



# Cisco on Cisco Best Practices Data Center Operations Management

# Cisco Data Center Management

**Cisco IT Operational Practices / Data Center Operations Management:** This document provides an overview of how Cisco Systems manages its data center operations command center and production data centers. Data centers are the core of the global Cisco network, one of the largest and most complex networks in the world. Customers can benefit from Cisco IT's real-world data center management practices.

**“There is a success story here, and it goes further than just the OCC team. It is not just a success story of operations. It is a success story of Cisco IT and how we have come together to build a data center solution.” —Dick Corso, Manager, Data Center Operations Group**

## Background

Cisco has 5 production data centers and 41 engineering data centers worldwide. Two production data centers are located in San Jose, California, and the remaining three are in Research Triangle Park (RTP), North Carolina; Amsterdam, the Netherlands; and Sydney, Australia.

The Cisco IT Operations Data Center is the main production data center on the San Jose, California, campus. The IT Operations Data Center supports Cisco's intranet systems; enterprise resource planning (ERP) systems such as financial, data storage, and IP telephony infrastructure; and the many employee-facing applications and databases. It also houses the Operations Command Center (OCC), where business-critical resources within Cisco data centers and across Cisco networks worldwide are monitored.

Remaining production data centers perform specific functions, as follows:

- The second production data center in San Jose supports the public Website, Cisco.com, and the online applications and tools Cisco provides to customers and partners.
- The production data center in RTP supports application development, testing, and staging environments and serves as a disaster recovery site for the two San Jose data centers.
- In Amsterdam, the Netherlands, the production data center houses systems and databases that support the Europe, Middle East, and Africa (EMEA) region.
- In Sydney, Australia, the production data center houses systems and databases that support the Asia-Pacific region.

The 41 engineering data centers, called server rooms, house servers and databases to support Cisco software and hardware product development. Ranging in size from 20,000+ square feet to server rooms without raised floors with only a few hundred square feet, most of these sites were part of acquisitions by Cisco.

In 1999 when additional data processing hardware was needed but space was unavailable in the existing San Jose data center, Cisco built the current IT Operations Data Center. Since then, this data center has expanded to occupy 14,269 square feet consisting of four areas: Cisco IT OCC, the “original” data center constructed in 1999, a Build room, and the “expanded” data center added in 2001.

The remainder of this document describes the operations, management, design, and functions of each of these areas.

## Cisco Operations Command Center

According to Dick Corso, manager of the Data Center Operations Group, “The mission of the Operations Command Center is to facilitate problem resolution for significant failures that could impact business continuity.”

The OCC is tasked with tracking and responding to issues regarding priority 1 (P1) and priority 2 (P2) systems located in *all* the data centers worldwide. The OCC currently monitors 374 P1 applications and 500 P2 applications and 7857 P1 and P2 resources, including switches, routers, and servers across all operating systems and architectures. Among the P1 applications are:

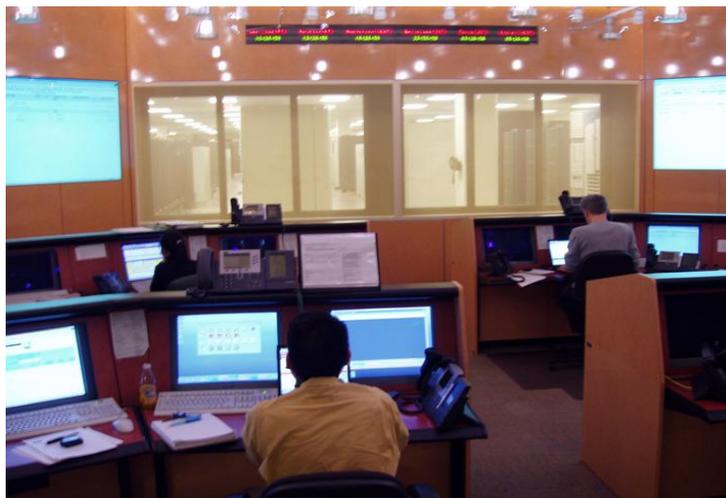
- Oracle ERP applications that include pricing, order entry and viewing, lead-time planning, manufacturing, invoicing, and financing
- Business-to-business (B2B) e-commerce tools for exchanging business documents with trading partners
- E-sales support tools to create sales quotes and to view real-time bookings, data, alerts, and relevant news
- Content management and delivery tools to connect employees with streaming video events and stored video training information
- Telephony, call center, audioconferencing, and e-mail services

Initially, the OCC monitored only P1 and P2 hosts and applications within the five production data centers. In 2001 the engineering and business production resources were merged. As a result of this reorganization, it became clear that managing all resources from one place would be more efficient, and that the OCC could scale to manage the added resources.

The operation of the OCC has evolved in another way as well. Until 2004 it was the only site where global incident management was performed. Two shifts (6 a.m. to 6 p.m. and 6 p.m. to 6 a.m.) of three technicians each staffed the OCC 24 hours a day, seven days a week. In February 2004, Cisco relocated the 6 p.m. to 6 a.m. shift from San Jose to the Divyasree data center building in Bangalore, India, where a similar command center is located.

In 2000 there was a staff of 20 handling 400 to 500 incidents per year. Today, the worldwide OCC team consists of 14 members who handle approximately 9000 incidents per year—a remarkable improvement in productivity. “That’s been a real victory for our process, and our automation tools,” says Ian Reddy, Cisco IT Global Operations manager.

The OCC in the main data center in San Jose (Figure 1) occupies approximately 1500 square feet. This includes about 900 square feet in the main area, approximately 300 square feet in the viewing or Executive Briefing Center platform area, and 300 square feet in a side cube area. In comparison, the other OCC in San Jose is about 550 square feet and the Bangalore OCC is about 350 square feet.

**Figure 1 Main Data Center OCC in San Jose, California**

The role of OCC staff is to provide communication, coordination, and documentation during incidents involving P1 and P2 hosts and applications. The OCC team does not troubleshoot technical problems. These are addressed by approximately 150 teams worldwide that have responsibility for P1 and P2 applications, systems, databases, and network infrastructure.

### **Communication**

“Communication is letting the right business or support groups know about the existence of a down or degraded resource,” says Ian Reddy. When a P1 or P2 resource goes down, the management tool displays a notice in red on the monitors in the OCC. The OCC team is trained to open a case on the failed resource within five minutes, which automatically initiates a page to the support engineers responsible for that resource.

It should be noted that a distinction is made between P1 and P2 alerts. P1 resources support business-critical functions, and require an immediate response 24 hours a day. P2 resources, on the other hand, support employee functions that are mostly used during the workday, and are treated like P1s only during local business hours where the failed resource is located.

To ensure the right people are notified in the event of a resource failure, the support staff responsible for each resource subscribes to mail aliases that are used by the OCC team to alert them by pager. If the responsible support staff fails to contact the OCC within five minutes of receiving the notice, the OCC will page the on-call support person, then the on-call person’s cell phone. If those efforts are unsuccessful, the OCC pages the support person’s manager, then the director and, if necessary, the organizational vice president to get a response.

Cisco employees calling in to report problems or to respond to pages call the OCC. All the phones in the OCC ring simultaneously, and anyone on duty can answer any call. The goal is to answer each call before the second ring. Support staff remains on the call with the OCC until the problem is resolved, or they negotiate a time when they will call back to the OCC.

### **Coordination**

“Our team will coordinate the overall response for multiple groups,” says Reddy. Some failures may affect several applications or resources simultaneously, requiring several duty support engineers working together on a problem. The goal of the OCC team is to get all the duty support

responders required to identify and resolve the problem talking together to keep the resolution process active. Typically, a conference bridge is used to connect, for example, a database administrator, network technician, and system administrator together to diagnose the problem.

### **Documentation**

Every detail of an incident, from a short-term fix to a full recovery, is captured by the team in real time. This ensures that other technical resources and managers are kept informed and also helps support engineers focus on fixing the problem by off-loading documentation and outbound communication tasks. “Everything that takes place during an incident is documented by the OCC team,” says Reddy.

All incident-related information is input into the Alliance system, a trouble-tracking application customized by Cisco IT. Critical data captured includes the resources that went down; when they were again operational; what areas of the business were affected; how, why, and when the telephone call was set up; which engineers were on the call; what decisions were made; and what actions were taken. Information not captured as a “data value” is logged as an ad hoc comment in the activity log. This documentation can be used to review the case at a later date, to help with continual process improvement efforts.

The OCC focus is on getting a resource operational. Engineers responsible for the resource and responsible for getting the resource operational under the coordination of the OCC are also responsible for follow-up problem management. This problem management process includes root-cause analysis and a long-term resolution after the service has been recovered. The OCC initiates the process by assigning the case to one of the duty support responders, whose responsibility is to shepherd it through the long-term resolution process. It is up to the support teams to perform the root-cause analysis, propose a long-term fix, and document everything in the Alliance system.

### **Other OCC Responsibilities**

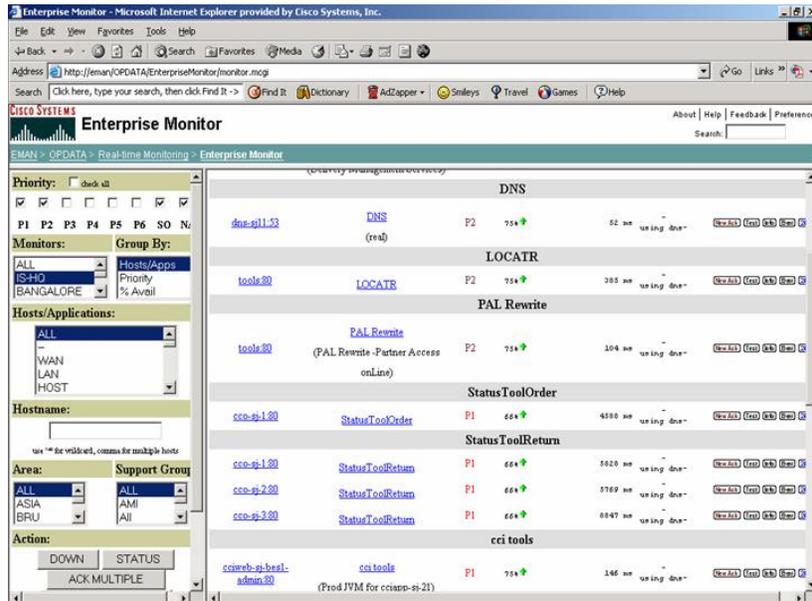
In addition to its primary responsibilities of communication, coordination, and documentation, the OCC handles incidents and change management, and is involved with month-end data processing. Month-end processing is a set of batch jobs that are run to close the monthly financial cycle. A product scheduling group within the OCC team works closely with the month-end processing teams to ensure that Cisco receives its month and quarter-end financial reports on time.

### **Monitoring**

The OCC team uses a suite of internally developed management tools known as Enterprise Management or EMAN to perform resource monitoring, automatic page alerting, change management tracking, and availability measurements. The OCC specifically uses the EMAN Enterprise Monitoring tool to supervise P1 and P2 resources. Approximately 30,000 applications, databases, and network devices are monitored by EMAN, with about 10,000 of those identified as P1 or P2.

The EMAN Enterprise Monitoring tool sends out “pings” to each resource it monitors, 24 hours a day. A series of two pings are sent out to network resources every 15 seconds. If a resource fails to respond to one of these, EMAN reports a degraded service condition. If the resource fails to respond to these pings four consecutive times, EMAN reports zero percent availability—the resource is down. Failures associated with P1 and P2 resources are displayed in red on OCC monitors.

Figure 2 EMAN Availability Monitors



EMAN has 14 network health collectors worldwide. These include two in San Jose, California, and one each in RTP, North Carolina; Richardson, Texas; Boxborough, Massachusetts; Sydney, Australia; Tokyo, Japan; Bangalore, India; Singapore; Beijing, China; and Hong Kong. Each site has its own EMAN rack of servers dedicated to monitoring the local environment.

The OCC also uses HP OpenView VantagePoint Operations (VPO), which monitors a production-scheduling tool called Dollar Universe. Dollar Universe schedules and runs production batch jobs on the hosts. Should a batch job fail, Dollar Universe sends an alarm through HP OpenView to the OCC team. Resolution of a failed batch job follows the same process as a P1 incident.

## Modems

Not all equipment monitoring is done by Cisco. “Vendors need a way to remotely monitor their equipment in our data center,” says Dick Corso. Many of the storage frames have small modem boxes next to them. If a device experiences a problem, it automatically calls the vendor office. The vendor can then dial in through the same modem and diagnose the problem.

Analog modems will soon be replaced by a VPN solution over the Cisco IP network and the Internet. This will give vendors direct access to their equipment, but to no other devices.

## Change Management

“Change is a constant within Cisco, and change management is critical to the OCC team and to the rest of Cisco,” says Dick Corso. The OCC monitors all approved change requests within their windows of implementation—approximately 80 each day. Carefully managing change is critical to maintaining a highly available network. Even with the best controls, a large percentage of problems result from changes, so the OCC team watches them closely.

EMAN supports Cisco IT’s change management tool, which is tightly integrated with the EMAN alerting process and also availability monitoring. The engineer performing a change submits a change request through the change management tool, answering a series of “risk and

effect” questions and identifying the resources that will become unavailable. The answers to these questions (that is, the level of risk and impact) determine who must approve the change—the higher the risk, the higher the level of approval required.

When the change window begins, the engineer brings down the device or application. The monitoring tool records this scheduled downtime and monitors it, still continuing to ping the resource every 15 seconds, but no action is taken to alert the support teams. Monitors in the OCC display these resources in blue, unlike incidents that display down or degraded resources in red.

If a resource remains unavailable when the change window expires, the display on the OCC monitor changes to red and support staff is paged, as if an incident had occurred. Alarms and pages similarly occur if a change is initiated prior to the scheduled change window, or if a resource not listed in the change request is affected. This helps motivate engineers to use the change management process, and to complete all changes within the scheduled change window.

### ***OCC Redundancy and Disaster Recovery***

Uninterrupted monitoring and problem resolution is critical. Redundancies and back-up provisions must be in place, and the OCC has several contingencies in the event of equipment or communication failure. If communications are interrupted at the OCC in the data center in building 12 during the day shift, the building K data center in San Jose becomes the failover site. If Building K becomes unavailable, the OCC staff can establish a virtual OCC from their homes with their laptops and VPN connections. If necessary, the Bangalore staff could be called to work.

If communications are interrupted at the OCC in Bangalore during their day shift (PM Pacific Time), the Waterford building (Bangalore) becomes the failover site for the Divyasree (Bangalore) OCC. If Waterford becomes unavailable, Bangalore OCC staff can establish a virtual OCC from their homes with their laptops and VPN connections. If necessary, the San Jose staff could be called to work.

The same technology that enables these failover scenarios also allows calls to be sent to the OCC in San Jose during the day (Pacific Time) and Bangalore during the evening (Pacific Time). “We use Cisco voice over IP, which allows the same phone number to ring anywhere in the world,” says Corso. Within this IP telephony infrastructure built on Cisco AVVID (Architecture for Voice, Video and Integrated Data), Cisco CallManagers switch incoming calls automatically from San Jose to Bangalore at shift change, and back again 12 hours later. This process can be managed consistently, ensuring reliability of the voice network.

To protect communications to and from the OCC in the event of a disaster, the IP telephony service within the two San Jose OCCs has been equipped with Survivable Remote Site Telephony (SRST). Most IP phones on the San Jose campus are connected to the CallManager super cluster. IP phones in the two OCCs, however, are connected to a pair of dedicated switches within the data center, and then to a pair of Cisco 3745 routers running SRST. If IP phones within the San Jose OCCs lose communication with the campus super cluster, they automatically register with the nearby SRST routers, preserving communications capabilities—even if the remainder of the campus is without phone service. Direct drops to the local exchange carrier for the primary OCC phone numbers further ensure continuing communications.

Note: For more information about SRST in the OCC, a case study is available at <http://www.cisco.com/go/ciscoit>.

For data, a disaster in the San Jose building 12 data center would initiate a failover to RTP, North Carolina, where all backup ERP and Cisco.com applications are stored.

### **Build Room**

“The Build room provides an area for equipment vendors to rack, stack, configure, and burn in new systems before they go into production and to try out new equipment and configurations without impacting our production environment or setting off alarms,” says Ian Reddy.

The Build room and the Engineering data centers are similarly built for flexibility, ease of access, and ease of configurability, and portend the direction in which Cisco’s production data centers will likely evolve. Cabling and network architecture in the Build room is designed to flexibly

support quick equipment changes, unlike the production data centers that are designed for very few changes to equipment placement. Whereas the Production area of the data center has a single network area at one end of the room, the Build room has a network cabinet in every half row of each of its four rows. Not having to pull new cable the length of the room makes connecting and reconnecting new equipment and moving equipment much easier.

**Figure 3 Build Room**

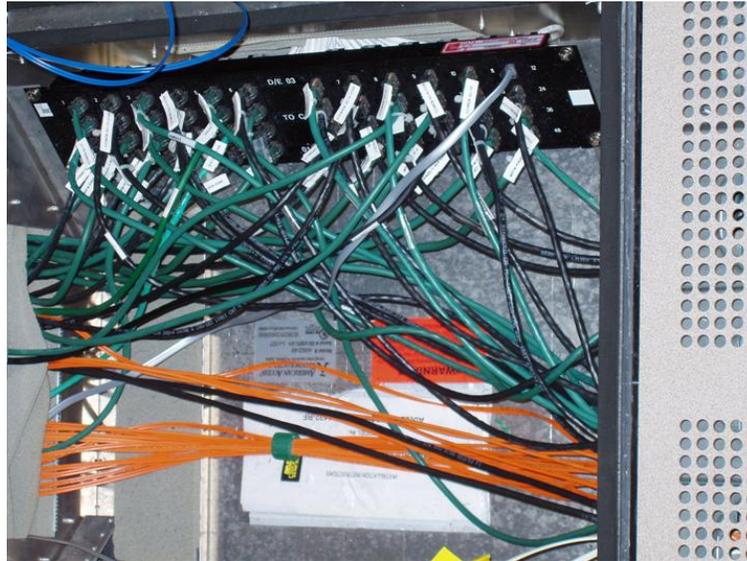


Within the network cabinet in each half row of the Build room is a Cisco Catalyst 6500 Series Switch. The Cisco 6500 Series is used in all Cisco IT data centers to connect data center resources to the desktop LAN and to support all levels of Cisco IT's desktop network worldwide. By standardizing on a single platform, the infrastructure becomes more stable, predictable, and easier to maintain. The Cisco 6500 Series also supports various media types, including copper and single and multimode fiber, to accommodate the disparate types of equipment in Build rooms and in data centers.

Also in each network cabinet is a Cisco 3600 Series Router. The Cisco 3600 Series routers are used to connect all the server console serial ports and concentrate them. By putting all the console ports on the network, Cisco IT eliminates the clutter of individual keyboards and monitors traditionally attached to each device. Using very consistent standards for host and router names, engineers can easily access the right host, router, or switch through the network from any network-attached PC or laptop.

The cabling system in the Build room is standardized as well. Under each floor tile is a cable breakout box connected to 12 or 24 fibers and clearly labeled with port numbers. Connecting a new device is as easy as dropping a patch cable to the breakout box, going to the zonal cabinet—which is clearly labeled with the row, breakout box, and port—and plugging that into the Cisco Catalyst 6500 Series. Engineers no longer must pull a series of floor tiles or cables. This same, standardized, and more flexible cabling system has been adopted in all the newer Cisco IT data centers worldwide.

Figure 4 Breakout Box Under Floor Tiles



## Data Center

“The interesting fact about the San Jose building 12 production data center is the variety of solutions and partners represented here,” says Ian Reddy. The equipment within this data center, as in the four other production data centers, is largely supported by vendors under contract with Cisco IT. Vendors perform the upgrades and changes, as well as troubleshooting and repair if a problem arises related to their equipment. Because support contracts stipulate that equipment is to be left in its vendor state of packaging, much of the equipment is installed with its original cabinetry rather than in standard engineering racks.

Unlike the Build room where a network rack is situated at the end of every half-row, the San Jose building 12 production data center uses a single rack of network equipment at the end of the data center. If the data center were to be rebuilt, it is likely that the more flexible Build-room model would be used. Because of the minimal changes that occur in a production data center, however, network design flexibility is not yet a critical issue.

### Storage and Servers

One of the larger categories of equipment in the San Jose building 12 data center is storage, representing about 800 terabytes. Much of that storage uses EMC frames, with HP frames supplying the remainder. Until two years ago, nearly all storage was connected directly to each host. Connecting two or three hosts to a single storage frame was inefficient and caused storage frames to be underutilized. Today, hundreds of hosts are connected to a group of storage frames through a storage area network (SAN), creating a large, efficient pool of shared storage. This SAN is supported by Cisco MDS 9509 storage switches.

Note: For more information about Cisco IT data center SANs, case studies are available at <http://www.cisco.com/go/ciscoit>.

Many servers that can be stacked and pooled together are in distributed environments in the data center. Most of these run Linux and Windows OSs. Some are as large as the Sun E-10000 servers with 28 processors, supporting multiple e-commerce applications. Others are smaller and highly specialized, such as Cisco CallManagers. Cisco has 54 buildings in San Jose. In 2001, every building had a PBX to provide telephone

service. Today, a cluster of five CallManagers in the primary San Jose data center—occupying a quarter of one rack—has replaced all the PBXs.

Note: For more information about Cisco AVVID (Architecture for Voice, Video and Integrated Data) network and network management, see the case studies at <http://www.cisco.com/go/ciscoit>.

The primary San Jose data center also provides tape storage for vital records; however, backup storage for San Jose is provided in the RTP data center, which acts as a hot standby site. The RTP data center was created to replicate and store critical San Jose systems data should a major failure occur. The ERP environment in San Jose continuously transmits data to RTP. Should the data need to be recovered, the process would take about 20 minutes.

### Cabling Beneath the Raised Floor

Cisco IT has standardized the cable layout under the raised floor in the San Jose production data centers, as well as in the other production data centers around the world. Network cables rest in suspended trays closest to the raised tiles. Power cables are located near the concrete floor to provide vertical separation from the network cabling. Horizontal separation is created by running network cabling beneath one row of tiles and power beneath another row in each aisle. Closest to the concrete floor is the copper grounding wire arranged in a two-foot grid pattern throughout the data center.

Figure 5 Cabling Under Raised Floor Tiles



### Fire Suppression

“Fire suppression is important in a data center,” says Ian Reddy. In the San Jose building 12 data center, two forms of fire protection are activated in stages. Smoke sensors are mounted in the ceiling throughout the data center. When one detects smoke, it sets off an alarm, which dispatches Cisco security to investigate. If two sensors detect smoke, the system assumes a fire condition exists and begins a 30-second countdown procedure. Room lights begin flashing and, unless a technician in the area presses one of the designated panels to suspend the countdown, FM200 will discharge throughout the entire data center.

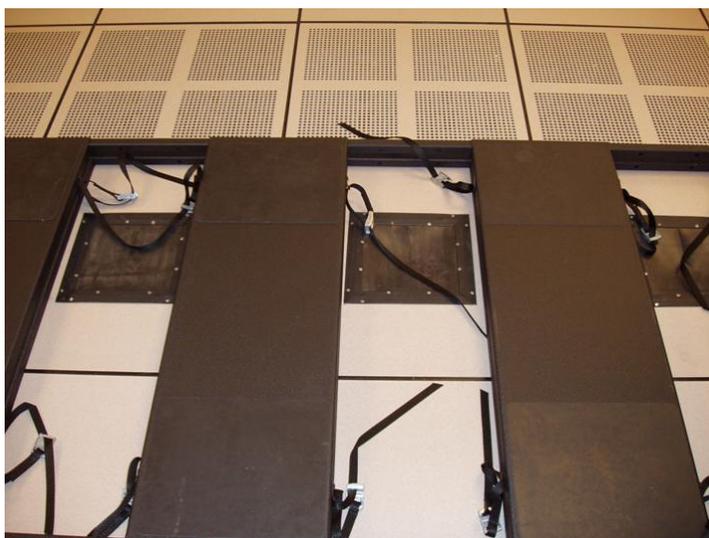
FM200 is an environmentally and human-friendly replacement for Halon. FM200 removes enough oxygen to extinguish the fire but not enough to suffocate a person on the data center floor. When FM200 is released, empty or “dry” sprinkler pipes fill with water. Only a sufficiently hot fire beneath one or more of the sprinklers will trigger the release of water, and only in the area of the fire.

Water can seriously damage any equipment it contacts. The combination of water and FM200 creates a highly corrosive mixture that can cause even more damage to circuit boards. Cisco IT accepts this risk to limit the spread of fire and to give anyone in the data center time to exit the area.

### Earthquake Protection

“We’ve been concerned about the impact of an earthquake on our data center here in San Jose because it’s a seismically active area,” says Reddy. Many companies attempt to prevent equipment from moving around in an earthquake by bolting it to the floor or wall. But an earthquake can transmit significant shocks to hard drives and other equipment that can damage or even destroy them. Insurance can replace sheared cables and cards, and memory can be plugged back in, but insurance can’t replace lost data.

Figure 6 Seismic Isolation Platforms



Cisco IT installed seismic isolation platforms in the San Jose building 12 data center at a cost of nearly \$1.5 million. The platform contains two parabolic plates with a large ball bearing between them. The hosts or frames are fastened to the upper seismic plate with nylon straps. In an earthquake, this allows the upper portion of the platform to remain relatively stationary while the lower portion and ground move side to side. Extra slack in cabling prevents disconnection during all but the largest tremors. The platform limits equipment damage from an 8.3 earthquake to little or no damage.

### Temperature Sensing System

“Hosts are sensitive to heat and must be kept cool,” says Dick Corso. Cisco IT is concerned about temperature at the frame or host and recently placed temperature sensors in a grid-like pattern in many of the racks and frames in each data center. These sensors are connected to the IP-based console network, allowing them to be monitored remotely.

If the temperature at any sensor exceeds a threshold, an alarm is sent to the OCC. If all the sensors are reading high temperatures in an area, the problem is probably with the air conditioning system. If only one sensor is high, it indicates an overheating problem with a single piece of equipment or a problem with airflow, which could lead to a disabled resource. This network of sensors has been credited with eliminating two or three temperature-related system problems a year.

## Power Distribution

“Our need for power drops has been increasing, putting a strain on our power distribution network,” says Ian Reddy. In the past, hosts and frames took up an entire rack and required one or two power drops. Today, these large hosts are increasingly being replaced with many smaller hosts that still require one or two power drops each. In addition, these new hosts have redundant power supplies, adding to the number of power drops needed and, in some cases, requiring separate isolated power drops to the same device.

In the newer section of the San Jose building 12 data center, Cisco IT deployed three power distribution unit (PDU) cabinets, and ran drops from each of these three PDUs to three circuit breaker distribution cabinets in each row. The physical circuits were then run under the floor to each frame, supplying ample connections for power drops and separate power sources for power redundancy where required.

## Power Backup

“Running a data center requires a great deal of electrical power, and we have to plan for outages,” says Corso. The San Jose building 12 data center receives electricity from the local San Jose power grid through a single drop. There is no redundancy; therefore the data center must provide a backup power source.

An uninterruptible power supply (UPS) system and dual backup generators provide continuous power to the data center in the event of a power failure. During normal operation, power flows from the power grid through the UPS system, providing the data center with filtered power. If power from the grid is lost, battery power from the UPS system will support the entire data center, Build room, and OCC without interruption for up to 20 minutes, if necessary. Cisco maintains three UPS systems, but only two are needed to support the full design load of the data center, providing N+1 redundancy.

As soon as grid power is lost, two backup diesel generators begin to spin-up to full power, which takes approximately 20 seconds. When they are running and fully synchronized, generator power is sent through the UPS system. This power also recharges the UPS batteries. One generator is sufficient to supply the load for the entire data center, but a second generator ensures that a mechanical failure in one generator will not affect service. When grid power is restored, Cisco IT waits for assurance and confirmation by the utility that the likelihood of further outages has subsided, at which point the data center is manually switched back to grid power.

The transition from grid power to UPS to generator is so seamless and automatic, it can be difficult to determine whether the power supply is grid, UPS, or generator. To remedy this, Cisco IT installed two lights in the data center. A red light indicates the data center is on UPS power, and a blue light indicates the facility is on generator. Because the lights are not within sight of the OCC, an IP closed-circuit camera was set up to monitor the lights. The video output of the camera is viewable at a Website that can be monitored by the OCC team. Similar lights and cameras are set up at the other data centers.

Figure 7 State Indicator Lights for UPS and Backup Generators



## Conclusion

“Standardization and reliability have gone a long way in this organization,” says Dick Corso. “We’ve standardized and become much more reliable in the way the OCC team is managed, and the way the DCIT team is managed. In addition, we’ve standardized and become much more reliable in the way the network is configured, with backups and remote monitoring and management; and all those changes put together create a robust environment that everybody depends on daily. It’s like a utility, and everyone expects it to be up and running every hour of every day. And if something goes wrong, then we fall back to redundant locations, redundant power, or a redundant network, and no one on the outside notices that anything has gone wrong. So there’s a success story here, and it goes a lot further than just the OCC team. This is not just a success story of operations; it’s a success story of Cisco IT and how Cisco IT has come together to build a data center solution.”

For additional Cisco IT best practices, visit  
**Cisco on Cisco: Inside Cisco IT**

[www.cisco.com/go/ciscoit](http://www.cisco.com/go/ciscoit)



**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](http://www.cisco.com/go/offices).

 CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aronnet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCOIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, FastStep, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0809R)  
(© 2008 Cisco Systems, Inc. All rights reserved.)