



Unified Communications - Best Practices

Cisco on Cisco
Technology Tutorial



Kevin O’Healy

Member of Technical Staff, Cisco IT

Ian Pudney

IT Manager, Cisco IT, (Host)

IPT Operational Excellence Best Practices



Solution Redundancy

Cisco Unified Communications Manager (UCM) Cluster Redundancy

- Place Cisco UCM servers in multiple locations
 - World regions
 - Multiple data centers with a large campus
 - Primary and secondary servers in separate locations
- Distribute Cisco UCM & TFTP servers
- Deploy redundant media resources (e.g., conference bridges, music-on-hold servers, transcoders)
- Cluster Cisco UCM servers over the LAN/WAN

Solution Redundancy

Diverse routing for voice gateways (carrier and device)

- Multiple vendors (use LEC and IXC circuits interchangeably)
- Multiple, physically separate gateways
- Provide multiple paths out of each Cisco CallManager cluster
- Deploy Cisco Survivable Remote Site Telephony (SRST) and PSTN gateways for backup call services in remote offices
- Use the PSTN as a back-up route for on-net dialing between corporate offices

Solution Redundancy

- Core, distribution, access switches with high availability
 - Redundant power supplies, different power circuits
 - Redundant line cards and supervisor modules
- Redundant core and distribution routers throughout the network
 - Test and minimize route convergence
- Redundant WAN routes
 - Use Hot Standby Routing Protocol (HSRP) to create primary & secondary data and voice paths
- UPS 2-hour run time in all wiring closets
 - UPS audit against a UPS policy
 - Networks grow - verify UPS is keeping up
- Disaster recovery plan
 - Identify the telephony disaster recovery policy
 - Test disaster recovery procedures

Change Management

- Integrate voice and data teams into a single review board
- Develop a policy that defines which actions must go through the change management process
- Create email aliases to review all change requests that impact voice services
 - One alias includes all IT personnel who interact with the voice and data network
 - Second alias includes voice support personnel for all Cisco CallManager configuration changes that do not require an approved request
- Example policy: No changes that will impact voice services can be made before 9:00pm local time
- Use standard configurations globally (e.g., LAN, WAN, Cisco CallManager, etc.)

Voice Quality

- VoIP audit to identify network readiness
 - QoS, Call Admission Control, WAN, capacity planning
 - Redundant line cards and supervisor modules in switches, diverse power circuits, UPS
- Auxiliary VLANs for voice traffic
 - Separate voice and data
 - Conserve address space
- Use a codec that meets voice quality and bandwidth requirements
 - Test in the lab and with a pilot group or steering committee
 - Consider multiple codec types to meet different business needs (e.g., contact center)

Voice Quality

- Trust IP phone traffic, rewrite all other traffic to 0
 - Consistently apply QoS end-to-end
 - Classify and mark voice, signaling, and video traffic
 - Classify and mark voice applications traffic (e.g., Cisco IP/IVR, conferencing, etc.)
- Priority queuing at the WAN edge
 - Low-Latency Queuing (LLQ) to dedicate bandwidth to voice traffic and signaling
 - Develop consistent QoS policies for links with varying bandwidth
- Ensure consistent Call Admission Control bandwidth configuration across the entire IP telephony environment
 - Match Cisco UCM *locations* bandwidth to WAN queueing (LLQ) configuration
 - Account for variations in codec bandwidth (i.e., G711 vs. G729)
 - Use only one codec type on WAN links

Security

- Install anti-virus software on all Cisco UCM servers
 - Automatically updated with latest DAT file
 - Regular, automated reporting on compliance
- Install Cisco Security Agent on Cisco UCM servers for intrusion protection
- Streamline deployment of patching the systems
 - Standard versions of hardware and applications
 - Implement a maintenance cycle for patching and upgrades

Security

- Tight control on external network access
 - Standard Internet access controls, i.e., firewall, DMZ, intrusion detection
 - Strong authentication for remote and VPN users
 - Network Admission Control and IP filters
 - Separate voice and data VLANs
 - Reset passwords frequently
- Tight internal controls on network devices
 - Well-managed PC environment
 - Tight control of lab environment; physical security
 - Maintain a log of device access and changes
 - Control access to management ports and functions

Monitoring

- Measure service availability
 - Monitor device uptime and service availability
- SNMP monitoring for device components
 - Memory and CPU utilization
 - Interface utilization and errors
 - Power supplies and disk drives
- Voice gateway and trunk availability
 - Gateway utilization
 - Voice mail port utilization
- Establish thresholds and automatic notification
 - Provide email and pager notification when thresholds are exceeded
 - Tune current monitoring environment
 - Standardized monitoring policies for all hosts

Support

- Operating system patches and upgrades
 - Establish an upgrade policy
 - Use remote administration tools: virtual network computing (VNC) or RILO for remote server management
 - Onsite resources can support remote installations
- Application patches and upgrades
 - Establish an upgrade policy
 - Pull redundant hard drive on major upgrades
 - Use change management process for all updates
- Minimize impact during the upgrade
 - Use the bulk administration tool & save data about all registered devices
 - Stagger Cisco UCM system reboots
 - Monitor TFTP performance
 - Disable alerting during the upgrade
 - Perform post-upgrade testing on the dial plan and voice mail

Support

- Assign the correct user privileges
 - Grant access rights based on job requirements
 - Use multi-level access for Cisco UCM
 - User vs. privilege access on Cisco IOS software-based devices
- Documentation
 - Develop implementation and support documentation and store in a central location
 - Develop FAQs for frequent problems and solutions and provide to the Tier 1 support team
- Manage support cases
 - Enforce escalations through proper channels to identify trends

Unified Communications Deployment at Cisco: Best Practices in Action



Best Practices Deployment at Cisco

The global Cisco Unified Communications Deployment has over 100,000 IP Telephony Endpoints. 40,000 are on a single cluster in San Jose, California.

How did Cisco deploy Unified Communications?

- Device redundancy:
 - 19 servers in the Cisco UCM cluster
 - 8 redundant Cisco Unity Pods (voice mail)
 - Servers deployed in two campus data centers
 - High availability servers (dual CPU, redundant power supplies and disk drives)
- Gateway & call routing redundancy:
 - 100 voice gateways distributed across 8 buildings
 - Separate local and long-distance carriers with connections to separate CO's
 - Multiple calls paths including Cisco Gatekeeper and the PSTN

Best Practices Deployment at Cisco: Cisco UCM Configuration

- Install operating system and Cisco UCM
 - Name the server according to the global naming standard
 - Assign standard passwords
 - Re-map drive letters to Unified Communications operations standards
 - Enable only necessary services on each server and cluster
- Install anti-virus software
 - Configure to automatically update virus definition files
- Verify network configuration
 - Hard-set speed/duplex on Cisco UCM servers & uplink switch
- Verify time configuration
 - Implement Network Time Protocol (NTP) or Windows Time Service

Best Practices Deployment at Cisco: Remote Offices

Over 300 Cisco sites worldwide are served by just 20 CUCM clusters located in 12 regional hubs

- Consider Clustering over the WAN
 - Extends geographic reach
 - Provides consistent services throughout a region (Ext. Mobility, etc.)
- Implement Cisco SRST for remote sites
 - Verify SRST fallback
 - Test the dial plan while in fallback mode
 - Verify emergency dialing
- Deploy redundant voice gateways
 - Distribute across multiple devices
 - Provide “shared” resources for redundancy
- Considerations when developing the dial plan
 - Identify site-specific dialing requirements (e.g., 7-digit vs. 10-digit local dialing)
 - Implement automated alternate routing (AAR) to protect against out-of-bandwidth conditions

Best Practices Deployment at Cisco: Cisco UCM Configuration

- **Configure Cisco UCM Trace Files**
 - Configure traces to be written to dedicated drive array
 - Store traces for at least 7 days (14 is better)
 - Update trace file configuration to include Cisco UCM server name in each trace file
 - Set the appropriate trace level

- **Configure Monitoring Alerts (Real Time Monitor)**
 - Monitor drive space, registered devices, and Cisco UCM heartbeat
 - Minor alerts: (email every 15 minutes)
 - Major alerts: (page every 5 minutes)

Best Practices Deployment at Cisco: Service Monitoring

- Monitoring the User Experience of Service Availability
 - Automated Synthetic Testing to emulate end-clients
 - Required for all Critical Communications Services
- Reporting on exceptions
 - MOS Thresholds to highlight trouble spots
- Parallel to System Level Monitoring
- IT Solution Components:
 - Cisco Unified Operations Manager
 - Cisco Unified Service Manager
 - Cisco Unified Service Statistics Manager

Prioritized Recommendations



Prioritized Recommendations

- **Change Management:**
Integrate voice and data teams for a single change management body.
- **QoS:**
Create, document, test, then implement QoS policies.
- **Management Metrics:**
Identify and prioritize metrics for success. Develop automated systems to collect and report data for the metrics
- **Standardized Configurations:**
Develop and deploy standard configurations.
- **Documentation:**
Create an IT Operations intranet Web site to store and serve documents. Identify an owner for the site and each document.

Q and A



Further Resources



Cisco on Cisco Website

<http://www.cisco.com/go/ciscoit>



Call to get Product, Solution and Financing Information

1-800-745-8308 ext. 4699



Order Resources

<http://cisco.com/en/US/ordering/index.shtml>

