC and Collision Errors
Environment Check: Fan, Power, Temperature and Voltage Status
Buffer Usage: Small, Medium, Large and Huge buffer utilization and failures

IP PHONES
Availability and Registered State

Proactive Synthetic Transactions for VoIP using **Cisco's IP SLA** Technology. These monitors understand VoIP traffic characteristics and ensure successful implementation and sustained service level compliance for VoIP. VoIP service level killers such as excessive jitter, packet loss, latency or poor MOS are exposed by these monitors to help pinpoint bottlenecks.

Past Call Analysis from call records of the UCM. With these monitors, all completed calls are processed to check for quality that was experienced, duration, traffic, and other parameters. These values are then presented in real-time reports for analysis.

3.1.3. Alert Management

CDI alert management function extends alert monitoring abilities by CDI services to further investigate, diagnose, determine the cause for alert generation, and take corrective action on the alert. Scope covers management of alerts whose severity are classified as either "Emergency", "Critical", or "Error" by the product manufacturer.

3.1.4. Standard Operating Procedures (SOP) and Run books

CDI SOP function enables the execution of a set of step-by-step instructions that are used to achieve predictable, standardized, and desirable results for the alert management function. Currently CDI has created SOPs to act on thousands of alert types that have severity defined as "Emergency", "Critical", or "Error" by the product manufacturer. These include runbooks for nearly 5,800+ alerts generated by CUCM, Unity Conn, & UCCX. These SOPs are stored within the CDI knowledge-base and used by the CDI services team to remediate alerts detected by the alert monitoring function. SOPs are an ongoing effort and CDI continuously adds SOPs to the knowledge-base.

CDI supports custom SOPs in addition to CDI predefined SOPs. This means that the solution provider or the end client can submit custom SOPs to be executed when an alert is triggered for an issue on UC device.

- Incoming alerts will initially be validated to identify false alerts or alerts where no action is required
- Actionable alerts will be ticketed by the appropriate CDI personnel, and documented SOPs will be executed by CDI as first level of support
- If SOPs fail to resolve the problem, the ticket will be updated and immediately escalated to CDI technicians for further troubleshooting and remediation

The following are examples of additional UC/VoIP SOPs executed by CDI:

Device Status (Up/Down) on Critical Alerts	CDI runs diagnostics to check status of problematic device from a different device in same network in order to eliminate any LAN/WAN issues.
Memory, Processor, Buffer Utilization High on any Network Device	CDI validates utilization by logging into device, and identifying reason for high utilization.
Inbound/Outbound Errors on Interfaces	CDI checks errors on interfaces and clears errors. If errors persist on WAN link at same rate, CDI checks physical connectivity issue and then escalates to ISP.

Interfaces or Link Down	CDI logs on to device and checks if interface is "admin down" or "protocol down." In case of "admin down," CDI will alert client and if "protocol down", CDI will check logs to see if issue is due to network flap.
VPN Tunnels (Mainly For Firewalls, But Can Be Applied For Routers Also)	CDI checks tunnel status, and if tunnel is down, then determines reason.
Cisco Device Hardware Issues (e.g. Voltage, Fans, Temperature, Power)	CDI runs SOPs for remediation of power, temperature, fans and voltage issues. SOPs include follow-up on inspection of facilities such as power, cooling systems, etc.,
Cisco QoS issues (Jitter, Packet Loss, MOS)	CDI executes SOPs to check impacting factors, such as UDP delays and changes to QoS, routing, etc., as needed.
Poor Call Quality Metrics	CDI runs SOPs to validate phone specific call quality checks and fixes QoS, routing, and configurations as needed.
Buffer Statistics	CDI executes SOPs to validate buffer hits, misses, failures, etc.,

3.1.5. SOP and Runbook Automation

CDI SOP automation and runbook automation functions promote operational efficiencies by shifting the processing of the step-by-step instructions defined in SOPs and runbooks from humans to computers. Examples of SOP or runbook automation include "disk space clean-up", etc. SOP and runbook automation is an ongoing effort. As SOPs and runbooks mature and reach a point where all possible outcomes (both positive and negative) of executing a command are captured, and no ambiguity exists, then these SOPs and runbooks are automated.

3.1.6. Incident Management

CDI incident management function enables and provides the process, people, and tools required to quickly restore any unplanned interruption or reduction in quality of UC systems. This function covers in its scope the following: incident detection, recording, classification, analysis, diagnosis, resolution, and recovery of the incident.

3.1.7. RMA Coordination For Hardware Parts & Hardware Vendor Escalations and Follow-ups

CDI RMA coordination function extends the alert and incident management responsibilities by providing additional vendor coordination activities that is required to quickly order and ship replacement parts to the end-client site. To execute this function, the following is required of the client:

- Client shall have an active warranty or maintenance service contract with the respective product manufacturer
- Client shall have signed a Letter of Agency (LoA) during the services on-boarding phase, that authorizes CDI to act as a representative of the client, and empower it to contact and co-ordinate with the product manufacturer when a hardware failure occurs

CDI will contact hardware vendor (tech support) in the event of any hardware failure. CDI will create a ticket and work with the vendor online to identify the problem, perform the RMA process, and get the replacement of the device or the faulty part as applicable.

- The SLAs are as applicable in the hardware support contract

3.1.8. Circuit Management & Telco or ISP Vendor Management

The circuit management function extends the alert or incident management responsibilities for telco circuit related issues (SIP, PRI, or Analog). CDI will support vendor escalations to ISPs or telcos for issues related to internet, leased lines, or MPLS circuits in the event of link down, high latency, or high interface errors. The process is as follows:

1. Open a ticket (either phone or online ticket system) with the respective telco service provider, and
2. Follow up with the telecom service provider until the circuit is restored to normal
3. Summary of conversations with the ISP or telco will be updated within the ticket
4. Response and resolution SLAs of vendors are applicable to issues escalated by CDI

Client shall have signed a Letter of Agency (LoA) during the services on-boarding phase that authorizes CDI to act as a representative of the client, and empower it to contact and co-ordinate with the telecom service provider when a telco circuit related issue occurs. CDI requires the client to maintain valid support contracts with all ISPs and telcos.

Note: *It is mandatory that CDI be allowed to monitor internet or WAN links on interfaces of managed devices, in order for CDI to support ISP or telco vendor escalations.*

3.1.9. Vendor Coordination & Vendor Tech Support

If there are issues identified by CDI services that requires help from the UC system vendor or other 3rd party vendors, CDI will contact the tech support team of vendor to resolve them.

- The SLAs are as applicable by the Vendor Tech Support contract
- CDI recommends that client maintain valid support contracts for all managed UC and network devices
- It is required that the client authorize CDI to act on their behalf when coordinating with the support team

3.1.10. Device Configuration Backup

Periodic configuration backup of VoIP devices is performed along with difference reports between any two revisions of configuration. CDI will take a backup of device configurations of Cisco routers, switches, and voice gateways (CLI based) every 15 days, or during any change in device configuration. The configuration backup will be stored in the CDI cloud for configuration management.

NOTE: *If supported by the network device, configuration backup will be an automated process. If an automatic process is not supported by device, then CDI will not be able to perform backup network device configuration.*

Deliverables:

- If configuration backup did not run during the scheduled time, then CDI will investigate the issue and resolve it. If devices have missed or failed two (2) consecutive scheduled backup events, then CDI will execute SOPs to resolve issues.
- If backup configuration event caused device related issues, then CDI services will engage within the defined SLA.

3.1.11. UC Application Backup

CDI will utilize native backup tools available in the UC and UCCE application to securely backup and store application data to a customer provided secure data store as defined by customer's backup schedule.

CDI will also monitor status of backup job and generate alerts for backup failures and will follow the incident management process to resolve issue.

NOTE: Client will be responsible for providing a secure data store for storing backup data.

3.1.12. Problem Management (For Core Infrastructure Elements, Excluding Phones)

CDI problem management function (for UC core infrastructure, excluding phones) enables and provides the process, people, and tools required to investigate and determine the root cause of recurring incidents on core UC devices (e.g. applications, operating systems, hypervisors, server hardware, network, etc. – but excluding end-users, phones, mailboxes, and agents). It also develops a plan of action to address the root cause while following appropriate change management processes to implement action items. Goal is to avoid similar incidents from occurring again in future.

CDI will troubleshoot and fix issues for alerts that are generated from existing configuration of UC devices:

- If the SOPs fail to resolve the problem, the ticket will be updated and immediately escalated to appropriate domain expert within CDI to troubleshoot the issue and remediate comprehensively
- If needed, CDI will contact Vendor Tech Support for further troubleshooting and full remediation
- CDI will conduct Root Cause Analysis of critical (P0) incidents to identify underlying problem
- Incidents are fixed within the predefined SLA
- All activities are logged into an ITIL based ticketing system and updated within the ticket with complete chronology and steps taken to remediate the incident

3.1.13. Change Management

CDI change management function enables and provides the process, people, and tools required to ensure that standardized methods and procedures are followed, in order to efficiently and effectively handle any change management activities within the UC infrastructure. A key goal of the change management function is to minimize downtime to UC services.

Changes can be broadly classified as “Standard Changes”, “Non-Standard Changes” and “Emergency Changes”:

- **Standard Changes** means the impact of the change is limited to a single user. Standard changes are pre-approved by client. Please refer to the Moves Adds Changes Deletes (MACD) Section 3.1.14 for the list of standard changes.
- **Non-Standard Changes** means the impact of the change is system wide. Examples include -- apply a patch, reboot a server, change route patterns, add a new gateway, modify SIP Trunk parameters, etc. Non-standard changes require client approval, as well as specification of a maintenance window by client.
- **Emergency Changes** means the impact of the change is system wide, but the change needs to be executed immediately in order to resolve a “Critical” incident. CDI will follow the client’s emergency change management approval process. CDI highly recommends client to categorize emergency changes as pre-approved so as to reduce the time to restore or resolve the critical incident.

Changes in scope are changes that are trigged by alert, incident, problem, and release management functions that are oriented towards either (a) resolving server, application, network, security, and/or storage infrastructure related issues, or (b) enhancing stability and availability of the UC and/or UCCE environment.

Any change request that falls outside the type of changes defined in the MACD Table (Section 3.1.14), but if considered by CDI as implementable and in scope, will require both client approval and approval for a time window. To enable the approval process, CDI will make best effort to generate appropriate information, to enable client to quantify the business impact of the change, if it is made during the time window. Client will be responsible to make the decision, as well as to provide a time window to execute the change.

3.1.14. MACD Support For End-User Management

The following MACD are supported for end-user management for the “Advanced” service level.

MACD
Reset password
Change user
Add user
Unlock mailbox
Add agents
Remove user
Add mailbox
Change lines
Add line
Change call handler
Change CSS
Add phones
Change name
Add EM profile
Change agents
Change call forwarding
Change mailbox
Remove agent
Remove lines
Reset EM PIN
Add admin user

Add Callhandler
Add phantom line
Add speed dial
Add Webview user
Change hunt group
Change phones
Add call park
Add night bell
Add to reskilling tool
Call blocking
Change greeting
Change line settings
Change night bell
Change Supervisor view
Change ToD routing
Change user rights
Enable call monitoring
Logout from EM
Remove hunt group
Remove Webview user

Some constraints:

- High priority MACD service requests to be completed within 24 hours, provided there are no capacity constraints for processing of MACD service requests (e.g. sudden spike in MACD service request demand resulting in high volume of MACDs).
- Number of MACD service requests per month is limited to 5% of total number of end users and agents in scope for engagement. Additional MACD service requests will be handled on a T&M basis. Contact CDI for more details.
- Emergency MACDs that need immediate assistance are to be opened as P0 ticket (i.e. Severity 1) over phone. Emergency MACDs will be charged on a T&M basis at a premium rate. Contact CDI for more details.

3.1.15. Service Requests (SR)

CDI service request function acts as a provision to handle situations that cannot be classified as either (a) incident (b) change request, or (c) project. Example include “Client wants to add a new SIP Gateway”, etc. To efficiently and effectively handle such service requests, the CDI contract typically includes a bucket of professional services hours that may be applied against service requests.

Note: Service requests are those that do not result from disruption of service (i.e., not due to incidents in the infrastructure, monitored events, or change requests arising out of root cause analysis).

Following are some examples of service requests:

- Restore of device configuration due to misconfigurations or device replacement failures
- Upgrade of firmware and/or patches to UC to fix security issues
- Basic configuration changes on features such as hunt group, call park, call pickup, etc.,
- Bandwidth control requests that are on-demand, or as part of remediation
- Enable or disable modules
- Trunk gateway parameter changes that are as part of remediation
- Residential gateway parameter changes that are as part of remediation

3.1.16. Availability Management

CDI availability management function ensures that the UC infrastructure is designed, implemented, and managed to meet the availability requirements of the client for communication and collaboration. This function is executed during multiple phases of the engagement:

- During the "Discovery" phase, the on-boarding team reviews and captures client's requirements for availability for communication and collaboration.
- During the "Design" phase, the existing UC infrastructure is audited to ensure that it can meet the availability requirements for communication and collaboration set by the client. If gaps are identified, then appropriate recommendation and remediation plans are constructed and presented to client to eliminate any single points of failures. In cases where it doesn't make economic sense or technical limitations exist to design and implement a fully redundant setup, then cost effective contingency plans are put in place to ensure client's business requirements are met.
    - For example, assume a 24x7 contact centre where agents work on the same floor in the same building. Since IP phones can only connect to one network switch, in this case, the IP phone, network switch, patch panel, and cable are single points of failure. The solution is to ensure that IP phones of agents within the same team are connected to different network switches. This way, in the worst case, the failure of one switch does not impact all agents in the team.
- During the "Operate" phase, this function is extended to conduct service outage analysis initiatives, determine root cause, analyze trends, and take appropriate actions to ensure that service availability meets defined SLAs.

3.1.17. Service Maps

CDI service map function provides service maps and/or application dependency mapping to key components of UC services infrastructure. The benefits are multiple: (a) enables monitoring of UC services as a single entity even though they are composed of multiple components, (b) aid in identifying root causes of failure and drive allocation of proper resources to rapidly restore the service and resolve the problem. CDI's advanced application mapping technology enables understanding of the physical assets that make up the UC infrastructure, the applications that run on them, as well as how outages impact their parent business services.

3.1.18. SLA Management

CDI SLA management function performs the following: (a) negotiates SLA targets with clients to drive the appropriate design of services to meet SLA targets, (b) ensures that all SLA targets flow through into operations and that SLA targets are met in operations, (c) monitors and reports on service levels.

3.1.19. IP Phone Management

CDI IP phone management function manages multiple types of requests such as:

(a) Add new IP phones
(b) Associate a phone to a user
(c) Set up the right phone template
(d) Configure settings for call forward, phone ringer, etc.,

Changes that are in scope includes direct support to end users to resolve issues related to IP phones, soft phones, and/or Jabber clients, etc., Typical issues that need support include, but not limited to:

(a) Choppy voice
(b) Echo issues
(c) Phones unregistered
(d) Unable to place outbound calls
(e) Phone not ringing
(f) Call forward not working
(g) Single number reach not working
(h) Call drops during transfer
(i) Unable to do ad-hoc conference calls
(j) Paging not working
(k) Incorrect caller-ID displayed, etc.,

3.1.20. Voice Mailbox Management

CDI voice mailbox management function manages multiple types of requests such as:

(a) Add voicemail boxes

(b) Delete voicemail boxes
(c) Unlock voicemail boxes
(d) Reset passwords
(e) Change greetings
(f) Setup holiday schedules, etc.,

Changes that are in scope includes direct support to end users to resolve any issues related to their voice mailboxes. Typical issues that need support include, but not limited to:

(a) Message waiting indicators not working
(b) Personal greeting not working
(c) Unable to disable vacation greeting
(d) Unable to login to mailbox, etc.,

3.1.21. Agent Management

CDI agent management function manages multiple types of requests such as:

(a) Add agents
(b) Setup agent skill groups and skill levels
(c) Reset passwords
(d) Change skill groups and skill levels, etc.,

Changes in scope includes direct support to end users to resolve any issues related to Cisco Agent Desktop. Typical issues that need support include, but not limited to:

(a) Agent unable to login
(b) Calls not getting routed to agents
(c) Call indication pop-up not working
(d) Unable to transfer calls to a different skill group
(e) Call getting dropped when hit the answer key, etc.,

3.1.22. RMA coordination for IP Phones

CDI RMA coordination for IP phones function extends alert and incident management responsibilities by providing the following when an IP phone becomes defective:

(a) Provide vendor coordination activities to quickly order and ship replacement IP phone to client site
(b) Remove the defective IP phone from the system
(c) Add the replacement IP phone to the system
(d) Ensure that the new IP phone is working fine

The client shall have an active warranty or maintenance service contract with the respective product manufacturer. Additionally, client shall have signed a Letter of Agency (LoA) during the services on-boarding phase, that authorizes CDI to act as a representative of the client, and empower it to contact and co-ordinate with the hardware product manufacturer when the hardware becomes defective.

3.1.23. Problem Management for IP Phones, End-Users, Voicemail Mailboxes, and Agents

This CDI function provides the processes, people, and tools required to investigate and determine the root cause of recurring incidents with IP phones, end users, voicemail boxes, and/or agents. It also develops a plan of action to address the root cause while following appropriate change management processes to implement action items. Goal is to avoid similar incidents from occurring again in future.

3.1.24. Voice Quality Monitoring and Management

1. **Proactive Management**

CDI uses synthetic voice packets to capture the delay, jitter, packet drops, etc., and arrive at the Mean Opinion Score (MOS) on an end-to-end and per hop basis. The synthetic voice calls are generated once every five (5) minutes and data from it is utilized to perform monthly trend analysis as part of the **Quality of Service (QoS) Optimization** deliverables. This provides a high level picture on the overall quality of the network to support voice traffic and also identifies weak links (if any) from a bandwidth or

priority queue allocation standpoint. The QoS optimization reports along with the historic CDR reports (Call Detail Reports) also correlate bandwidth and priority queue provisioned on WAN links in conjunction with peak voice traffic that traversed the link. These reports also provide recommendations on either increasing the priority queue settings or allocating more bandwidth to the links under question so as to proactively address any potential voice quality issues that are perceived by end users.

2. Reactive Management

CDI monitors voice quality metrics (delay, jitter, packet drops, and MOS) of active calls that are in progress for:

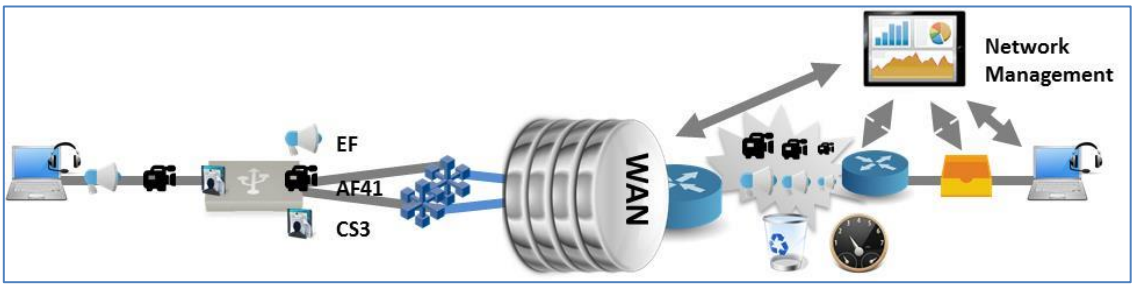
- Both inbound and outbound voice streams on a per hop basis (at each Layer 3 router)
- End-to- end -- i.e.
    - Between IP Phones
    - Between IP Phone to voice gateway (PRI Trunks), or
    - Between IP Phone to Session Border Controller (SIP)

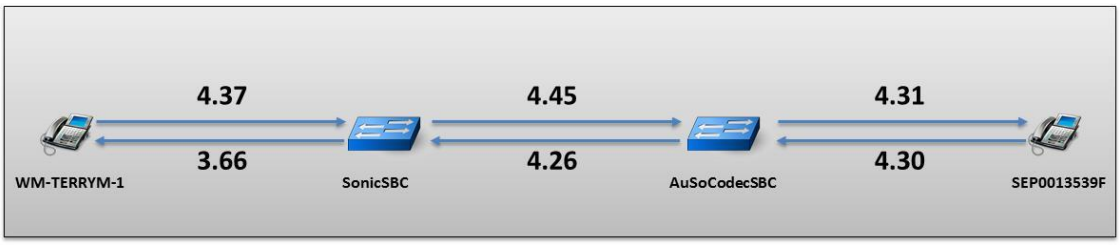
The monitors generate alerts if voice quality is below defined threshold, and if applicable alert management process can be initiated to meet response time SLAs. Calls can also be categorized by VIP profile of end user (e.g. CEO, VP, contact center agent, standard user, etc.) so that the appropriate priority of ticket can be determined. This is used by CDI to trigger the appropriate incident management process for further diagnosis and troubleshooting, and to resolve incident within defined resolution time SLAs.

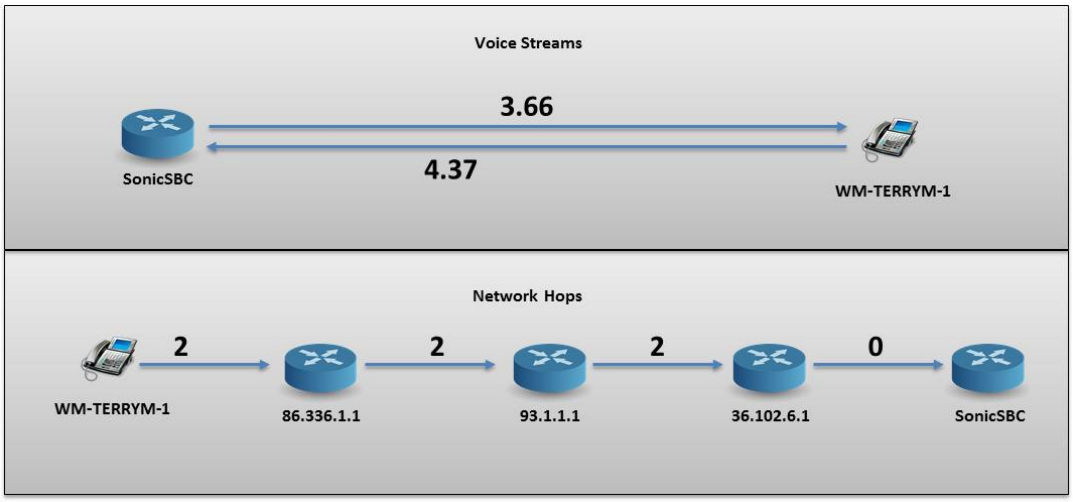
Many key capabilities enable the CDI problem management process and teams to quickly focus on problem domain and determine root cause of recurring voice quality incidents reported by end-users. They include:

- Ability to capture voice quality metrics on a per call basis
- Ability to categorize data by site, location, and time of the day
- Availability of data on a per hop basis

To resolve a voice quality issue, CDI follows the change management process to obtain approvals from client and implement the appropriate solution.







3.1.25. Location Bandwidth Monitoring and Management

1. **Proactive Management**

CDI captures the location bandwidth usage statistics from Cisco UC Manager to understand the inter-site call volume pattern during peak hours. This information is used for trend analysis that is conducted on a monthly basis as part of deliverables for **Quality of Service (QoS) Optimization**. The bandwidth and priority queue configured on WAN links is correlated, and recommendations are provided to either increase priority queue settings, or allocate more bandwidth to links and/or locations in question, in order to proactively address any potential call drops experienced by end-users due to lack of available bandwidth between sites.

2. **Reactive Management**

CDI monitors the location bandwidth usage and alerts generated when available bandwidth goes below defined threshold. The applicable **Alert Management process** is initiated by CDI to meet defined response time SLAs. The **Incident Management process** is next triggered for further diagnosis and troubleshooting, and to resolve incident within defined resolution time SLAs.

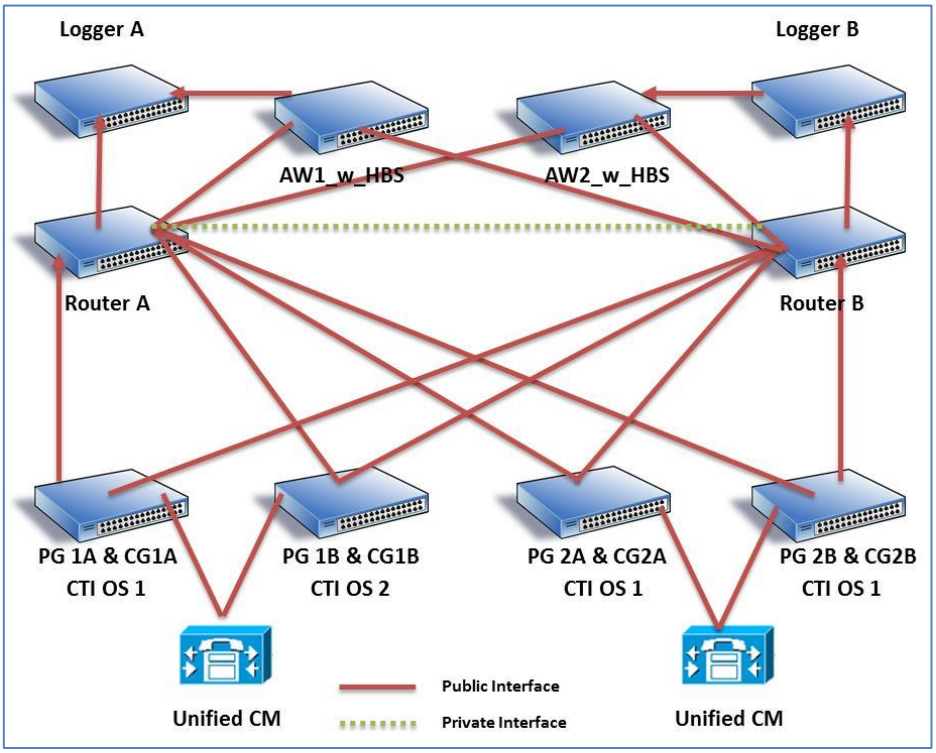
The ability to capture historic call drop statistics due to lack of bandwidth and the ability to categorize data by location, enables the CDI **Problem Management process** to quickly focus on problem domain and determine the root cause of recurring call drops reported by end-users. CDI next follows the **Change Management process** to obtain required approvals from client to implement an appropriate solution to resolve call drop issue.

3.1.26. Cisco Unified Contact Center Enterprise (UCCE) Monitoring and Management

The UCCE is a distributed solution with no single-server implementation, but rather employs multiple servers with multiple software components. Objectives such as performance, capacity, and network topology drive the design of deployment of UCCE, and deployment options are very flexible.

There are four major components of a UCCE deployment - the Router, the Logger, the Peripheral Gateway, and the Administration & Data Server. The basic function of each is as follows:

- **Router**: Makes the routing decisions and selects a peripheral or agent to receive an inbound contact (voice call, email, chat and so on)
- **Logger**: Stores and replicates all configuration, real-time, and historical data
- **Peripheral Gateway**: Acts as a gateway to a peripheral device such as an IP PBX or an Interactive Voice Response (IVR) unit, as well as a CTI gateway to link agent desktops
- **Administration & Data Server or Administration Workstation**: A server implementation that provides a copy of configuration data (from Logger), an interface for real-time data, and a platform for the historical data server (HDS). The Administration & Data Server also offers an interface for administrators to alter configuration and routing scripts (Script Editor and Internet Script Editor).



1. Fault Monitoring

The UCCE has an internal, proprietary, event management system (EMS) that provides guaranteed delivery of application faults and status events from distributed nodes to the Logger component. Alarms are delivered (via MDS) to the Logger where they are stored in the database. The SNMP agent infrastructure is installed on all of these component servers with a subagent that serves CISCO-CONTACT-CENTER-APPS-MIB instrumentation for that server. The MIB defines a number of tables of instrumentation – one set for discovery and basic health monitoring and an additional set of tables for component-specific instrumentation. Each common component of a UCCE deployment has a table of objects:

- Router (with a sub-table of NICs),
- Logger
- Administration Server and Real-time Data Server (AW)
- PG (with a sub-table of PIMs)
- CG
- CTI OS
- Outbound Option components
- Campaign Managers on the Logger
- Dialer on the PG

The component-specific table of instrumentation provides, where possible, links to dependent components that are distributed within the solution -- for example (a) the Router a peripheral gateway communicates to (b) the Logger that is the primary for a specific Administration Server and Real-time Data Server, etc. Real-time status of each component is monitored by polling the cccaComponentTable. The status of a UCCE component is derived by analyzing the collective status of each component element (i.e. the processes). The Component Element table lists all UCCE processes that should be executing, and exposes the operating system process identifier and the current status of the process.

CDI uses native SNMP monitoring capabilities to capture the operational status of all the components of a UCCE deployment, detect process faults, call failures, etc., and generates alerts so the applicable **Alert Management process** can be initiated to meet the defined response time SLAs. Additionally, the appropriate priority of the ticket is determined to trigger the **Incident Management process** for further diagnosis and troubleshooting, in order to resolve the incident within defined resolution time SLAs.

2. Performance Monitoring

CDI monitoring tools do the following to control performance related issues in order to prevent service outages: (a) acquire **CPU** and **memory** usage metrics for each process of the UCCE, (b) detect processes that are consuming excessive CPU cycles and/or

system memory, (c) poll the **Logger average database write time** to detect potential **contention for database access,** and (d) generate alerts so the applicable CDI **Alert Management process** can be initiated and **Automated Run books** can be executed.

For historical reporting and trend analysis, CDI monitoring tools also capture and record the **Inbound call rate, Agents logged in, Agents ready, Agents talking,** and other metrics. This data is utilized during multiple phases of services management:

- During **Services Discovery** phase, by **CDI UCCE Architects** for Busy Hour Call Analysis (BHCA).
- During **Service Design** phase, by **CDI UCCE Architects** for **Capacity Management** analysis to (a) determine if enough capacity is provisioned from a compute, storage, network, trunk, agent standpoint to handle the busy hour call traffic volumes, and (b) provide recommendations (if any).
- During **Service Transition** phase, by **CDI Service Delivery Managers** to identify time duration when call volume is at its lowest in order to recommend and/or agree upon **Pre-approved Maintenance windows** for UCCE infrastructure
- During **Service Operations** phase, the BHCA serves as a baseline for **CDI** to set utilization thresholds for CPU, memory, network, and trunk in order to minimize false positives
- During **Service Optimization** phase, by **CDI UCCE Architects** to analyze and provide deliverables for ongoing **Capacity Management** and **Trunk Optimization**

CDI monitoring tools also track performance on **CTI Gateways** by watching the number of sessions (connections) that were established between the CTI Gateway and CTI clients. Metrics tracked include **total number of sessions** (connections) between CTI Gateway and CTI clients that are **not normal,** as well as **open** and **active sessions**. This includes sessions that are **'opening'** (not yet established and initialized), sessions that are **'closing'** (connections being torn down), sessions that are in an **'unknown'** state, and sessions that have failed. These values fluctuate from time to time, but it stabilizes during normal operation. A steadily increasing value could potentially indicate a **software defect** or **Denial of Service (DoS)** attacks. Appropriate thresholds are set for metrics during the **Service Transition phase** to generate alerts, initiate applicable CDI **Alert Management process**, execute **Automated Runbooks** – in order to control performance related issues to prevent a service outage.

CDI monitoring tools also track performance metrics for **Outbound Option Campaign Manager**. These include:

- **Database utilization metrics** (percentage of allocated space in database that is in use)
- **Queue depth** before system restarts itself (by default the campaign manager deliberately restarts when this value exceeds 10,000 messages in queue as a self-defense mechanism)
- **Average queue time**

3. **Intelligent Business Operations:**

CDI monitoring tools also capture and record the count of contact center agents, count of active calls, calls that are in various states of treatment, calls in queue, etc., This level of business intelligence is made available to the **Call Center Supervisors** of client and may be used for designing and optimizing call coverage plans, determining the count of agents needed per shift, skillsets of agents needed, etc.,

CDI can also provide automated notifications to **Call Center Supervisors** of client when certain business conditions are triggered. For example, if count of calls in queue is higher than average, and based on count of agents currently logged in, if average call answer time crosses a certain threshold, then an automated email, phone call, or text SMS message can be sent to the Call Center Supervisors of client, so that they can initiate contingency plans to mitigate potential CSAT issues.

3.1.27. Cisco Unified Communications Manager (CUCM) Monitoring and Management

CDI has the capability to monitor and alert on 2,500+ conditions related to CUCM health. By default, the services cover monitoring and alerting of 600+ conditions that are critical in nature and that could potentially have a business impact.

1. **Availability Monitoring and Management**

    - Monitor status of all services for CallManager, CTI Manager, TFTP, etc., and alert on status changes

2. **Fault Monitoring and Management**
    - Monitor status of database connection between publisher and subscribers, as well as intra cluster communication signalling between subscribers, and alert on connectivity issues
    - Monitor status of database replication and alert on failures
    - Monitor validity and status of security certificates and alert on certificate mismatches
    - Monitor status of HTTP service and alert if any issues found with connecting to administration pages

- Monitor status of FTP connection during upload of CDR files and alert on failures

3. **Performance Monitoring and Management**
   - Monitor call processing load and alert when system reaches throttling point and could either (a) potentially start to drop calls -- Code YELLOW, or (b) reaches point of rejecting calls and commences restarting CallManager process -- Code RED
   - Monitor usage of CDR files and alert if disk usage exceeds defined thresholds
   - Monitor usage of SIP and PRI trunks and alert if insufficient availability of channels or trunks to place or receive calls

Table below shows data points captured by CDI for performance trend analysis

CUCM PERFORMANCE MANAGEMENT METRICS

CUCM PERFORMANCE METRICS	DATA POINTS COLLECTED FOR TREND ANALYSIS		
	DATA POINT 1	DATA POINT 2	DATA POINT 3
CPU Usage	Max.	Min.	Avg.
Physical Or Virtual Memory Usage	Total	Used	Free
Disk Space Usage	Total	Used	Free
Number Of Active Phones	Total	n/a	n/a
Gateway Registrations	Total	n/a	n/a
Calls In Progress	Min.	Max.	n/a
Calls Active	Min.	Max.	n/a
Calls Attempted	Min.	Max.	n/a
Calls Completed	Min.	Max.	n/a
PRI Channels Active	Min.	Max.	n/a
Active Conferences	Min.	Max.	n/a
Available Conference Resources	Min.	Max.	n/a
Active Transcoding Resources	Min.	Max.	n/a
Available Transcoding Resources	Min.	Max.	n/a
Available Location Bandwidth	Min.	Max.	n/a

3.1.28. Cisco Unified IM and Presence Monitoring and Management

1. **Availability Monitoring and Management**
   - Monitor status of all services such as Presence Engine, SIP Proxy, Config agent, Sync agent, etc., and alert on status changes

2. **Fault Monitoring and Management**
   - Monitor status of CTI gateway and alert on connectivity problems
   - Monitor status of SIP registrations and alert on errors
   - Monitor status of connection of Cisco Intercluster Sync Agent service to remote IM and Presence Service clusters, and alert on connectivity issues

3. **Performance Monitoring and Management**
   - Monitor SIP Route Interface resource usage and alert when configured limits are exceeded
   - Monitor CPU utilization and alert when new requests are blocked as a result of CPU utilization exceeding configured thresholds

3.1.29. Cisco IP Phone Monitoring and Management

1. **Availability Monitoring and Management**
   Monitor registration status of phones and alert if number of phones registered is below defined threshold

2. **Fault Monitoring and Management**
   [Optional] Monitor and alert on individual phones. However this is not generally recommended as it creates false-positives when end-users deliberately or voluntarily unplug phone cable. Regardless, it may be enabled for critical phones – e.g. CEO's phones, conference room phones, lobby phones, etc.

3. **Performance Monitoring and Management**
   Monitor and report on usage of licenses

3.2. Service Management - Optimization

1. Health check reporting
2. Capacity Mgmt.
3. Release Mgmt.
4. Product Lifecycle Mgmt.
5. SIP/PRI trunk usage review
6. QoS Audits

3.2.1. System Health Analysis

On a monthly basis CDI gathers data and conducts analysis on multiple UC components to identify potential issues:

- Ensure no mismatch between operating system and application software versions on all the servers
- Successful replication of databases between Publisher/Subscriber, Active/Standby, or Primary/Secondary instances
- Reachability of publisher and local database
- Acceptable limits of system clocks
- Acceptable limits of WAN delays
- Uptime of servers
- Utilization of CPU/Memory/Disk utilization within defined thresholds
- Status and health of critical services required for proper functioning of UC application
- Successful backups of applications at scheduled intervals

3.2.2. Capacity Management

CDI gathers data for current month for various key metrics and compares them against data from previous three months to determine trends in usage.

- CPU
- Memory
- Storage
- NIC bandwidth
- Licenses

CDI makes recommendations to ensure enough capacity is provisioned to meet client's collaboration requirements.

3.2.3. Software Patch Management

CDI determines the latest software update or minor release made available by product manufacturer for each UC application. It then compares them against current running version and makes appropriate recommendations and patch rollout plan (if required).

3.2.4. Product Lifecycle Management

CDI reviews and analyzes lifecycle state of each software and hardware component of UC Infrastructure from a product standpoint as published by product manufacturer.

- End of Life (EOL)
- Deferred Release
- Security Advisory
- Field Notice
- Major Release Available

CDI makes appropriate recommendations for technology refresh, if needed.

3.2.5. Telco Trunk Optimization (SIP, PRI, Analog)

CDI reviews inbound and outbound traffic trends for each telco trunk and makes appropriate recommendations to ensure that enough trunks are provisioned cost-effectively to meet client's collaboration requirements. Some common scenarios that are covered include:

- For remote sites with high volumes of long distance or international dialing, make recommendations to change dial plan, so that long distance or international calls utilize centralized SIP trunks at data center (vs. local PRI circuits) to achieve increased cost efficiency.
- For remote sites with local PRI circuits, but with very low outbound call volumes, make recommendations to migrate from PRI to an analog trunk or CAMA trunk (Centralized Automatic Message Accounting), in order to meet outbound calls or emergency dial requirements as well as to achieve increased cost efficiencies.

3.2.6. Quality of Service (QoS) Optimization

Before implementing recommendations from telco trunk optimization phase that may involve changing dial plan from a distributed to centralized model, CDI analyses and determines if WAN is provisioned to accommodate additional voice traffic. It then performs the QoS optimization phase that includes information gathering, analysis, and recommendations.

1. **Information Gathering**
   - Trends on inbound, outbound, and inter-site calls
   - Trends on MPLS and WAN interface utilization
   - Configurations of QoS for MPLS and WAN links for each site

2. **Analysis**
   - Is Low Latency Queuing (LLQ) configured on MPLS and WAN links?
   - How much bandwidth is set aside in priority queue for voice traffic on MPLS and WAN links?
   - What is maximum number of calls traversing MPLS and WAN?
   - Is priority queue sufficient to accommodate additional calls traversing MPLS and WAN?
   - How much additional bandwidth should be provisioned for priority queue?
   - How will change in bandwidth allocation between priority queue and other queues impact existing data traffic and applications?
   - Is there a need to increase total bandwidth of MPLS and WAN links?
   - Does site have redundant MPLS and WAN (primary and secondary) links?
   - Should Layer 3 routing be changed to load balance the voice and data traffic among primary and secondary links with each acting as a backup?

3. **Recommendations**

Based on the analysis, CDI makes recommendations for QoS optimization.

4. Supported Solutions, Products, and Devices

4.1. Cisco Unified Communications Solution

#	Product	Function
1.	**Cisco Unified Communications Manager (CUCM)**	CUCM is the software-based call-processing component of the Cisco enterprise Unified Communication solution. CUCM software extends enterprise telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, voice over IP (VoIP) gateways, and multimedia applications. A CUCM cluster can support a maximum of 30,000 phones and 250,000 Busy Hour Call Completions (BHCC).
2.	**Cisco IM and Presence**	Cisco IM and Presence Service provides native standards-based, dual-protocol, enterprise instant messaging (IM) and network-based presence as part of Cisco Unified Communications. IM and Presence Service delivers enhanced enterprise IM features, including group chat, persistent chat, and IM logging, along with a suite of business-to-business and business-to-consumer IM and presence open federations.
3.	**Cisco Unity Connection**	Cisco Unity Connection is a robust unified messaging and voicemail solution allowing users access and manage messages from an email inbox, web browser, Cisco Jabber, Cisco Unified IP Phone, smartphone, or tablet.
4.	**Cisco Emergency Responder (CER)**	Cisco Emergency Responder helps assure that Cisco Unified Communications Manager sends emergency calls to the appropriate Public Safety Answering Point (PSAP) for the caller's location. It also helps ensure that the PSAP can identify the caller's location and, if necessary, return the call.
5.	**Cisco Business Edition (BE)**	Cisco BE is a stackable, packaged collaboration solution optimized for organizations with 1000 or more users and thousands of devices. The solution offers premium voice, video, mobility, messaging, conferencing, instant messaging and presence, and contact center features on a single, integrated platform. It provides core communication capabilities that fast-growing companies need for improved collaboration for employees, customers, and business partners.
6.	**Cisco Unified Communications Manager Express (CME)**	Based on Cisco IOS, CME provides call processing for distributed enterprise branch-office environments and retail deployments for up to 450 IP Phones.
7.	**Cisco Unity Express**	Cisco Unity Express offers industry-leading integrated messaging, voicemail, fax, Automated Attendant, interactive voice response (IVR), time-card management, and a rich set of other messaging features on the Cisco Integrated Services Router (ISR) platform. It provides these integrated services specifically designed for the small and medium-sized office environment or enterprise branch office for up to 500 users.
8.	**Cisco Expressway**	Cisco Expressway facilitates collaboration with users outside your firewall to provide highly secure access to video, voice, content, IM, and presence. Collaborate with people who are on third-party systems and endpoints or in other companies.
9.	**Cisco Unified Border Element (CUBE)**	CUBE is a session border controller, allows control of SIP services with registered external entities, most commonly service providers that offer VoIP services based on SIP or H323 protocols.
10.	**Cisco TDM Gateways**	Cisco TDM Gateways offer a variety of different voice network modules to deliver IP connectivity to the PSTN, a PBX, or an analog device.
11.	**Cisco VG Series Gateways**	Cisco VG Series Gateways provide added flexibility during migration to unified communications by supporting traditional analog devices on IP networks. These devices include analog phones, fax machines, modems, voicemail systems, and speakerphones.
12.	**Cisco Jabber**	Cisco Jabber lets you access presence, instant messaging (IM), voice, video, voice messaging, desktop sharing, and conferencing

13.	**Cisco UC Integration for Microsoft Lync**	Desktop integration that provides access to Cisco Unified Communications from Microsoft Lync. The solution extends the presence and instant messaging (IM) capabilities of Microsoft Lync by providing access to a broad set of Cisco Unified Communications capabilities, including soft-phone standards-based video, unified messaging, audio and video conferencing, desk-phone control, and phone presence.
14.	**Cisco Unified Attendant Console**	Cisco Unified Attendant Console gives corporate operators and receptionists the tools they need to handle incoming calls efficiently and professionally. This desktop application communicates directly with Cisco Unified Communications Manager to control the operator's phone.

4.2. Cisco Contact Center Solution

#	Product	Function
1.	**Cisco Unified Contact Center Enterprise (UCCE)**	UCCE delivers intelligent contact routing, call treatment, network-to-desktop computer telephony integration (CTI), and multichannel contact management over an IP infrastructure.
2.	**Cisco Unified Contact Center Express (UCCX)**	UCCX delivers a highly secure, available, virtual, and sophisticated customer interaction management solution for up to 400 agents. This integrated, comprehensive, contact center solution is intended for both formal and informal contact centers in midmarket, enterprise branch, and corporate departments.
3.	**Cisco Agent Desktop (CAD)**	CAD is a tightly integrated computer telephony interface (CTI)-enabled productivity and management software suite that deliver a rich set of services and call-event data to contact center agents and supervisors operating in a Microsoft Windows, web, or IP phone service environment.
4.	**Cisco Finesse**	Cisco Finesse is a next-generation browser based agent and supervisor desktop implemented through a web 2.0 interface; no client-side installations required.
5.	**Cisco MediaSense**	Cisco MediaSense is an open-standards, network-based platform that supports recording, playback, live streaming, and storage of media, including audio and video, with rich recording metadata
6.	**Cisco Outbound Option**	Cisco Outbound Option enables the multi-functional contact center to include outbound campaign solutions to maximize the use of skilled agents, utilize individual dialing modes, and deliver rich call contact information to a best-in-class CTI desktop.
7.	**Cisco Unified E-Mail Interaction Manager**	Cisco Unified E-Mail Interaction Manager enables the contact center, helpdesk, and customer service team to intelligently and efficiently route and process inbound e-mails from customers, employees, and other users
8.	**Cisco Unified Web Interaction Manager**	Cisco Unified Web Interaction Manager helps ensure that your online customers are connected easily and transparently to the right agent every time, even if the customer is connecting from behind a firewall.
9.	**Cisco Unified Intelligence Center**	Cisco Unified Intelligence Center is a web-based reporting application that provides real-time and historical reporting. It allows contact center supervisors and business users to report on the details of every contact across all channels in the contact center from a single interface.
10.	**Cisco Unified Workforce Optimization for UCCX**	Cisco Unified Workforce Optimization empowers supervisors with information in real time and gives them the tools they need to evaluate and continually improve team performance and customer satisfaction.
11.	**Cisco Unified Customer Voice Portal (CVP)**	CVP provides IP-based self-service and call routing. It combines open-standards support for speech with intelligent application development and industry-best call control to deliver personalized self-service to callers - either as a standalone interactive-voice-response (IVR) system or transparently integrated with a contact center.

12.	**Cisco Unified IP Interactive Voice Response (IVR)**	Cisco Unified IP Interactive Voice Response (IVR) provides enhanced call control, platform management, speech integration and reporting services.
13.	**Cisco Unified Call Studio**	Cisco Unified Call Studio is an integrated development environment (IDE) for voice self-service applications which allows creation of sophisticated speech-enabled telephone self-service using VoiceXML (Voice Extensible Markup Language).

4.3. Versions and Models Supported

CDI support covers all versions and models of above products made available by Cisco that has not reached End-of-Life (EOL)

5.Incident Classification

CDI will perform incident management in an SLA based service delivery model. CDI requires a lockdown of the UC environment, with full control over environment provided to CDI, in order for CDI to assume responsibility for meeting important onsite operational requirements such as availability, capacity, and outages. The client needs to inform CDI of any device additions or deletion, or changes to network devices in the associated UC environment.

5.1. SLAs for Incidents

The following table describes the various priority levels and SLAs associated with incidents. The sources of alerts are either from the monitoring system or from user requests entered via the ticketing system, phone or e-mails.

PRIORITY	RESPONSE TIME SLA	RESOLUTION TIME SLA	MEASURED
P0: Critical (Severity-1)	15 Min	85% of the cases resolved in 4 hours	Monthly
P1: High (Severity-2)	2 Hours	85% of the cases resolved in 24 hours	Monthly
P2: Medium (Severity-3)	4 Hours	85% of the cases resolved in 36 hours	Monthly
P3: Low (Severity-4)	8 Hours	85% of the cases resolved in 72 hours	Monthly

- Resolution SLA timer is paused when ticket status is changed to “Handed-over to Client” “On-Hold,” “Under observation,” “Work around” or “Resolved”

5.2. SLAs for MACDs

The following table describes the SLAs associated with various types of MACD service requests. The sources of MACD requests are typically from end-user requests entered via ticketing system, phone or e-mails.

PRIORITY	RESPONSE TIME SLA	RESOLUTION TIME SLA	MEASURED
Emergency MACD	15 Min	85% of MACD requests completed within 1 hour	Monthly
Standard MACD	2 Hours	85% of MACD requests completed within 24 hours	Monthly

6. Reports

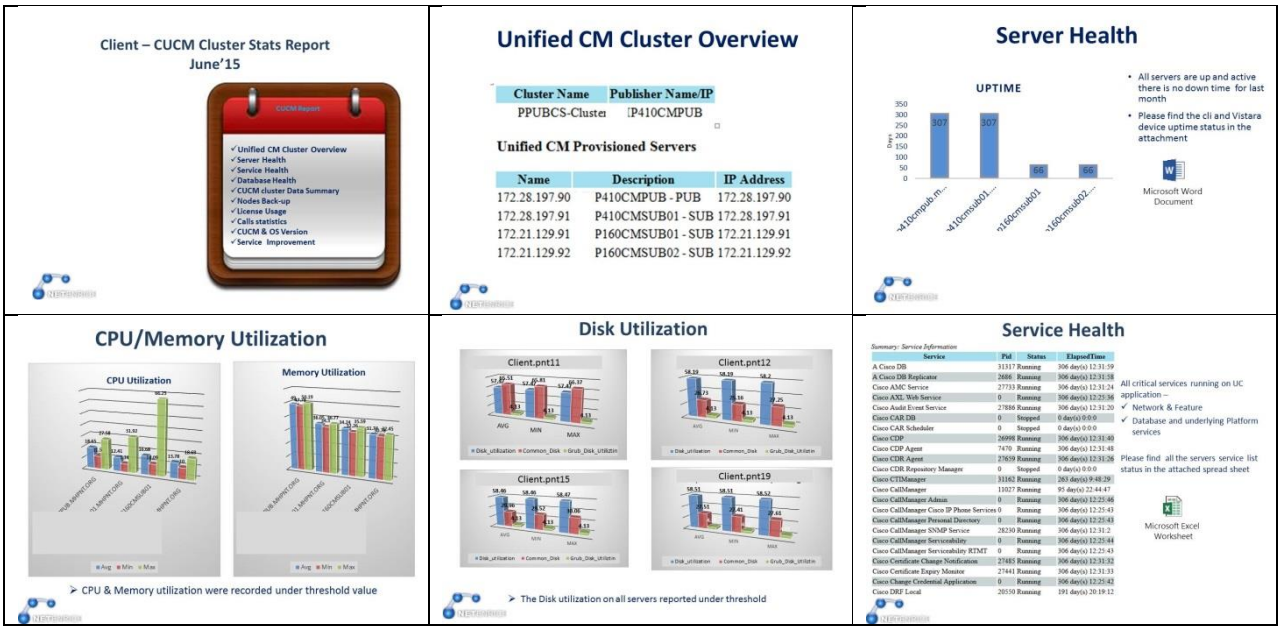
6.1. UC Reports

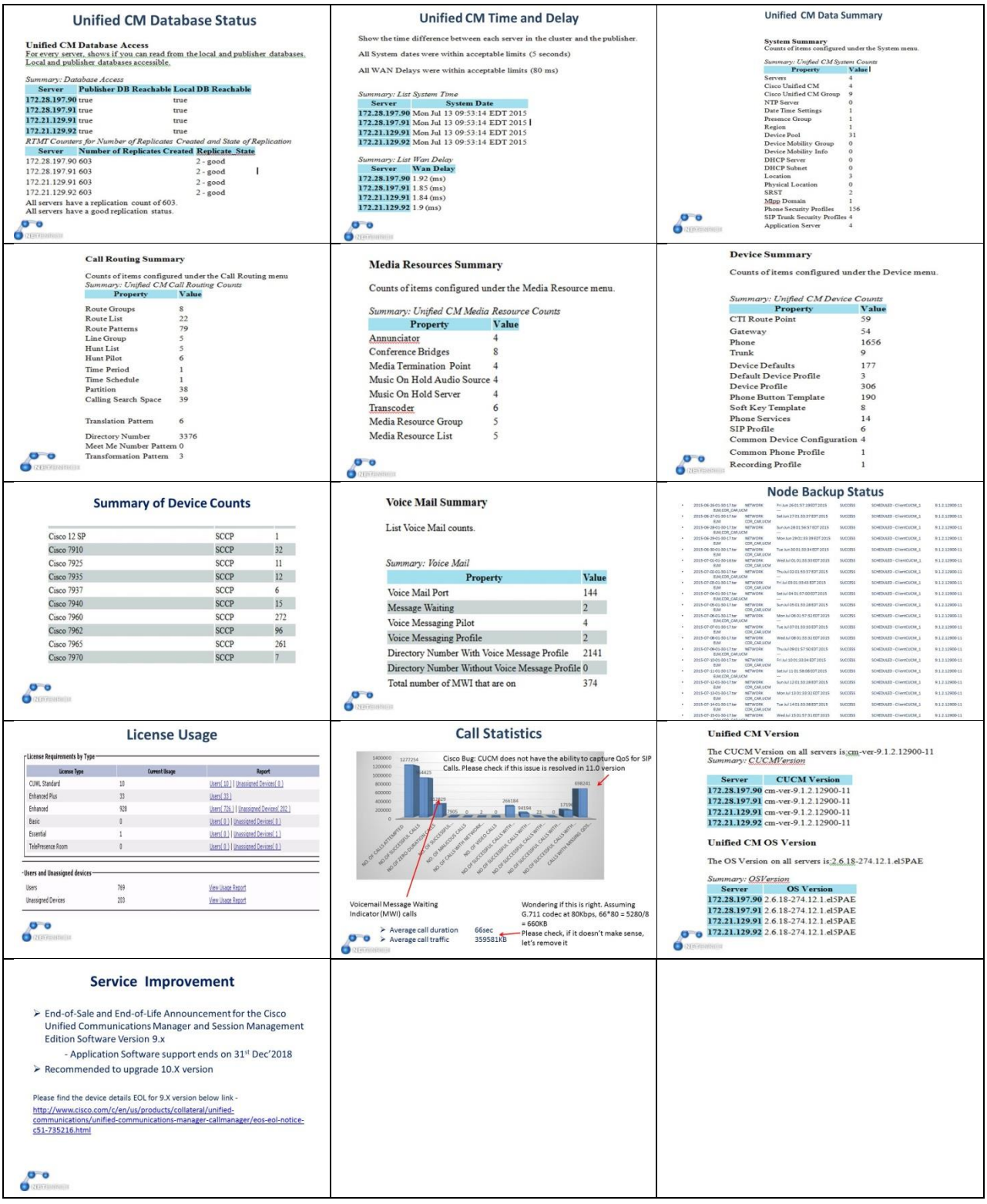
Healthcheck reports to be provided on a monthly basis.

1. Server Health
    a. Uptime of System/Device -- Since how long has the device been up after last reboot?
    b. Status/Utilization Snapshot on CPU, memory, fan, power, RAID, Disk, Network(NIC) -- utilization based on threshold
    c. Is the hardware already EOL or reaching EOL in the near future?
2. Service Health
    a. Critical Service State – for all critical services running on UC application (Network/Feature)
3. Database Health
    a. Database replication with replicate status?
4. Application Health
    a. Validate no version mismatch between Publishers/Subscribers?
    b. Is the application version old and needs to be patched?
    c. Is the hardware already EOL or reaching EOL in the near future?
5. License Health
    a. When does the license expire?
    b. Current license usage?
6. Backup Health
    a. Check backup schedule
    b. Validate backup process status
    c. When was the last successful backup?
    d. Storage space availability at the Backup Data store?

6.2. Example Reports

6.2.1. Example Report 1 – CUCM Report For Client





Unified CM Database Status

Unified CM Database Access
For every server, shows if you can read from the local and publisher databases. Local and publisher databases accessible.

Summary: Database Access

Server	Publisher DB Reachable	Local DB Reachable
172.28.197.90	true	true
172.28.197.91	true	true
172.21.129.91	true	true
172.21.129.92	true	true

RTMT Counters for Number of Replicates Created and State of Replication

Server	Number of Replicates Created	Replicate_State
172.28.197.90	603	2 - good
172.28.197.91	603	2 - good
172.21.129.91	603	2 - good
172.21.129.92	603	2 - good

All servers have a replication count of 603.
All servers have a good replication status.

Unified CM Time and Delay

Show the time difference between each server in the cluster and the publisher.

All System dates were within acceptable limits (5 seconds)

All WAN Delays were within acceptable limits (80 ms)

Summary: List System Time

Server	System Date
172.28.197.90	Mon Jul 13 09:53:14 EDT 2015
172.28.197.91	Mon Jul 13 09:53:14 EDT 2015
172.21.129.91	Mon Jul 13 09:53:14 EDT 2015
172.21.129.92	Mon Jul 13 09:53:14 EDT 2015

Summary: List Wan Delay

Server	Wan Delay
172.28.197.90	1.92 (ms)
172.28.197.91	1.85 (ms)
172.21.129.91	1.84 (ms)
172.21.129.92	1.9 (ms)

Unified CM Data Summary

System Summary
Counts of items configured under the System menu.

Summary: Unified CM System Counts

Property	Value
Servers	4
Cisco Unified CM	4
Cisco Unified CM Group	9
NTP Server	0
Date Time Settings	1
Presence Group	1
Region	1
Device Pool	31
Device Mobility Group	0
Device Mobility Info	0
DHCP Server	0
DHCP Subnet	0
Location	3
Physical Location	0
SRST	2
Mlpp Domain	1
Phone Security Profiles	156
SIP Trunk Security Profiles	4
Application Server	4

Call Routing Summary

Counts of items configured under the Call Routing menu
Summary: Unified CM Call Routing Counts

Property	Value
Route Groups	8
Route List	22
Route Patterns	79
Line Group	5
Hunt List	5
Hunt Pilot	6
Time Period	1
Time Schedule	1
Partition	38
Calling Search Space	39
Translation Pattern	6
Directory Number	3376
Meet Me Number Pattern	0
Transformation Pattern	3

Media Resources Summary

Counts of items configured under the Media Resource menu.

Summary: Unified CM Media Resource Counts

Property	Value
Annunciator	4
Conference Bridges	8
Media Termination Point	4
Music On Hold Audio Source	4
Music On Hold Server	4
Transcoder	6
Media Resource Group	5
Media Resource List	5

Device Summary

Counts of items configured under the Device menu.

Summary: Unified CM Device Counts

Property	Value
CTI Route Point	59
Gateway	54
Phone	1656
Trunk	9
Device Defaults	177
Default Device Profile	3
Device Profile	306
Phone Button Template	190
Soft Key Template	8
Phone Services	14
SIP Profile	6
Common Device Configuration	4
Common Phone Profile	1
Recording Profile	1

Summary of Device Counts

Cisco 12 SP	SCCP	1
Cisco 7910	SCCP	32
Cisco 7925	SCCP	11
Cisco 7935	SCCP	12
Cisco 7937	SCCP	6
Cisco 7940	SCCP	15
Cisco 7960	SCCP	272
Cisco 7962	SCCP	96
Cisco 7965	SCCP	261
Cisco 7970	SCCP	7

Voice Mail Summary

List Voice Mail counts.

Summary: Voice Mail

Property	Value
Voice Mail Port	144
Message Waiting	2
Voice Messaging Pilot	4
Voice Messaging Profile	2
Directory Number With Voice Message Profile	2141
Directory Number Without Voice Message Profile	0
Total number of MWI that are on	374

Node Backup Status

License Usage

License Requirements by Type

License Type	Current Usage	Report
CUWL Standard	10	Users(10) | Unassigned Devices(0)
Enhanced Plus	33	Users(33)
Enhanced	928	Users(726) | Unassigned Devices(202)
Basic	0	Users(0) | Unassigned Devices(0)
Essential	1	Users(0) | Unassigned Devices(1)
TelePresence Room	0	Users(0) | Unassigned Devices(0)

Users and Unassigned devices

Users	769	View Usage Report
Unassigned Devices	203	View Usage Report

Call Statistics

Unified CM Version

The CUCM Version on all servers is cm-ver-9.1.2.12900-11
Summary: CUCMVersion

Server	CUCM Version
172.28.197.90	cm-ver-9.1.2.12900-11
172.28.197.91	cm-ver-9.1.2.12900-11
172.21.129.91	cm-ver-9.1.2.12900-11
172.21.129.92	cm-ver-9.1.2.12900-11

Unified CM OS Version

The OS Version on all servers is 2.6.18-274.12.1.el5PAE

Summary: OSVersion

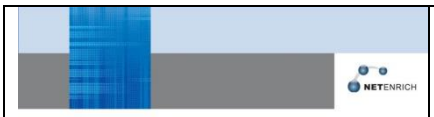
Server	OS Version
172.28.197.90	2.6.18-274.12.1.el5PAE
172.28.197.91	2.6.18-274.12.1.el5PAE
172.21.129.91	2.6.18-274.12.1.el5PAE
172.21.129.92	2.6.18-274.12.1.el5PAE

Service Improvement

- End-of-Sale and End-of-Life Announcement for the Cisco Unified Communications Manager and Session Management Edition Software Version 9.x
  - Application Software support ends on 31st Dec'2018
- Recommended to upgrade 10.X version

Please find the device details EOL for 9.X version below link -
http://www.cisco.com/c/en/us/products/collateral/unified-communications/unified-communications-manager-callmanager/eos-eol-notice-c51-735216.html

6.2.2. Example Report 2 – Unity Connection Healthcheck Report for Client

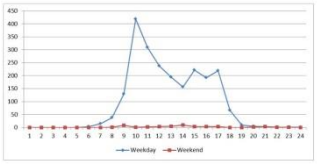


Client - Unity Conn Healthcheck Report
July 6, 2015

VM Database

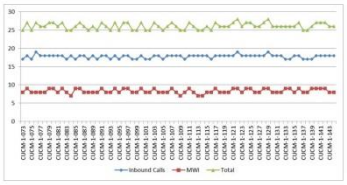
Database name	UnityMbxDb1
Server	Client410ucpub.client.org
Number of mailboxes	734
Current size	2.6 GB
Status	OK

Voice Message Traffic



- Peak hour during weekdays 9AM-10AM – 419 messages
- Average 2200 messages during week day and 50 messages during weekends

VM Port traffic analysis



- Calls equally distributed among the 72 ports
- Each port handling on an average 18 inbound calls and 9 MWI per day

Findings

#	Findings	Next Steps
1.	160 Non Delivery Receipts during the month of June	John is investigating the cause
2.	25 Unused voicemail accounts	1. Linda to review with Client to confirm the voicemail accounts that can be safely deleted 2. Linda to place MAC ticket to delete voicemail accounts
3.	Eva Jones (8793) is placing outbound calls from Unity	Linda to check with Client if the user is authorized to place outbound calls

7. Out of Scope and Service Limitations

7.1. Out of Scope for Alert Monitoring

System parameters that can be monitored and alerted are limited to what is exposed by the product manufacturer via SNMP, Event Viewer, WMI, APIs, etc., Any custom errors, logs, and/or parameters that needs to be monitored or alerted are out of scope.

Any customizations to monitoring templates are subject to review and acceptance by CDI.

7.2. Out of Scope for Problem Management

Investigation and analysis of root cause of problems are only performed on the following:

(a) Alerts and incidents that re-occur more than thrice within a five day period
(b) Major incidents

For these alert and incident types, root cause analysis reports are created within five days of the alert or incident.

7.3. Out of Scope for Change Management

Client generated changes that are oriented towards adding additional features, functions, and/or integration capabilities are considered out of scope.

7.4. Out of Scope for End User and IP Phone Management

Support ends at the core UC application for soft phone, Jabber clients, and/or other UC related applications installed on end-user or agent desktop or laptops. This means that that if any underlying component of the core UC application such as operating system, anti-virus, malware protection software, hardware, etc., cause the UC application to malfunction, then the support needed to resolve the issue related to the underlying components is out-of-scope for UC managed services. (However, client may purchase separate management services from CDI for those underlying components).

7.5. Out of Scope for Agent Management

The support for Cisco Agent Desktop application is limited to the application only. This means that that if any underlying component of the core UC application such as operating system, anti-virus, malware protection software, hardware, etc., cause the UC application to malfunction, then the support needed to resolve the issue related to the underlying components is out-of-scope for UC managed services. (However, the client may purchase separate management services from CDI for those underlying components, if it is offered by CDI).

7.6. Out of Scope for MACD

Any change requests that are not defined in MACD Table (Section 3.1.14) are out of scope.

7.7. Out-of-Scope Service Requests

Some service requests are out-of-scope including the requests below. However, they can be addressed on a T&M basis. Contact CDI for more details.

- New device deployment, provisioning , configurations and migrations
- New site architect, design, redesign, migrations of VoIP network infrastructure, remote office or branch office
- DNS changes and IP allocations
- UC/Network topology changes