



Cisco on Cisco Best Practice

Contact Center Migration to UCS

Don Bayliss

March 2012

Contents

Introduction	3
Background	4
Problem	5
Solution	5
Design	6
UCS Design Considerations	7
Network Design	8
Network Topology in the Data Center	8
Migration	10
Phase 1: Migrating the Domain Controllers	10
Phase 2: Migrating the Historical Data Servers	10
Phase 3: Migrating the Central Controller Node	11
Conclusion	12
For More Information	13
Note	13

Introduction

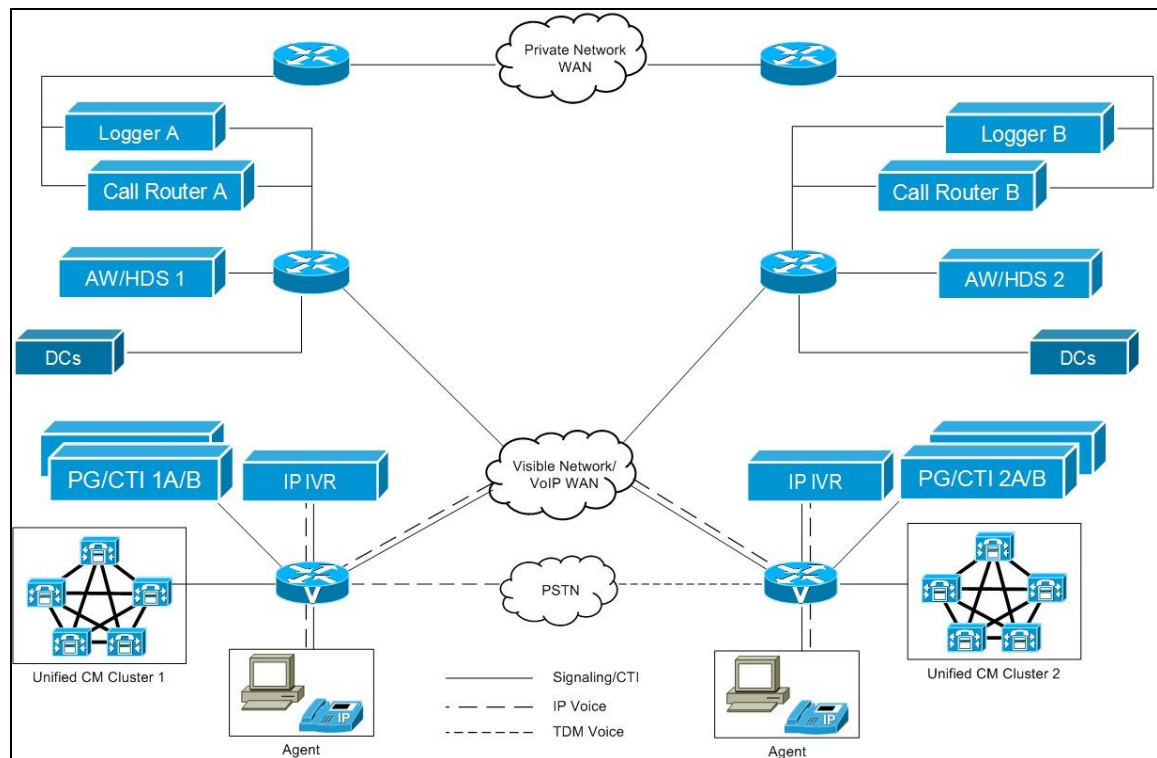
This white paper, intended for business decision makers and IT architects, describes Cisco best practices for Cisco Unified Contact Center Enterprise (UCCE) on Cisco Unified Computing System™ (UCS™). These best practices are based on a case study that allowed Cisco to migrate from the Media Convergence Servers (MCS) Legacy contact center infrastructure to the most efficient and advanced data center platform, Cisco® UCS. This Cisco on Cisco white paper will help you understand how to:

- Design your private network to support UCCE on UCS.
- Migrate your enterprise central controllers (UCCE) from MCS servers to Cisco UCS, and migrate UCCE nodes from physical to virtual.
- Move the locations of your central controllers.
- Migrate your Historical Data Server (HDS) servers from MCS to UCS with minimal data loss.
- Migrate dedicated physical UCCE domain controllers from Windows 2003 to Windows 2008 R2 running on UCS servers.
- Do all this without interruption to your contact center business.

Background

Cisco UCCE routes 22 million+ calls per year. Cisco has 63 global contact center clients of four specific types: Single-site noncustomer facing, multisite noncustomer facing, single-site customer facing, and multisite customer facing. Our contact centers support approximately 3000 agents globally. Cisco uses a fully redundant distributed UCCE with distributed call processing. Its central controllers are geographically dispersed between two sites, an A side and a B side (see Figure 1).

Figure 1. Cisco IT Core UCCE Architecture



Key:

- AW/HDS = Administrative Workstation / Historical Database Server
- DCs = Domain Controllers
- IVR = Interactive Voice Response system
- PG/CTI = Peripheral Gateway / Computer Telephony Integration

Problem

For several years, Cisco UCCE central controller components had been running on old MCS hardware located in the Cisco San Jose (SJC) and Research Triangle Park (RTP) data centers. The San Jose data center, one of the oldest at Cisco, was being replaced by a new data center pair in Texas; applications such as UCCE needed to be migrated out of the old SJC data center so that the center could be retired as a production data center and repurposed. Cisco IT needed to move these critical contact center servers. This move provided Cisco IT with the perfect time to upgrade to a new and better hardware platform, Cisco UCS.

Solution

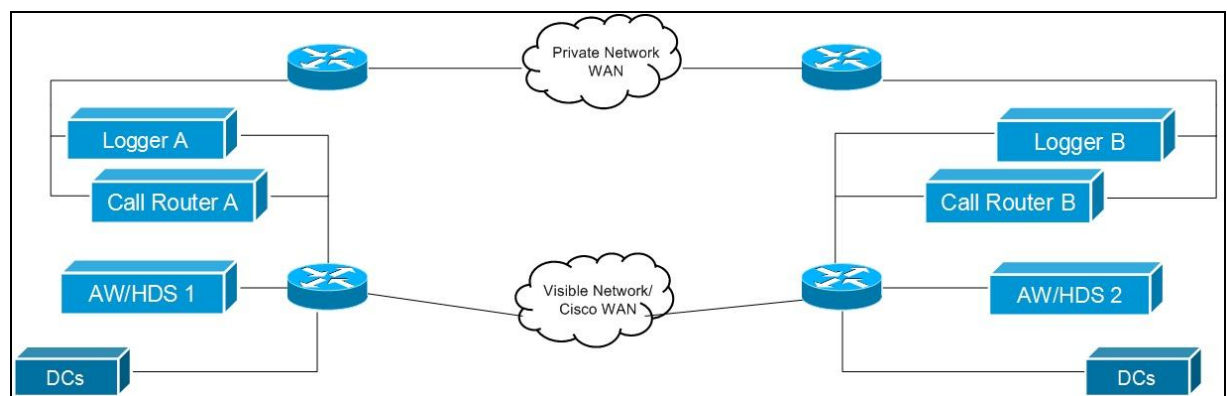
The IT initiative to move all applications from the old data center, and from MCS to UCS, would allow Cisco IT to significantly improve its UCCE infrastructure by moving to the most advanced data center generation platform, UCS. Cisco UCS aligns with the Cisco green initiative because it brings more efficiency than a legacy infrastructure, it saves on data center space and electrical power, and it uses compute and storage resources much more efficiently. (This migration cut UCCE power requirements in half, and requires only one-quarter the physical space in the data center.)

Cisco UCS also greatly simplifies hardware deployment and administration as well as saving significant cost on support and provisioning. For the contact center, where uptime is critical, having the central controllers running as a virtual machine on UCS also provides more resiliency in case of a failure, because the application can be easily and quickly moved to a new physical machine at any time. This project focused on UCCE components that did not have significant carrier network dependencies and thus were site independent.

To take advantage of Cisco UCS benefits and fulfill the IT directives, Cisco IT determined that the central controller A side would migrate from San Jose, CA to Richardson, TX into a new data center designed around UCS. The B side would remain in RTP but also move to the newer UCS platform.

Only certain UCCE components were addressed in the Cisco UCS migration project and detailed in this whitepaper. These components consisted of the central controller components, UCCE router and logger, historical data server (HDS), and two domain controllers (DC) per side, a primary and backup. Cisco has a separate domain and forest dedicated for the contact center. Figure 2 outlines the UCCE components addressed.

Figure 2. Part of Cisco IT Core UCCE Architecture Being Migrated to UCS



Design

The migration to UCCE on UCS had to be designed so that the migration met the functional requirements of the application but also accounted for the platform changes of UCS. The migration also had to be designed in a way that allowed for no impact to the business during the migration. Although the UCCE application remained the same, all the changes that UCS brought into the environment needed to be thoroughly tested. The principal portions of the design were developed in a UCS development environment. In this development environment, Cisco IT discovered that distinct ports (described later) needed to be opened in the access list between the Windows 2003 and Windows 2008 RS domain controllers. In this environment, Cisco IT also developed the configuration for the UCS network adapter cards.

After being tested in the development environment, the design was implemented and tested in the staging environment, which was setup in Cisco IT's Solutions Verification lab. The staging environment more closely mimicked Cisco IT's production environment, and several key portions of the design were verified, including the network configuration required for quality of service (QoS) and the full UCCE application migration from MCS to UCS.

While the design was being developed and tested in the lab, the portions of the design that were known and already tested were built in production. All the UCCE components for this project were built Greenfield (that is, built completely new) on UCS, essentially setting up a parallel UCCE to migrate contact center traffic. The Virtual Machines (VMs) for UCCE were installed in UCS server groups (or pods) that met the Unified Communications (UC) on UCS requirements. For additional failover resiliency, a spare UCS blade is available in the event that a failure occurs with the current production blade and VMs need to be moved.

Table 1. Comparison of Space and Power Required by UCCE on MCS and UCS

Comparison: UCCE (MCS vs UCS)	UCCE on MCS	UCCE on UCS
Number of servers	10 MCS 7845	10 VMs on UCS B-200 half-blades
Space required	20 RU	4.8RU
Power required	3.38 kW	1.58 kW (2)

(1) The two loggers, two call routers, and two AW/HDS: these six of the ten virtual machines (VMs) were initially deployed on six new dedicated half-blade UCS servers. Eight half-blades fit into one six-RU UCS chassis, so those 6 half-blades use 6/8 of a chassis (although they were not all deployed in the same chassis in the data center). The four domain controller VMs were placed into existing data center half-blade servers, which were already running 7-12 other VMs. Prorating these numbers came to a total of 6.4 UCS half-blades dedicated to UCCE. This number will decrease as Cisco IT loads more VMs onto these half-blade servers.

(2) Based on MCS 7845 requiring 338W to run at 50 percent load; and a B-200 half-blade requiring 247W to run at 50 percent load; using the prorating described in footnote (1).

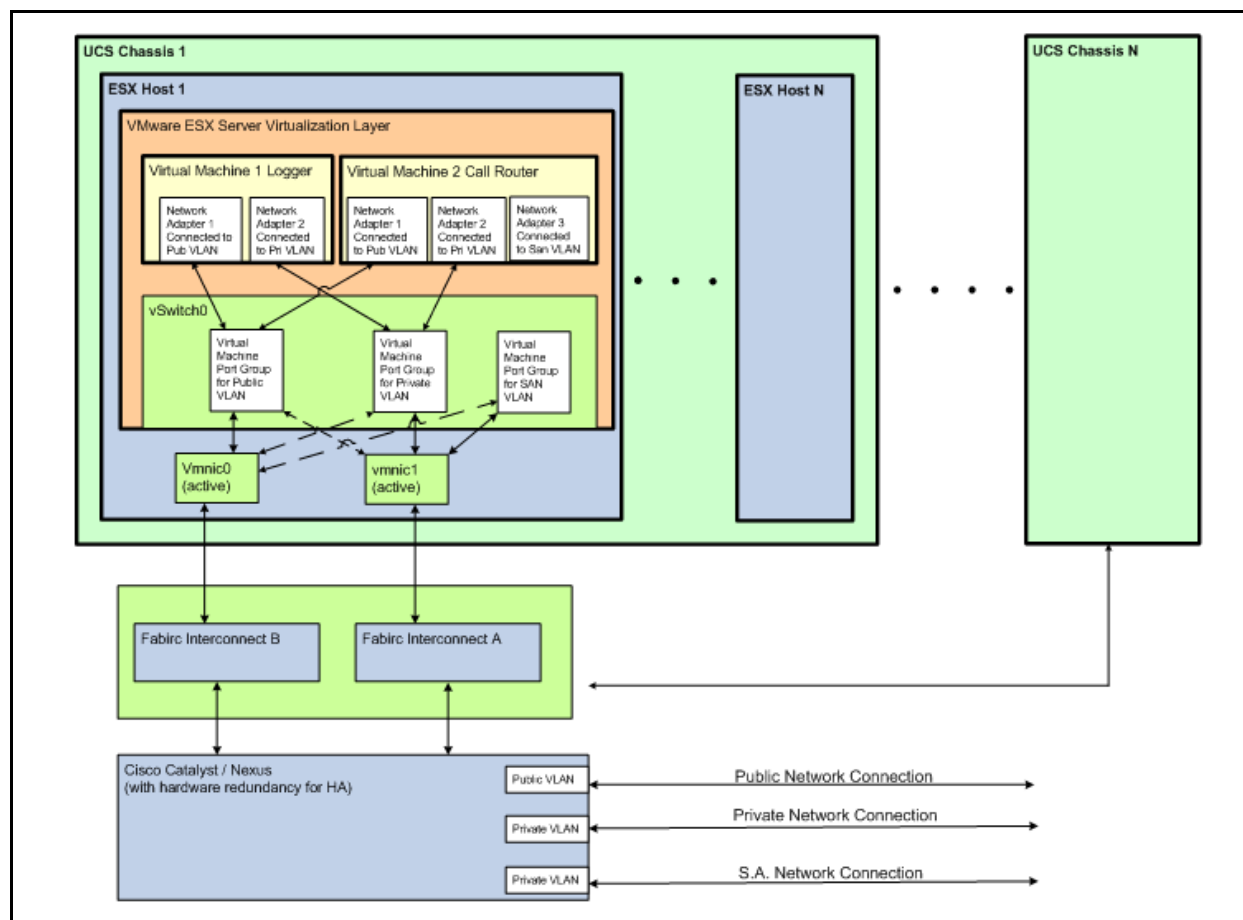
UCS Design Considerations

Virtualizing the application on UCS required some additional networking configuration in ESXi Server and the UCS Manager for the UCCE components to communicate with each other. In designing UCCE on UCS, Cisco IT referred to the Customer Contact Business Unit (CCBU) wiki:

http://docwiki.cisco.com/wiki/UCS_Network_Configuration_for_UCCE

All CCBU recommendations were followed, except for the network adapter card recommendation. The production UCS server groups chose the M71KR converged network adapter cards instead of the M81KR cards. The M71KR cards were our current internal Cisco IT UCS standard, and they were able to accommodate our failover requirements of the public, private, and SAN networks required to run UCCE. A suitable workaround was made that creates a primary and secondary failover path between the ESXi Server's vSwitch and the Network adapters for each of the UCCE networks as outlined in Figure 3.

Figure 3. UCCE Configuration Components on a UCS Blade Server



Network Design

Cisco IT's initial deployment of UCCE 8.0.2 on VMs is on UCS B-200 servers. The VMs are configured based on the VMware ESXi 4.0 hypervisor, running Windows server software.

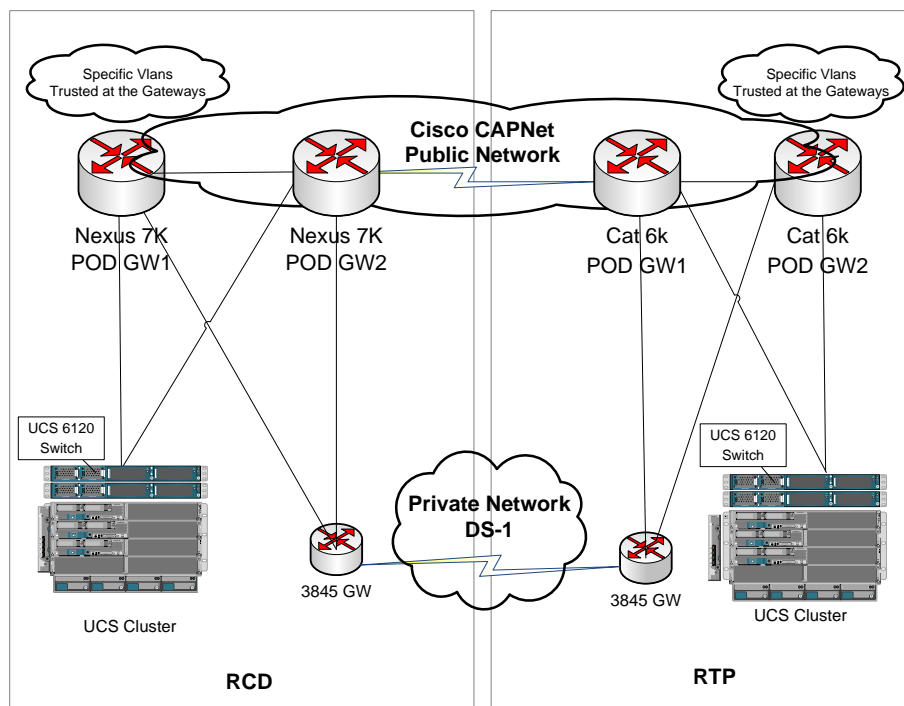
Once the VMs and UCS were configured for the various UCCE networks, these networks needed to be configured. For the public network, which allows communication from various contact center sites around the world to the central controller, Cisco IT used the corporate backbone network, which is designed to carry all of Cisco IT's voice, data, and video traffic. For redundancy and reliability, the team also built a private network to communicate between the A and B side central controllers and an additional private point-to-point connection similar to the private communication between the MCS central controllers. We ordered and installed two new routers with T-1 cards and a new T-1 to connect each side of the central controller sides.

The UCCE application enables its traffic to be marked for QoS using DSCP, but some special accommodations had to be made for private and public traffic on separate VLANs to be correctly recognized and prioritized by the network for QoS. We selected the top-of-rack UCS distribution layer switch (the 61XX series was used because the Cisco Nexus® 1000v is not yet supported for UCCE in 2011), but the 61XX does not allow ports to be trusted. The distribution gateways, Cisco Nexus 7000 in Site A and the Cat 6K in Site B, needed to be configured so that the VLANs used for private and public traffic could be trusted. During the network discussion, we considered using the Nexus 1000v virtual switch, which works well in the Unified Communications environment but is not recommended with UCCE (in 2011). Future UCCE releases are planned for better Cisco Nexus 1000v interoperability in future, which will make our QoS planning easier.

Network Topology in the Data Center

The two new routers (one server in Richardson Texas, and one in RTP) for the private and signaling area networks (SAN) were downlinked to a pair of distribution gateways (Cisco 3845 routers). This is the same pair of distribution gateways that the UCCE VMs on UCS were configured on at each site. Each router has two GigE ports (one uplinked to UCS server gateway 1, and the other for the redundant link to UCS server gateway 2). In addition, each gateway router has a serial interface for the T1 connection that passes the heartbeats and synchronization between the central controllers of the two sides A and B (see Figure 4).

Figure 4. Network Topology on the Data Center Floor



The GigE ports were configured for sub-interfaces to route the private and signaling access network separately, on two separate VLANs. The distribution gateways' southbound interfaces to the new routers were configured for VLAN trunking.

A layer 2 adjacency was established between the UCCE VM on UCS to the new routers, to isolate the public network and the signaling access network. The VMs were configured with static routes to the IP address of the new router on the private subnet for the private communication. The default gateway (Hot Standby Router Protocol [HSRP]) addresses of the server pod gateways were configured on the UCCE VM, which is used for all other communications.

Due to the potential of the UCCE VMs needing to route intelligent contact management (ICM)-to-ICM traffic, a Cisco EtherSwitch® module was also installed on the routers to provide Ethernet connections for carrier network routers. At the time of this implementation, the Cisco EtherSwitch module was not being used, but it is there in case we need to interconnect ICM-to-ICM with an outsourced contact center partner. In addition, the Integrated Routing and Bridging (IRB) was configured to allow bridging of the uplink interfaces to the LAN ports on the EtherSwitch module.

Migration

The migration to UCCE on UCS had to be designed in a way that allowed for no impact to the business during the migration. The network was down for only about 4-5 minutes in the middle of Saturday night: the length of time that it took to shut down the router on the MCS side and to bring up the router on the UCS side. Test calls made right after that proved the migration went smoothly.

With the MCS UCCE components upgraded to the 8.0.2 supported version in 2011 that was compatible with UCS and with the new UCS infrastructure installed and tested for proper communication, the migration process could begin. The migration plan consisted of three phases, which were performed over a period of 4-5 months. This phased migration was done to mitigate risk and perform work during distinct maintenance windows.

Phase 1: Migrating the Domain Controllers

We began the domain controller migration in late August 2011. With four new VMs installed on UCS running Windows 2008 R2, the new UCS domain controllers (DCs) were configured using the `dcpromo.exe` command (part of Windows Server). For `dcpromo` to connect from the Windows 2008 R2 server to the 2003 servers, four ports are used (specifically ports 138 UDP, 139 TCP, 445 TCP, and 123 UDP). Thus any access control lists (ACLs) between the servers must have these ports opened. New VM DCs were added to the existing contact center forest, and current configurations were imported from the MCS 2003 domain controllers. Once that was completed, the UCS UCCE components were added to the UCS domain controllers. Because UCCE synchronizes its time through the domain controllers, a series of registry additions were made to synchronize the DCs to the corporate time servers. These time servers are the same as those used by the ESXi servers, so that the UCCE VMs reside so all components are in synch.

Once the domain controllers were in place, a Cisco IT-developed custom java batch (release, reregister, refresh) script was run during a maintenance window. The script went to every peripheral gateway and distributed AWA nodes and updated the DNS settings to point them to the new UCS domain controllers. UCCE services were restarted in a controlled fashion on each node of the redundant pair to minimize impact on our contact center agents. Once services came up, the UCCE nodes throughout the enterprise all used the UCS domain controllers. The Domain Name System (DNS) settings for the HDS and Central Controller Nodes were updated during their respective migration phases.

Phase 2: Migrating the Historical Data Servers

We began this HDS migration in early November. The HDS servers on UCS were built in the A and B side locations. Custom reporting applications and the Work Force Management application were then installed on top of the base HDS. The data retention times for the various database tables were configured the same on the UCS HDS as on the MCS HDS. With about 6 months of data stored locally, a full SQL backup of the database was taken from the MCS database and then copied to the location of the new UCS HDS. It took nearly two full days to copy all the data over the network. This data was restored into the HDS database. Then the data for the past two days was quickly backed up and copied over the network and appended to the HDS database.

Because some of the custom applications resolved to the original HDS hostname, an alias was setup to route traffic from the MCS HDS servers to the new UCS HDS servers. The new HDS servers were

added to DNS on the UCS domain controllers. The UCS HDS servers pointed to the MCS central controllers and were started. Replication of the newest data (starting from when we made the earlier backup to the present) completed adding data to the HDS database during the Saturday night 1-2 minute change management window. A separate Webview server that was pointed to the MCS HDS was re-pointed to the UCS HDS server. Because Cisco IT uses Cisco Unified Intelligence Center (Cisco UIC) for contact center reporting, the CUIC data stores that were originally configured to leverage the MCS HDS were rebuilt to leverage the UCS HDS servers as data stores. Reports were tested and verified to be working correctly.

Phase 3: Migrating the Central Controller Node

We completed the last phase of the migration in the first weekend of December 2011. The UCCE central controllers on UCS were all new hardware, and had completely new hostnames, and new IP addresses; on the A side, they had even moved to a new location over 1600 miles away. The only thing that was the same was the version of UCCE and the configuration.

Even though the A side was moving to UCS in the new data center, in a new time zone, all four central controller nodes were configured with the time of the MCSA side. The same time zone on UCS central controllers was used so that it would not affect the client's understanding of reports.

Before the migration, additional testing was performed. With one peripheral gateway (PG) node configured on the UCS central controllers, services were started to help ensure that all processes would go active. Tests of the new UCS infrastructure were performed to verify network connectivity as well as QoS.

Once these tests were performed and the infrastructure was verified to work correctly, work on the last phase of UCS migration, the central controller, could begin. After every step taken, central controller migration process test calls were made to confirm correct UCCE operation.

During a maintenance window (one 5-minute outage time on Saturday night in December), all changes to the database were locked out by altering the registry on the MCS central controller. The ICM registries from the MCS Call Router were exported, and we imported these registries to the new UCS Call Routers. The number of PGs configured on the MCS Call Router was verified and UCS router matched. The Logger database server configuration was exported using the Cisco icmdba utility export function (built into the ICM software). The UCCE configuration was exported into files from the MCS logger and imported into the UCS logger database using the icmdba utility. Then all services on the UCS central controllers were shutdown, and all services on the B side MCS routers and loggers were also shut down. At that point, all call control routing was being handled by the A side MCS central controllers.

An alias to redirect all PG servers to new A-side UCS central controllers was created, and the MCS central controller hostnames in DNS were renamed to "-old". All PG services were cycled and verified that they could resolve to the A side for the UCS logger and routers. After this was confirmed, it was time to switch the active central controller from MCS to UCS. The MCS A side Router / Logger was shut down, and immediately after services stopped, the A side UCS Router / Logger was started. At this point, central controllers were running on UCS. This was the stage where the back-out plan could be implemented if needed. Because the UCS A side was successful, the same steps were performed on the UCS B side. An alias was created to redirect the PG servers to new B-side UCS central controllers, and we then renamed MCS central controller hostnames to "-old". All PGs were verified to resolve to

the B side for the UCS logger and routers. The B side UCS Router / Logger were started and synchronized to UCS Logger A to Logger B. All distributive administrative workstations (AWs) were pointed to the new UCS central controllers. This included the UCS HDS servers that had been had migrated in an earlier phase. Finally, the database lock on the logger database was removed, and the configuration changes were tested.

This completed the migration.

Conclusion

When all phases of the upgrade were complete, final test calls were made to verify the correct functionality of all UCCE applications. No incidences were reported of any impact to the routing of calls to any contact center business. In fact, the upgrade was so successful that until communications of the upgrade were sent out, none of the contact center businesses were aware of any change. Additionally, all data in the HDS servers were preserved. Most importantly, Cisco upgraded its infrastructure to take advantage of the resiliency and tremendous efficiency savings that UCS provides.

Cisco IT attributes this success to many months planning, design, and testing and to taking the design and implementation through Development and Stage environments. This enabled issues to be identified and mitigated before the project moved into the production environment. Even at the production level, a detailed test plan was followed to help ensure the platform and applications were in stable condition.

Many internal Cisco engineering groups were involved in this process from Design, Networking, UCCE Application, Hosting, and Virtualization to Project Management, CCBU, and in particular, the Cisco Assessment to Quality (A2Q) process. Only by following and adhering to internal Cisco policies on design, Project Lifecycle, and Change Management could this project be successfully planned and implemented.

When this UCCE on UCS project began, a few instances existed of Greenfield UCCE on UCS, but no examples were available of an enterprise contact center brownfield migration the size of Cisco's from which to draw insight. This whitepaper shares the UCCE on UCS design and migration approach, which Cisco hopes can be an aid to other customers planning UCCE on UCS upgrades.

For More Information

To read additional Cisco IT best practices and case studies on a variety of business solutions, visit Cisco on Cisco:
Inside Cisco IT www.cisco.com/go/ciscoit

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)