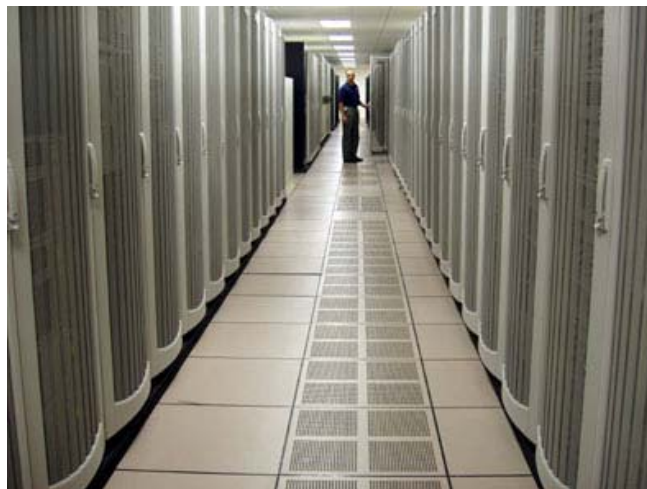


# Cisco IT Data Center and Operations Control Center Tour



## There and Back Again



# Cisco Data Center Tour

## INTRODUCTION

What follows is a guided tour of the Cisco Systems main production data center, located in San Jose, California. This entire document is 71 pages long, with 45 photographs that help bring an experience of the Data Center tour to reader. This tour is based on a series of interviews with Cisco IT data center operations managers Dick Corso and Ian Reddy.

Customers visiting Cisco usually request to visit the main production data center, and this tour remains one of the most popular, year after year. The data center is still one of the most impressive areas to visit on the Cisco San Jose campus.

Typically, to take this tour would require visiting San Jose and making an appointment with the Executive Briefing Center to schedule Dick or Ian to show you some portion of the data center. By reading this set of documents (or reading this document) you can experience a “virtual data center tour.” Click the links on the left to take the tour from start to finish, or in any order of your choice. Links to printable PDFs of this tour are available at the end of each section, and a link to the entire document is available at the end of the tour.

This description of the Cisco Data Center environment and management practices provides a good background into the inner workings of a global data center. It describes the servers, storage and network found in the Cisco production data center; but more importantly it shows:

- How Cisco IT staffs, monitors, and performs change management;
- How the data center is designed to remain available despite network or power outages, and
- How the data center guards against damage from fire and earthquake.

The tour consists of the following nine sections. Select where you want to start and enjoy.

## Contents

[Data Center and Operations Command Center Background](#)  
[Technology in the OCC: Telephony, Monitoring, and Backup](#)  
[In the OCC: Staff, Process, and Ongoing Process Development](#)  
[Root Cause Analysis and Change Management](#)  
[Inside the Build Room](#)  
[Data Center Storage and Servers](#)  
[Data Center Power](#)  
[Overheating, Fire, and Earthquake Protection](#)  
[Conclusion](#)

## BACKGROUND

### Data Center and Operations Command Center Background

**Figure 1.** Dick and Ian at Entrance to the OCC and Data Center



**Dick:** “My name is Dick Corso. I’m the senior manager of the IT Data Center global operations group. My overall team is responsible for the health of Cisco data centers and server rooms, more than 40 in all, worldwide.”

**Ian:** “My name is Ian Reddy. I manage global operations at Cisco. My teams are responsible for incident management, supporting-infrastructure problem management, and for managing the batch processing environment across the many production and engineering data centers worldwide.”

## Cisco Data Centers

**Figure 2. Dick Corso in Operations Command Center (OCC)**



**Dick:** “Today we’re going to take a tour of the IT Operations Command Center and the San Jose, California, main production data center. This data center is one of five production data centers that Cisco maintains worldwide.

“This San Jose data center houses all the intranet systems, the enterprise resource planning (ERP) systems like financials, and all the other internal applications and databases that our employees use.

“In addition to this main data center, there is also a second production data center on the San Jose campus. This second production data center, about a mile and a half from the first, houses the Cisco Website, Cisco.com, which is everything that our customers see over the Internet. Those are our two primary business production data centers. In North Carolina there is a third data center that we use primarily for disaster recovery of these two data centers and also for application development, testing, and staging environments for the production applications back in San Jose.

“In Amsterdam there is a fourth production, or business, data center that houses systems and databases to support local needs, or houses data that must be hosted in the Europe,

Middle East, and Africa (EMEA) region for tax reasons or other financial reasons . In Sydney Australia there is a small but growing business data center for the same reasons, for Asia and the Pacific region (Asia-Pacific). So, those five data centers support the core business processes of Cisco Systems. This is where we do most of the corporate business processing.

“In addition, we support another 40 or so data centers or server rooms that are of varying sizes. Some could be up to 20 thousand feet or more of data center space, but most are smaller. These data centers are predominantly focused on the development environment—the business of engineering Cisco products, whether it be Cisco IOS Software or new releases of a product.

“These data centers are scattered through 11 countries and 10 time zones. Most of these engineering data centers come about because Cisco acquires a company for its engineering talent, and then maintains its data center. When the acquisition took place, we left those engineering data center sites where they were.”

## San Jose Operations Command Center

**Figure 3.** Ian in the OCC



**Ian:** “The key point is that all that management and administration for all those data center locations is done from this IT operations center. Whether it’s development or

production or the business process environment, we have responsibility for all that as an IT organization. So, this operations command center is the heart of a global data center.

“We’re mainly concerned with tracking and responding to high-priority issues: priority 1 (P1) and priority 2 (P2) systems in our 5 business data centers and 40+ engineering data centers. Yet despite these data centers being all over the globe, we are a single Global Operations team, in the sense that we have one set of processes, and one global set of teams that administers those processes for production operations and is responsible for monitoring and maintaining availability of these systems worldwide. The Global Operations teams all report to Dick Corso, who reports to Lance Perry, the vice president of infrastructure.

“The incident management team working here recovers any down or degraded systems or services worldwide, and was staffed out of here 24 hours a day, seven days a week, three people on a shift with 12-hour shifts, 6 a.m. to 6 p.m., and 6 p.m. to 6 a.m. Pacific Time. Until recently, this location was the only location for incident management for our global data center system. In early February, 2004, we took our night shift out of San Jose and relocated that job to a similar command center in Bangalore, India. Now, their day shift, which is our night shift, operates from India.”

**Figure 4. San Jose OCC**



## Bangalore OCC

**Dick:** “So now we have two command centers, one in San Jose and a second command center in Bangalore, India. We just completed the out-tasking to Bangalore. I call it out-tasking instead of outsourcing because I’m still responsible for it. We do a 12-hour shift here in San Jose, 6 a.m. to 6 p.m. Pacific Time. Then at 6 p.m., the operations center at the Bangalore site takes over immediately, because we’ve got the CallManager set up to switch over at that time.

“It’s a very productive situation for us. In fact, if we were to come here three years ago and attempt to out-task our operations center, we probably wouldn’t have been able to do it successfully. Today we are able to do it purely for two reasons. One is that the technology is in place; but more fundamentally it’s because we manage the processes so consistently that people are able to rely upon what we do with a high degree of certainty.”

*Q: And that’s transparent whether it is here or in Bangalore?*

**Dick:** “If you called the data center operations number you couldn’t tell who is handling your call. We’ve got nine people stationed here in San Jose, and nine people stationed in Bangalore India, and it has been very successful so far, although it took a lot of work to get us there.”

*Q: What kind of issues did you have to deal with in opening a second OCC?*

**Ian:** “There were a few infrastructure issues that we worked through, like making sure there was redundancy available within the Bangalore LAN, even through to the desktop switch level. We had to make sure that we provided the same failover capabilities that we have here in San Jose.

“For instance, in this OCC, which is active 24 hours a day, we have a backup OCC in a nearby building, a second command center, which is not normally staffed. If there is a fire alarm in this building, our team can go to the other building and as quickly as we can drive there, we can resume operations. We didn’t have that in Bangalore, so in the past four weeks we set up a second command center in India, a failover center, on the Bangalore campus.”

## Physical Environment of the OCC

**Figure 5.** The San Jose OCC from the Observation Deck



***Q:** A lot of people say this looks like the bridge of the “Starship Enterprise.” I see four banks of six monitors - 24 in all, with four big monitors. There’s also an unusual shiny stainless steel ceiling with a large number of different lights, and what looks like a movie theatre screen in the back. What’s this all about?*

**Ian:** “Well, this is no accident, the command center is meant to look like the bridge of the Starship Enterprise. It is the core of operations for our team. If something important is affecting the business, we’re going to know about it in here.

“Also, it is meant to be a pleasant facility for tour groups. We constructed the back balcony specifically for Executive Briefing Center (EBC) tours. But it’s also designed to spark our visitors’ imaginations, to get them to ask questions, to think about what’s possible and not just what they do today, and get a dialog going. So our data center tour is intended to be something a little different.”

**Figure 6. Ceiling Lighting in the OCC**



**Ian:** “Let me talk about the lighting first. I don’t know if you’ve noticed but it’s been constantly changing. There are a lot of fluorescent and incandescent lights—the halogen lights are different colors. These two sets of lights vary in their relative levels, and in the relative color, very slowly over time. This continual change helps keep people alert and awake without being obvious and distracting. When you’re on shift at 3 o’clock in the morning, these subtle changes help keep you awake

“The monitor desks are meant to be comfortable and flexible. You can change the heights of the benches; they are adjustable to each person’s height. The IP phones have helped because we can move them and plug them in anywhere there’s a network connection. We have flexibility with the laptops, plenty of screens, and the whole environment is intended to help make the workspace both comfortable and productive for the command center team.”

**Figure 7. OCC Staff at Work**

*Q: Why are there 24 monitors but only three people on staff right now?*

**Ian:** “The OCC was built for the worse-case scenario. The worse-case scenario would be a major infrastructure failure that would impact Cisco’s business. In that case we would need more than three people.”

*Q: Has a worse-case scenario ever happened?*

**Ian:** “It has happened, and unfortunately, I’m sure from time to time it will happen again. We’ve been surprised by things like nasty attacks from the Internet, and natural disasters that we can’t really do much about but we can plan for. Part of our plan was to always have enough capacity in the OCC for all the extra people we might need, plus a few extra spaces for manager coordination that might be necessary. During major crises we would use two separate bridges—we would have a technical bridge and a management bridge.

“And if there were extended incidents that lasted beyond a single shift, we would start a rotation of leads to keep the incident response process going for as long as we needed. There have been a few times when we’ve ended up with six or eight people in this room, coordinating as many as 20 to 30 or more people on bridges: 15 to 20 engineers on the technical bridge with another 10 to 15 people on the management bridge. The OCC room is built for scalability.”

**End**

**Data Center and Operations Command Center Background**

You can go back to the beginning of this tour, or move to the next section to learn about how Cisco uses technology in the data center to support telephony, to monitor more than 10,000 network resources, and to provide enough levels of backup to keep the data center running every minute of the year without fail. Or you can go to any other part of the tour.

## 2. Technology in the OCC: Telephony, Monitoring, and Backup

### Voice over IP

*Q: Can you tell me a little bit about the technology that allows us to out-task that to India?*

**Figure 8. Dick at an IP Phone in the OCC**

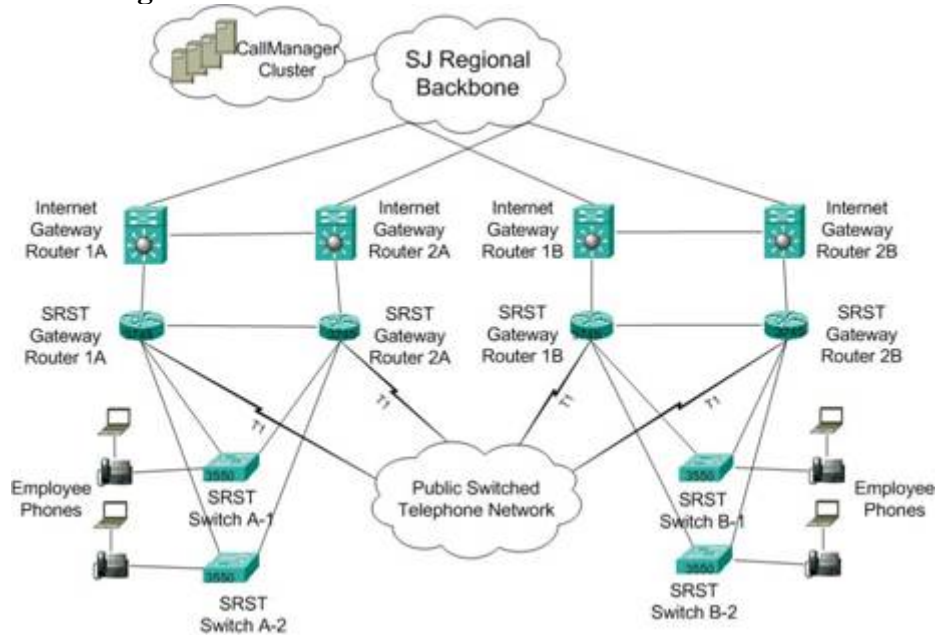


**Dick:** “Well, certainly Cisco technology is in play here at the network level and at the voice level. One thing that we’re using is Cisco voice over IP, and because of that the same phone number rings anywhere in the world. We can have it ring in San Jose, we can have it ring in Bangalore, or we can have it ring in both simultaneously. We can also have it ring in our nearby backup command center, if we have to evacuate this building.”

“One of the other things we also have in place here is a special Survivable Remote Site Telephony (SRST) architecture to protect the phone service in case of a severe network failure. We wanted the additional safety capability in place to back up the CallManager cluster that provides call processing to all the phones on campus.

“We were concerned that if there was a failure in the voice network, we might not be able to support the repair process because we would be unable to communicate, unless there was backup. We were never able to have a backup for our voice PBX pair. SRST creates that backup, by using a pair of local Cisco 3745 routers here in the data center that will perform CallManager functions in an emergency.”

**Figure 9. Diagram of SRST in the Data Center**



**Ian:** “Our phone call processing normally goes through to the CallManager super cluster, which normally handles all the calls for the San Jose campus. If, for some reason, our phones are unable to reach the super cluster, they register directly to the nearby SRST routers, which handle a significant subset of call management capabilities and allow our phones to continue to take calls. So the rest of the campus can be without phone service and we can still take calls.

“We also have direct drops from phone-service providers for the phone numbers we expect people to call. We have this extra redundancy in our call system, something we didn’t have with our previous third-party call system. If you think about it, all other systems depend on the OCC doing its job, mostly over the phones, and that makes the phone system in the OCC one of the most critical IT systems in Cisco. That’s why we put in this SRST solution. And it works.”

**Dick:** “We are one of only a few groups on the LAN using SRST, and now we’re starting to implement it in India.”

**Q:** *Have you ever needed to use your backup SRST system?*

**Ian:** “No, we’ve never *had* to use it; but we do use it pretty frequently anyway.

“Whenever we know that the phone system is going to have a scheduled change, like on the weekend, we test the SRST failover process. We ask the network team to block our connection to the CallManagers using a new line item on the data center gateway access control list (ACL), and our phones move to using the SRST routers completely transparently. There are no lights flashing or interruptions at all. And when they’re done with the scheduled change, they take the ACL block off and the phones reregister back to the CallManager cluster. The OCC never sees an interruption or anything that would cause it to pause for even a minute.”

## OCC Phone Procedures

**Figure 10.** Ian Reddy on an OCC Phone



**Dick:** “The phone system we use here is not like a typical call center where call routing occurs and a call is sent to the first available agent. Here, all the phones ring at the same time and the first available agent picks it up on the first ring, because by three rings it’ll roll to an alternate phone number with an alternate bank of people so that an individual should never get rolled into voice mail here. And if they do reach voice mail, they know they’ve got a problem because the voice mail actually says that.”

**Ian:** “When the phone rings in the OCC we know it’s about a high priority issue, so there’s always a race to the phone, and our goal is pick it up before the second ring. Even

if you're busy, even if there are other calls, our policy is that someone from the team picks it up and acknowledges receipt of the call, even if we have to put somebody else on hold. That helps to get people coordinated during a trouble event.”

## Monitoring Tools

**Figure 11.** Monitoring Data on OCC Screens



**Dick:** “We use a lot of tools, and most of them are parts of an internally developed suite of management tools, called Enterprise Management, or EMAN. It grew with Cisco. It’s got many different components such as DNS management, paging, and telephone service provisioning. The part we are using up on the screen is called ‘The EMAN Enterprise Monitoring Tool.’

“After our engineers identify the equipment or applications that should be monitored and give it a priority, EMAN begins testing. It can test anything in the environment as long as it can either be pinged or has an agent on it. For instance, an agent sits on the host and the agent responds back to the query from the EMAN tool.

“In the application space we’re doing a synthetic transaction. These synthetic Web transactions are nothing more than a URL that initiates a dummy setup transaction, which

could even be querying the database to see if that part of the application is working as well.

“The EMAN tool tests four times in a row, and if any one of those four tests were to fail, EMAN would start to show a degraded service. If all four were to fail, EMAN would show it as zero percent availability.

“We’ve got somewhere in the neighborhood of 30,000 resources EMAN monitors, including applications, databases, network devices such as routers and switches, and the CallManagers in Cisco. All are monitored inside the EMAN tool, and about half the issues turn out to be priority 1 or priority 2. The operations command center focuses only on priority 1 and priority 2 issues—those are important business-affecting issues that we need to support with an immediate response.

“EMAN has about 15 collectors that are at different sites worldwide. There are two in San Jose, and four more in the United States. There are three in Europe, and six in the Asia Pacific region. At each of these locations we have an EMAN rack of servers, doing testing in the local environment.

“Meanwhile, the IT support team responsible for supporting the application, network device, or host is aware that they must respond within 10 minutes of any problem event; otherwise, escalations will occur. This means that our Operations Command Center staff needs to page them within five minutes. This requirement is on 24 hours a day, 7 days a week. There is no grace period for P1s. For P2s the model is a business hours only model, because P2s are not considered business critical. Although we immediately page people, we don’t expect them to work outside of business hours to get P2s fixed.

“We monitor all the data centers all over the world from this Operations Command Center. We group the world into five primary areas in different time zones. One area is the Americas; they get monitored 5 a.m. through 6 p.m. Pacific Time. We start at 5 a.m. so we can catch the east coast at 8 a.m. We’re a little bit late for the South America group, but generally we’ve got all the Americas in one area.

“Europe is another area. Australia is another. In the Asia-Pacific region we’ve got at least two data centers. Because we monitor all P1s and P2s, and a P2 is treated like a P1 during business hours, we try to keep track of local business hours. If we see something fail, it gets treated like a P1, because it’s got business impact during the day – theoretically.”

*Q: I noticed there are some other tools you’re using here besides EMAN. What are these other tools I see up on the screens in front, and what are they used for?*

**Ian:** “We use other vendor tools as well, mostly for managing our server environment. One of the tools we use receives alarms that come out of the batch processing environment. We run on the order of about one and a half million batch job launches per month, about five million per quarter. All those batch jobs can generate alarms. A job abort, an error, or when a job misses a launch window or a completion window will

generate an alarm. When those alarms come to the OCC, our technicians can open the alarm to see meta information about the job; what the priority is; who the support pager alias is; what the impact on other systems of this job failing is; and they page out and they expect, again, a near-instant response from the support team for that failure.

*Q: What do you mean by a “page alias”?*

**Ian:** “When we identify a problem we don’t page a specific person, but instead we page the group of people responsible for taking care of that resource. One or a few of those people are responsible for responding to that page, day or night, weekdays or weekends. Often a team will rotate the duty so that only one person is on call during holidays. We call that person the “duty page”. And we in the OCC don’t have to know who has been selected to respond at any given time. We just page out to the entire group, the “page alias” and they determine who is responsible for responding.”

**Figure 12. Ian in Front of a P1/P2 Outage Screen**



**Ian:** “We’re continually tracking Priority 1, down or degraded resources: All the hosts, applications, middleware, databases, switches, gateways, routers, LocalDirectors, distributed directors, cache engines, and so on that make up the network infrastructure.

“There are about 30,000 monitored resources in the monitoring system, about 10,000 of them are Priority 1 and Priority 2. We monitor them continually, every hour of every day, by sending a ping through the network to that resource, or by sending a string to an application that initiates a synthetic transaction. This way we can tell, in two minutes or less, if any resource has become unresponsive.

“Anything that we can send a ping to through the network, and any application we can talk to using a short transaction string can be monitored in this way, and we monitor most of them. As soon as we see something of P1 or P2 priority that hits zero percent availability we open a case, with no exceptions.

“We only take care of P1 or P2s, everything else is handled by the internal help desk. The OCC tracks the most important problems. We are not a help desk, or a call center; we handle the emergency response process for P1 and P2 issues. One of the screens at the front of the room shows all the open P1 and P2 issues, the ones being handled by the technical response teams right now. When a high priority resource hits zero percent availability, we open the case, and then we click the resource, which shows us which technical team is responsible for that resource, and we page them immediately.”

## Backup in the OCC

*Q: This appears to be an extremely critical system. How do you make sure that you are always available to respond in a crisis, especially when the systems you use to function might be the very systems that are having problems?*

**Ian:** “There’s a lot of redundancy built into the OCC. We have another backup OCC on the San Jose campus, but within this location there’s a lot of redundancy as well. For example, this command center is on the same, very reliable set of power systems as the data center, and we’re on a separate network from the desktop networks that support the rest of the employees’ PCs and phones in this building. Our network is physical, separate, and secure. Physical entrance to the data centers is also controlled; we have different badge groupings for access.”

**Figure 13.** OCC Staff with Laptops



**Dick:** “You’ll notice that in the OCC everybody has a laptop. If we encounter a failure here—it hasn’t happened in the three years I’ve been here but if we did—staff can take their laptops and work down the street where we have a backup data center OCC.

“One of the things that made it easy to have a backup OCC was IP telephony. A staff member could pick up one of those phones in the backup data center, register it on the Cisco network, and be ready to go. And if there was a general failure throughout the San Jose campus, they could pick up their laptop and go home and work from there, over the Internet. And then there’s Bangalore.

“Bangalore has the same sort of situation going on there too, with redundant OCCs and IP telephony and so on. In addition, along with saving money, it gives Cisco IT the opportunity to manage using a “follow the sun” model, which takes the pressure off our team here. In the past we had people rotating from day shift to night shift and back again to day shift, and it was really difficult for them. Some were doing that for years.”

**End**

### **Technology in the OCC: Telephony, Monitoring, and Backup**

You can go back to the Data Center Overview, move ahead to learn about the problem resolution process that the Operations Command Center engineers follow to immediately respond to all high-priority alarms and issues, or you can go to any other part of the tour.

### 3. Process in the OCC: Staff, Process, and Ongoing Process Development

#### OCC Staff

Figure 14. OCC Staff on the Bridge



**Dick:** “Now we’re inside the gallery behind the operations center. In this environment we’ve got two or three people on shift at a time. During night shifts, we can typically manage with two people, but depending on the day of the week, we may have three. We generally look at it as a three-person model. Everybody on the team is cross-trained.

“The responsibility of the operations command center personnel is to ensure that when something fails, a case is immediately opened and within five minutes they send out a notice, telling people about the situation. They don’t ask questions—that’s critical to managing the OCC—they just open the case as fast as possible.

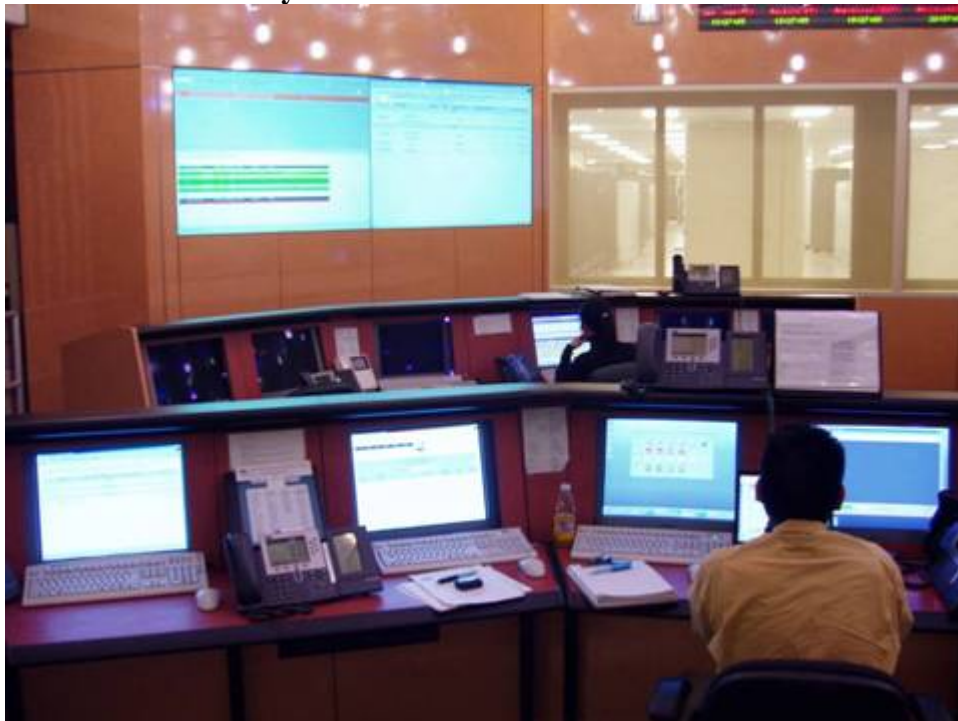
“When they open a case on a failed resource, a notice is automatically sent to all the people who are associated with that resource, so they can begin to take steps to fix the

problem as quickly as possible. It's not our job to identify these people; instead, people who are responsible for that resource, or who are interested in finding out about the health of that resource, subscribe to e-mail aliases that we use to alert them via pager. That way the OCC staff can identify the Cisco employees interested in that particular resource.

“Our OCC staff manages the case in our trouble-ticketing tool, from the time the alarm is raised until the time the immediate problem is solved. They require the on-call support engineers to phone, to get on the bridge, and not leave the bridge until after the problem is resolved or they've negotiated with the OCC staff as to when they're going to come back. That means that the support engineers can leave the bridge, but they have to tell our staff when they're coming back, and if they leave prematurely, our OCC people are going to call them right back until they get back on the bridge.

“If the on-call support engineers for the down resource don't respond within five minutes, our staff will escalate to the first tier – usually that person's manager.. The OCC staff will try the on-call duty support pager first, then the next thing they do is try to reach the on-call person's mobile phone. If they can't reach the duty engineer by pager or phone, they will escalate to that person's manager by paging or calling the manager. If that doesn't work, they page or call the director, and after the director then the VP, however high up they need to go to get somebody to respond to the outage situation. Also, when the OCC has to go to the VP level, they call me in and together we send pages to a couple of strategic people – the people in IT who can make things happen -- and that will solve the problem pretty quickly.”

**Figure 15. The OCC Day Staff**



*Q: How do you get by with only three people on staff to handle all these resources?*

**Ian:** “That’s been a real victory for our process, and our automation tools. Four years ago there were upwards of 20 people handling 400 or 500 incidents per year. Now we have this down to a team of 14—with 3 people per shift; 24-hour coverage seven days a week; covering nights and weekends; it works out to about 14 people. What’s amazing is that in that time we’ve gone from about 500 incidents per year to about 9000 incidents per year, with a reduced number of staff.”

*Q: Why did the number of incidents grow so much?*

**Ian:** “Part of the increase in incidents came when we went from monitoring just the five global production data centers to monitoring all 40 plus data centers; that is, when we started monitoring and doing incident management for the engineering data centers and server rooms as well. The rest of the increase took place because we started getting much more stringent on reporting and recording every single incident that took place.”

*Q: So what other kinds of things do they do in the OCC?*

**Dick:** “They manage nightly tape backups, month-end processing, and quarter-end financials.”

*Q: What is month-end processing?*

**Dick:** “Month-end processing is a large set of batch jobs that need to be run, in parallel, to close the books at the end of the month. To do that we need to stop and sum up the total revenue coming from our sales applications, and the total costs coming out of our manufacturing partner applications. We have to stop these processes long enough to take a snapshot of the financial flow within Cisco. This whole enterprise resource planning process runs on an Oracle database, which Cisco IT is migrating to Oracle 11i. In fact, our manufacturing, sales, finance, and human resources applications all run on the Oracle database platform.

“The OCC team coordinates with a product scheduling team in my group that works very closely with the month-end processing teams to ensure that we get our quarter-end financial reports run on time. At this point we’ve got the month-end processing to the point that it’s predictable and consistent, and the OCC team almost always handles it themselves.”

*Q: What types of people do you hire to handle all these different activities?*

**Dick:** “We’re looking for people who can work with people, and who can talk professionally just as well when they’re sitting around a table as when they’re on the bridge in the middle of the night, working with people who are screaming because they

just woke up to respond to a dozen pages and their baby is crying in the background and their manager is on the line yelling at them.

“We hire the OCC staff to be able to manage problem situations, to be calm in a crisis, and handle little problems or disasters by the book. I think we’ve been very successful in hiring the right people over the years.”

## OCC Process: Coordination, Communication, and Documentation

**Figure 16.** Ian with OCC Staff



**Ian:** “The goal of the command center is to communicate, coordinate, and document during incidents. Our team doesn’t provide technical resolution; technical response is provided by one or more members of about 150 teams worldwide, who have P1 and P2 responsibilities for applications, systems, databases, and infrastructure such as switches and routers, for which their team is responsible.”

*Q: That’s pretty catchy: Communication, Coordination, and Documentation. Could you describe that process for us?*

### Communication

**Ian:** “Communication is letting the right business or support groups know about the existence of a down or degraded resource. When a resource goes down, the first thing that happens is our team sees it on the monitor in front of them, and in front of the room. It starts with paging the person on duty responsible for supporting that resource, within 5

minutes of detecting a down or degraded service, and we expect a return phone call to the OCC within 5 minutes of paging out, no matter what the time or day.

“If we don’t get the expected response, we start our escalation process. That’s really aggressive, and requires that our team and the duty support engineers are very responsive. We ask a lot of them. And if they don’t respond, we escalate to their manager, and then their manager’s manager, to make sure we get the right engineering resources working on the problem as soon as possible.”

## Coordination

**Ian:** “Coordination is more complex. Some failures may affect several applications or several resources at once, because so much of what is on our network is dependant on something that’s down or degraded, so we may have several duty support engineers working on a problem together from a variety of angles.

“Our team will coordinate the overall response for multiple groups. We bring them onto a phone bridge together. For example, maybe we need a database administrator, a network person, or a system administrator, all together very quickly to look at the problem to determine what really is causing the incident. We have three MeetingPlace bridges reserved specifically for this team 24 hours a day that we use, as necessary, to get people talking together.

“Our goal is to get all the duty support responders necessary to identify and resolve the problem, and to keep them talking, so they can keep the resolution process moving forward. One of the skills on this team is knowing when the engineers are working productively and when they’re not. Sometimes things get quiet on the bridge, and it’s up to us to know the difference between when things are quiet because everybody knows what the problem is and they’re working madly to fix it, or they’re quiet because nobody knows what the problem is, and nobody wants to admit it. So, one of their skills is to ask questions, like “Why has nobody sent an update?” or “Can you give me an update?” or “Did you just mention you found the problem?” or just ask gentle questions to get people talking and moving along, to find out whether we’re progressing or not.

“It’s important for people on our team to know when to prompt the support engineers for the next step. We train them to ask gentle questions, like:

- “Do we need to bring in additional resources?”
- “Has anybody let their management know about this?”
- “Have you told the business clients about this?”
- “Can we page out for that person you just talked about, the one who might know something more about this?”

“A lot of their communication skills are people skills. This team is hired for communication skills, not technical skills. Of course it helps to have a technical bent, but the technical response we expect to come from the data support groups.”

## Documentation

**Ian:** “Everything that happens during an incident, from what we call a short term fix and all the way to a full recovery, is captured and documented by this team in real time. This keeps other technical resources and management aware of what’s being done to fix the problem, and helps the support engineers because it offloads the documentation and outbound communication from them and lets them concentrate on fixing the problem. We enter all this information as the problem resolution unfolds into an Alliance case.

“Alliance is a trouble-tracking application that we have customized for our use. For example, we added an extra tab called the Outage tab, which is specifically for capturing what resources went down, when they came back online, and what the impact areas were to the business: CEC, Cisco.com, manufacturing, ERP, and so on.. We also record which support engineers are on the bridge, how, why, and when the bridge is set up, who responded, any important decisions that were made, and any actions taken.

“Anything that’s not captured as a data value, we try to capture as a comment in the activity log. When we view the case later, we want to be able to go through the combination of the case data and the activity log to recover and piece together the sequence of events that show issue through to resolution.”

## Ongoing Process Development

### Process Redefinition

**Figure 17.** Dick Corso in the OCC



**Dick:** “I came to Cisco from Lockheed Martin. I think I was hired because I have a very strong process and methodology background in data center operations. The very first day I arrived, in 2000, I noticed that sometimes there would be no alarms at all, and other times there would be a lot of alarms, and it seemed to depend on who was on shift. The problem I saw really was during the times when there were no alarms, which sounds odd.

“But what was happening was part of the culture then; people helped each other. And if an engineer screwed up during a change and some resource got pulled offline that wasn’t scheduled, the people in the OCC would turn off the alarm and work with them to get it back online, rather than have a lot of people paged to try to fix it. So engineers got used to extra cooperation from the OCC, and they weren’t as motivated to use the change management process as scrupulously as they should.

“Problem tickets weren’t being created, availability was inflated, and people weren’t motivated to fix the procedural problems as long as no one was noticing it, or measuring it. In fact, at that time people were being rewarded for the reduced number of trouble tickets being created. It was seen as a sign that there were fewer problems, which was rewarded.

“Another issue was that people in the OCC weren’t always at their posts. I started to show up at different times, like in the middle of the night, and sometimes there would be nobody here. What happened was that they had gotten to know pretty well what the normal change and work schedules were, and they knew when things were likely to fail and when things were likely to be smooth. So if there was something critical going on they’d be right here, but if things were quiet they might be off having a smoke, or out to dinner, chatting, or in the closet sleeping. This also resulted in fewer trouble tickets being created, because sometimes people weren’t there to open the ticket.

“So we went through period of change when I got here. After communicating to the team how important it is to follow procedure, and how critical it is to the company to maintain control over the whole change management process, we selected a day to start out with our new process. We all know it in this group as “holding the line day,” sort of a military maneuver from my military days and from government contracting. From that day on, as soon as any resource became unavailable, for any reason, we created a problem ticket. On that day we went from almost no P1s per day to about 8 P1s per shift. We’d never seen more than 10 P1s in a day.

“People were really concerned, because a lot of bonuses in Cisco IT are tied to their resources being available, and meeting availability targets. There were a lot of managers who were unpleasantly surprised, because they’d been told that their systems were highly available and now they found out that this wasn’t true, and their bonuses might be at risk. This was all kind of a shock to people in IT.

“But after the initial shock wore off, people started understanding that Operations had become much more rigid, and much more predictable and reliable. After a while people no longer questioned it and it became part of our culture. It has resulted in P1 alarms returning to being pretty rare, and our availability statistics are back up to being very high, and we know that now it really means something. In fact, because we now track every single outage very carefully, and engineers focus on long-term root-cause analysis of problems and long-term fixes for those problems, our availability in many areas has hit all-time highs.

“My management style is a little more aggressive than most, and so I spent the first two years building relationships with people on my team and the support teams. My team knows that, in the middle of the night, any day of the week, if they need to get hold of me, they can, and they do. They could have support engineers or managers here on the bridge yelling about something that they did. And they can count on me to get on that bridge and take care of the problem, right away.”

**Ian:** “Another way to look at our process redefinition is to see it as our team focusing on our real core mission, and taking things that we used to do, which were not strictly incident management, and moving them out of the command center. Over the years some things had crept into our process that really didn’t belong there. For example, we used to help coordinate change requests: When someone would request a change on one part of the infrastructure, we would look up all the other parts of the infrastructure that would be affected, and contact all the other teams that were responsible for those areas to make sure that the proposed change wouldn’t affect them, or help schedule it at a time to minimize impact.

“But we decided that this was not incident management, and that the team requesting a change needs to coordinate its change request. This has not only reduced our workload but helped engineering teams to communicate with and understand all the other systems that their system affects, and all the other teams who work on them.

“Our team also used to spend time helping engineering teams through their changes through the night, or over the weekend. Well, that’s inefficient when our team is trying to jump from incident management to coordinating a change request and back, and we sometimes would end up with a conflict like, “I’ve got this P1 incidence I need to deal with, but this change request is also important, and I have to handle both at once,” which reduced our ability to manage incidents and keep our availability up. So we got our teams to stop all work that is not strictly incident management, which makes us more responsive during an incident, and allows us to do all this with as few resources as possible.

## Process Automation

**Figure 18.** Ian in the OCC



*Q: What did you automate to make it possible for fewer people to handle more than 10 times the number of incidents?*

**Ian:** “We made a lot of changes. Part of our success came from adopting the Alliance Remedy trouble-tracking tool and adapting it to our needs. We took some of the capabilities in the previous tools we had that worked well, and we integrated them with the Remedy case-management system to make the actual process or procedure more efficient for us. We also built boiler plate incident templates to help reduce the amount of time it took to record an incident.

“And that’s what gave us the ability to take on managing incidents for the entire network and all the data centers, both production and engineering. This makes sense, because we have the monitoring systems, we have well-trained support teams, and we do this well.

“It’s far more efficient for a single team to monitor and document, to capture the information succinctly going into the case, figure out who to page for support response, capture all the values and variables and the issues and responses, and that sort of thing. It helps drive down costs to consolidate the various means by which information can come to this team so that it’s consistent. More, because we have a single standard method for

how we respond to incidents and capture the information, and a standard language we use with all the engineering teams throughout IT, it becomes more familiar and easier to use for everyone in IT.

“There are things we can’t automate, though. Even though we try to find ways to simplify the procedure, to automate wherever possible, we want to make sure we don’t lose the value that we have with this team, because the great advantage of having humans over automation is that we’re able to see the big picture and think creatively for new and unexpected situations. Now, 99 + percent of the situations that we have are pretty boilerplate; but the critical ones can be very different. So we build our procedures to be consistent, we have predictable procedures for the type of incidents that repeat most often, but we don’t try to nail every last detail to the wall. That way when something unusual comes up, people still have the latitude to manage those exceptional situations.”

## Process Documentation

*Q: Are these procedures documented or are they picked up by your team over time?*

**Ian:** “They are documented. The documentation sometimes has to go through several changes until we get it right. We used to have separate procedures for different technologies, and for different environments, but found that this made our work too complex and made it hard to scale.

“Usually when we get new business capabilities and technologies that might affect our procedures, we first ask “How does this affect our current incident management process?” If we can, we try to adapt our current procedures rather than create new ones, because changing a procedure is difficult and time consuming and leads to a few initial failures and errors as people learn a new procedure. Because of that we try to make sure all our procedures are as independent as possible of any specific technical or functional area, since we know the technology will change over time.

“We also try to make our procedures independent of the applications being supported. Whether Cisco.com, CEC, or manufacturing ERP, we try as much as possible to make sure that our procedures are addressing all those areas consistently. That was one area of simplification that allowed us to really scale a lot. We went from a larger team with about 1700 cases in fiscal year 2000 to a smaller team with 8600 cases in fiscal year 2003. Simplifying our procedures helped make that happen.

“The next step for us was to engage in out-tasking, and to move to a two-location model. After we established and documented our processes in detail, we handed off responsibility for this incident management workflow to Cisco partners. We’ve tuned our processes to the point where they’re consistent, reliable, and capable, and when you can do that you’ve got something to outsource.

“You can give it to Cisco partners because Cisco is not in the business of doing incident management. We want to use our employees for our core business. We’re continually looking to the next levels of complexity, and when we have those support processes well

understood and well documented, we'll hand those off too. Moving our night shift to Bangalore India and using a two-location model for support was part of this process.”

**End**

### **In the OCC: Staff, Process, and Ongoing Process Development**

You can go back to the Technology in the OCC: Telephony, Monitoring, and Backup section, move ahead to learn about how long term solutions and other changes within the data center and network are carefully managed to keep availability high, or you can go to any other part of the tour.

## 4. Root Cause Analysis and Change Management

### Root Cause Analysis

**Figure 19. Ian Reviewing Updates**



**Ian:** “The incident management process that we’re in charge of focuses only on the short term fix: How did we get the system operational again and back in a state where it is returned to the client base or customer base that normally uses the service.

“The problem-management process includes root cause analysis and a long-term fix after the service is recovered. We start that process by assigning the case to one of the duty support responders whose job it is to shepherd it through the long-term fix process. Often, the person who responds during the incident and manages the short-term fix is also the person who is responsible for analyzing what went wrong and determining how to make sure it doesn’t happen again. But if not, they work with other support groups to figure out who really does need to do more analysis.

“Our team starts but doesn’t coordinate the long-term solution. When their short-term fix is done, they assign the problem-management case, and then they’re on to the next issue. It’s up to the support teams independently to do the root cause analysis, propose a long-term fix, and document it in the Alliance trouble case.

“The support teams have five business days to complete and document their analysis. The Alliance tool automatically starts a timer, and then starts telling the case assignee who’s been assigned to work on the long term fix, “You have five business days,” “You have three business days,” or “You have one more business day to do this root cause analysis

and long term fix proposal.” We have reporting that shows a few cases that have gone past that limit and when they do, a notification is sent to IT management to let them know that these cases are still outstanding and need to be addressed.

“The goal of all this is to reduce the number of problems that recur, to eliminate the problems we can eliminate. Sometimes you run into a problem that you just can’t fix, often because the solution is just too expensive in comparison to the severity of the problem. For example, it might be too expensive to have a completely redundant server cluster for an application that you can, on rare occasions, do without. Sometimes you may have to access data or reports through another means, or you may be able to afford to wait a day because it’s some kind of historical reporting capability. For another example, sometimes it just may not be possible to provide backup to a cluster or resource – the technology is just not there to do it -- and you live without it until the technology finally does become available”

## Change Management

**Figure 20. Dick Reviewing Equipment Changes in the Build Room**



**Dick:** “Change management is critical to our team and to the rest of Cisco IT. Change is a constant process in Cisco; we normally handle about 80 requests per day. One of the monitors in front of the room shows us all the change requests that are presently pending. Managing change very carefully is critical to maintaining a highly available network. Even with the best of controls, a lot of our problems come from changes.

“We actually have metrics that show correlations, strong correlations, between the number of changes and the number of resource failures in the network or data center. We

have “change freezes” at month end and at quarter end, because we’re doing critical financial analysis then, where we stop everybody from making any changes or upgrades except for the most rigorous and necessary things that need to get done. During those freeze periods we get an immediate reduction in problems.

“EMAN also supports our change management tool, which is integrated with the EMAN monitoring process. What happens is that during a change window resources will be taken offline and will then register as “unavailable” in the EMAN monitoring tool. But during a change management window the monitoring tool won’t alert the people responsible for fixing it, because it’s taking place as part of an authorized change.

“To get a change scheduled into the change management tool, the person doing the change first has to submit a change request through the change management tool. It pushes the requestor to go through a series of risk and effect questions, and asks them to list all the resources that will be made unavailable because of their change request. The engineer’s answers to these questions determines who has to approve the change. People whose resources will be affected have a chance to ask the change to be deferred or rescheduled. And the greater the risk, the higher level approval is needed. Service affecting change may require the engineer’s director to approve it, for example.

“Now we know that it’s very easy to work around the system by underestimating or ignoring some risks involved in the change request; but the key is that Cisco works on a trust system. It’s part of our culture to trust our employees to make the right decisions for the company. In addition, if the change ends up breaking something that wasn’t listed as a potential risk, then the engineer making that change is exposed to some serious repercussions.”

*Q: How do IT managers give their approval for proposed changes?*

**Dick:** “The EMAN tool has a place for managers to log in, sort of an automated approval tool that stores all approval requests for managers, and they can review all change requests that need their approval and respond there. They may need to talk offline with the requesting engineer, but usually there’s enough information in the form for them to make an informed decision.

“After the change request is approved, it stays in the tool for the scheduled change time and date. Then when the change window starts, the engineer starts to work and the device or devices go down. The monitoring tool records this downtime but doesn’t send alerts out to the support teams, although our OCC sees these resources as unavailable. We see down resources in red on the screen at the front of the room, but if it’s in an approved change request window, it will appear in blue.

“Although the monitoring tool records all outages within the change management window, it keeps two sets of availability statistics: Total availability and total availability not including scheduled changes. Our IT teams are motivated to meet availability targets

for the network or data center resources they're responsible for, but they use the availability statistics that don't include scheduled outages.

“If a resource is still unavailable when the change window ends, within one minute the availability monitor will catch it because it's pinging every 15 seconds. Applications get “pinged” every 30 seconds or so, but that differs depending on the application. Most of them will show “down” after two minutes. At that point alarms go off, and pages go out. The same thing will happen if someone begins a change that's not covered by a change management window, or that affects a resource not listed in the change request. This gives people a strong motivation to use change management procedures and to keep changes within the window, which is the change management philosophy here.”

*Q: I see a couple of people back there in the data center. What are they doing?*

**Figure 21. View of the Data Center from the OCC Window**



**Ian:** “They are on an approved change request or else they shouldn't be in there. They are backup technicians with constant access and they're changing tapes on the storage tape drives. If you're in there to make a change to the environment you need an approved change request, and your badge will be activated when you contact this team and they enter your badge number in the badge system. By default, almost nobody other than the backup team, workplace resources, and security and the emergency response teams would have long-term access to those primary business data centers. So everybody else should be in there only because of an approved change.

**End**

## **Root Cause Analysis and Change Management**

You can go back to the In the OCC: Staff, Process, and Ongoing Process Development section, move ahead to learn how IT stages new equipment and about the physical characteristics of the Build room and data center architecture in general, or you can go to any other part of the tour.

## 5. Inside the Build Room

### Introduction

**Figure 22.** Inside the Build Room



**Ian:** “The purpose of the Build room is for the system vendors to rack, stack, and configure new systems before they go into production, to try new equipment and new configurations and burn in new equipment without affecting our production environment or setting off alarms. I should be able to turn off the power to this Build room and we should see no alarms at all.

**Dick:** “The Build room also gives engineers a safe space to set up, configure, and test the boxes that will be going into the production environment. They get the boxes delivered here from the shipping and receiving truck, open them, put them in this room, do any assembly or configuration required, and then burn them in for whatever period of time makes sense to them and their applications. For example, we might want to take a critical storage frame or server and burn it in for a few weeks, whereas smaller servers might only require a few days. And then when the engineers are ready, they will place them in the data center. There is one Build room in each of the data centers.

“There is a separate subnet in the Build room so there are no problems leaking from this network into the production network. You deal with the problems in here, so you don’t have to deal with them in production.”

## Build Room Architecture

**Dick:** “I think you’ll notice that in the Build room we do our networking using a different architecture than we use in the business process areas. The Build room is very much like our engineering data centers, and I think we are probably going to end up that way in production environments.

*Q: How is the Build room architecture different from production? How is it more like engineering?*

**Ian:** “The engineering data centers are a little different from the production data centers. Engineering data centers are built for flexibility because engineering is a very dynamic environment. We want to make sure that when our engineers get a great idea, that in the space of six weeks or six months they can build a new project area in the data center, complete the first customer ship, tear it down and rebuild the systems differently to do a different set of compiles for bills, project stores, and so on. So they have thousands of small systems changing rapidly.

“Business data centers on the other hand tend to have a smaller number of larger systems, primarily supported by vendors that change infrequently. Production systems tend to go into production and then stay there for two or three years until they get replaced by the next version of the application.”

**Dick:** “Generally what you’ve got in this Build room environment is a rack of network equipment at the end of every half-row. In the production environment we keep the network environment all the way back out one end of the data center to protect it. It’s far enough away from the rest of the equipment that no one working on the servers will bump into it or touch it. The only way you’re going to see the network is if you lift the floor tiles to see the cables underneath. That architecture adds protection, but at the cost of reducing flexibility, which is necessary in the Build room.

“In here, in the Build room, you’re changing out equipment every week, and you need to build for flexibility. We know that when we plug in a box that in a few days we’ll unplug the whole thing, move it into this data center or another data center on this campus, and then plug it into another network. Nothing is permanent in here. So all our network connections are really close to your equipment, and you don’t have to run a lot of cable to connect it; it’s all right here.

“In a production data center we build the network all the way out at the end and then run cables all the way back to the data center equipment, so we end up with a lot of long cables. Adding new equipment or moving equipment means we have to pull long runs of new cable, which is difficult, but in production data centers we don’t change things very often. Everything in the data center is pretty well documented, and also pretty

predictable, so we know where everything is. In fact, I should be able to walk over and pick up any floor tile and know exactly what I'm going to find there.”

**Figure 23. Cisco Catalyst 6500 Series Switch and Cisco 3600 Series Multiservice Platform in Network Cabinet in a Half-Row**



**Ian:** “We use Cisco 6500 Series switches everywhere, in every one of the business data centers, and every one of the engineering data centers, and in fact in all the data facilities whether they are on a desktop or in a data center. By standardizing on a single platform we make the infrastructure more stable, and far more predictable and easier to maintain.

“We also have a couple of CCIE experts on our LAN team who have come up with a very stable system – a very scalable configuration for our Catalyst 6500s. It’s also a flexible platform that allows you a several choices in media type: Copper, single-mode or multimode fiber to accommodate the needs of a row in a Build room or data center. It’s so stable it’s like our floor tiles—you don’t need to think about it.

## Console Network

**Figure 24. Console Network Routers**



**Dick:** “Along with the data center network, we also support a separate console network here. In some data areas they have direct console connectivity, a monitor, and keyboard in various sections to allow people to log directly in to hosts or switches.

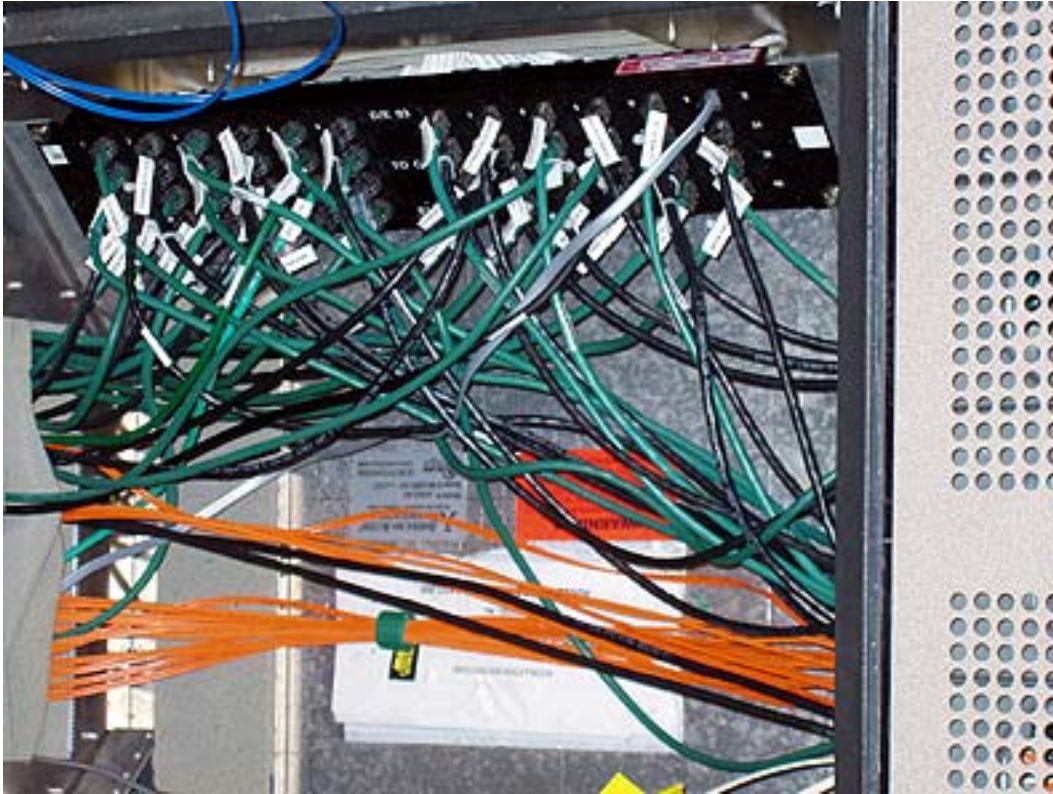
“You won’t see any monitors or keyboards here inside the data centers. Instead, all our console ports are connected into a separate and secure console network. This allows our network engineers and host engineers to work where they’re most needed, and without having to come into the data center they can network into the console ports and manage these resources from anywhere on the network.”

**Ian:** “Also, by putting all our console ports on the network we don’t have all the keyboards and monitors in our data centers. Our floor space is too expensive to be filling it with keyboards and monitors, and the like. We concentrate all the console server access over the network that way; and so that it’s easy for our engineers to access the right host or router or switch, we use consistent standards for the host names and router names that tell you where it is and what type of resource it is. It’s a naming standard that’s scalable in terms of nomenclature as well the subnet allocations and DNS as well.

**Dick:** “This is all set up to help a distributed environment, which really helped us with the move to Bangalore as the second Operations Center, because we’re set up to access everything remotely, and that means we can manage it from anywhere in the world.”

## Cabling

**Figure 25. Under Floor Cables with Breakout Boxes**



**Ian:** “The cabling system is standard as well. If we look under the floor, we’ll see breakout boxes. We see a box that is clearly labeled with the port numbers, and there is room for 12 and 24 fibers behind each floor tile. That allows us to drop a patch cable to the breakout box and then go over to the zonal cabinet, which is clearly labeled with which row and which breakout box and which port it is. When you plug that in to the switch, you’re done. You don’t have to pull up a whole series of floor tiles or cables under the floor.

“In fact, it’s so standard and consistent that, you can go to any Cisco data center in the world and use the same system, connect equipment in exactly the same way. I’ve been in Glasgow, Milan, Texas, Research Triangle Park (RTP) in North Carolina as well in San Jose, and they are all the same.

“The standardization keeps training costs down and keeps error rates down. It also helps our acquisition strategy. When we acquire a company for engineering talent, you want to keep all those people equal, you want to keep them productive and stable and the way to do that is to erase all the irrelevant differences, like how we access data center resources. “When we get SEC approval for an acquisition, our teams can go there that weekend and cut them over to the standard data center and network IT environment. When they come in on Monday, and they start working at Cisco, it’s all the same to them, except that now we can support them a lot more easily and with fewer people, because we don’t have to train on new standards. We’re able to do that kind of SWAT team approach because we have a standard architecture to work with. So the network is consistent, the racks, the

shelves, the screws, power bars, the power cabling, patch cabling, the supplies against the wall are all the same worldwide.”

## Production Data Center Architecture

**Figure 26. Network Rack at End of Half-Rows**



**Ian:** “You won’t see this same architecture or standardization in this business data center, however. In this data center, instead of a network rack at the end of each half-row, we use the production network standard: A single rack of network equipment at the end of the data center. There are two reasons for that: First, our production data centers are a bit older and their design predated the standardization effort here in Cisco. Also, business systems tend to go in and stay in for a long period of time, so you can afford a higher level of defense and a higher level of effort to put them in place because you’re not going to have to change them several times over three years. If we ever redo the production data centers or build a new one, we would build it like this, with these zonal cabinets.

### **End Inside the Build Room**

You can go back to the Root Cause Analysis and Change Management section, move ahead to see how storage and servers are kept and managed, or you can go to any other part of the tour.

## 6. Data Center Storage and Servers

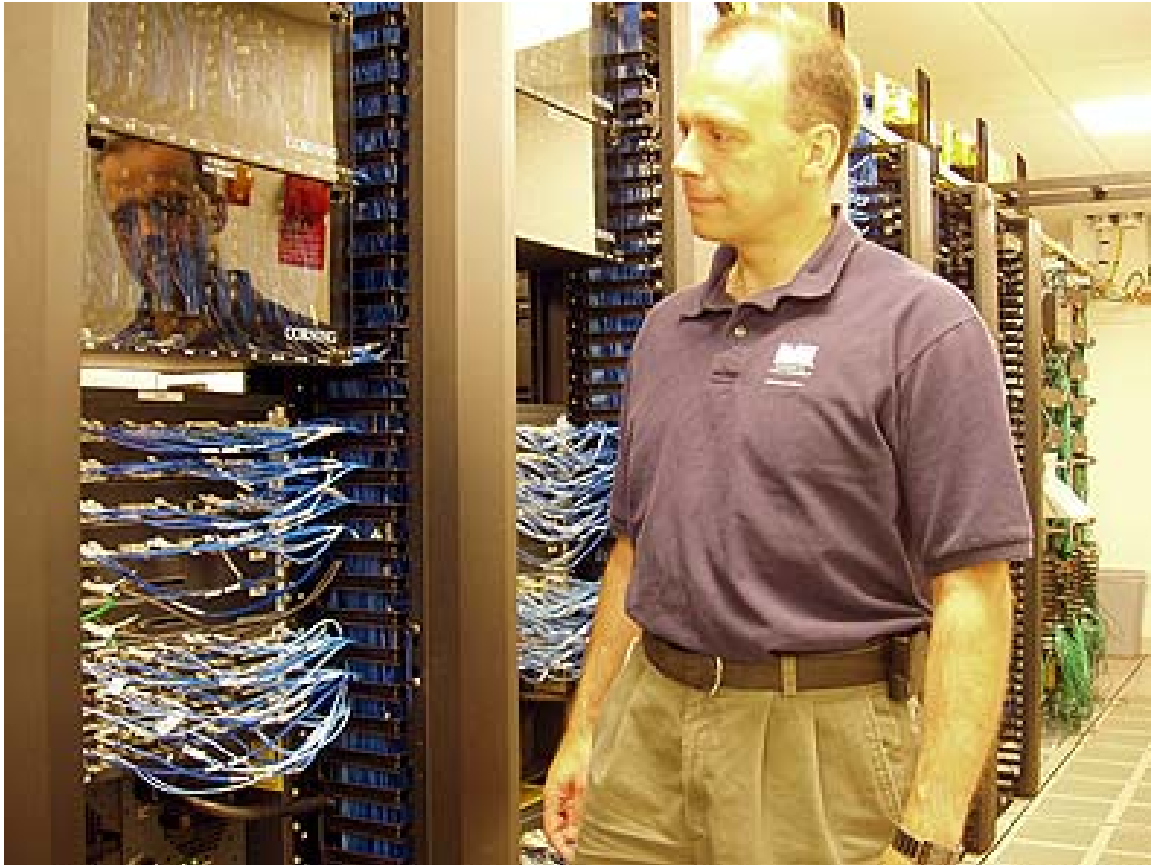
### Storage

#### Storage Area Networks

Figure 27. Storage Switches in the Data Center



**Dick:** “This data center is a little bit about everything. We have a lot of storage. Most of that storage is EMC, and most of the rest is HP. In this data center, and in the other production data centers around the world, we connect hundreds of hosts to these storage frames over a storage area network (SAN). This SAN is made up of Cisco MDS multilayer switches. There’s a great success story about this SAN. It has enabled us to fully utilize our storage resources. We already have about two Petabytes within Cisco – that’s more than two quadrillion bytes of data. Two years ago almost all our storage was directly connected to each host. We might get two or three different hosts connected to the same frame, and we had almost half of our storage unutilized. In our SAN environment our storage utilization is a lot higher. When you consider that an EMC frame might cost up to \$750,000, and we have a couple hundred frames, that’s a lot of money saved.”

**Figure 28. Ian with Fibers Connecting Storage Switches**

**Ian:** “These Cisco MDS 9509 storage switches have a lot of ports; they can have more than 200 each. Already they are almost all used. There are not many empty ports on these switches. And if you look around the corner, you’ll see why.

“We have a lot of storage in this data center, about 600 terabytes of storage in this room of the data center, and about 800 terabytes of storage in the whole data center. All these storage frames are connected to a storage area network using these switches, connecting our hundreds of production hosts to a large pool of shared storage. This helps keep our storage utilization pretty high, and saves money.

“All the blue cables you see here interconnect our storage frames into a storage area network using Cisco MDS multilayer director switches. The orange cables are the regular fiber that we used for data networking when we installed the data center about five years ago. This cable was pulled maybe a year and a half or two years ago. We don’t often have to pull new cable in production data centers, unlike in the Build room or the engineering data centers, which is why we still keep the network cabinets at one end of the data center. Otherwise we’d probably have migrated to the engineering data center architecture by now, with network equipment at the end of each half-rack.”

## Tape Backup Storage

Figure 29. Tape Storage Library



**Dick:** “We have a lot of tape storage for vital records, but we have backup storage offsite in the North Carolina data center. Its primary purpose is to act as a hot standby backup site. That data center was developed to support the critical systems here in duplicate on the other side of the United States, to replicate them and run if we encountered a failure here. The ERP environment updates the data to RTP on a continuous basis throughout the day and when we need it to recover the data, it takes about 20 minutes, which is time lost.

“In reality, the backup solution isn’t as automated as we want it to be because we still rely on several people to get it set up, and there are many things we haven’t been able to test adequately. We’re still improving our disaster recovery procedures and we still have some work to do.”

## Servers

**Figure 30.** Rows of Servers in the Data Center



**Ian:** “The interesting thing about the production or business data centers is the variety of solutions and partners that are represented here. The equipment in our business data centers is in large part supported directly by vendors under contract with us. Those vendors will come in, perform upgrades and changes to the systems, and troubleshoot and repair if there’s a problem. You’ll also see those systems in their cabinets, in their native habitats, instead of in standard engineering racks, because the support contracts specify that everything is left in its vendor state of packaging.”

**Dick:** “We have a lot of different servers in distributed environments, mostly smaller Linux and Windows servers that we can stack and pool together. We’ve got some enormous SUN E-10000 servers with 28 processors each and some Sun HP superdomes, which are big, heavy, and expensive servers.

## Remote Monitoring of Storage and Servers

**Figure 31. Modem access to monitored resources**



**Dick:** “A lot of the storage frames here have small modem boxes next to them. That way if any of these storage frames has a problem, it automatically calls back to the vendor’s home office, and tells the vendor we’re having a problem. The vendor can dial in and investigate, and then they alert operations about the situation.

“It’s good to have this level of support, but there have been problems. One day I got a rather big phone bill—for 10,000 calls in a month—all of them from this data center in San Jose and all of them from these storage frames. They were calling directly out of our regular number. I went to the storage provider to ask if they could do something about this and they got their own phone number. Now all these calls are billed to them.

“Analog modems will be a thing of the past very soon. We’re getting ready to go to a VPN solution over our IP network and our connection to the Internet, which will give a vendor direct access to those boxes, but to nowhere else in our environment.”

## CallManager Servers

**Figure 32. CallManager Cluster**



**Ian:** “Cisco has 54 buildings in San Jose, and hundreds of large buildings worldwide. In 2001 each building had a PBX. In San Jose each building had a large PBX, called an Extended Peripheral Node, with a pair of Primary Peripheral Node PBXs to direct them.

“When we first started replacing these PBXs, we replaced each one with a pair of Cisco CallManagers, and we ended up with hundreds of CallManagers worldwide. Recently we began migrating these CallManagers to a centralized call processing architecture, with a small number of CallManager clusters handling call processing for numerous locations in a region. When we finished consolidating the 50 buildings in San Jose, we ended up with a cluster of eight CallManagers, called a super cluster.

“The super cluster is backed up by a second super cluster in another data center, which isn’t doing any call processing but is ready to if the first one becomes unavailable. All the phones are registered to this cluster, but are set to automatically reregister to the backup super cluster if needed. What’s amazing to many people is how we can replace 50 large PBXs, each larger than a refrigerator, with a quarter of a rack of equipment. The savings in space, power, and management time is impressive.”

**Dick:** “You know, when I started at Cisco there were big telephone switches, one per building. We dedicated a room for telephony with that big box sitting in it, heating up the room for you. And two years ago we eliminated all those telephone PBXs in all those buildings. We replaced it all with our super cluster, which is six small servers inside of a single rack, maybe 1/3 of the rack. The super cluster supports telephony throughout the 50 campuses now, with more than 34,000 IP phones. So it’s pretty amazing to bring a customer in and to show how many people we’re managing with that little cluster of processors.”

**End**

### **Data Center Storage and Servers**

You can go back to Inside the Build Room, move ahead to learn about how data center components are powered and cabled, or you can go to any other part of the tour.

## 7. Data Center Power

### Electrical Power and Power Protection

**Figure 33.** Power Cabinets



**Dick:** “Running a data center takes a lot of electricity, and we have to worry about and plan for power outages. We have UPS batteries in all our data centers, and generator backup in all our major data centers. At first we just had them for production data centers, but we started to realize that engineering data centers can be just as critical to Cisco as business data centers.”

**Ian:** “The business data center gets a single electrical power drop from the local San Jose power grid. There’s no redundancy there, we don’t get two power drops; which leaves it up to us to provide good power backup. First, the power runs through an uninterruptible power supply (UPS) system so our systems in the data center are always running on filtered power. More importantly, if we lose power our system doesn’t lose a beat, since it’s running on the UPS all the time anyway. We have 3 UPS battery main systems downstairs in this building, part of our “N-plus-1” design, since we only need two UPS battery systems to support the full design load of the data center, command center and build room. The two UPS systems can support the full design load for about 15-20 minutes.

“During that time, two equal diesel generators behind the building, kept in separate bunkers with separate fuel supplies, spin up and then synchronize their power frequency. It takes about 15 or 20 seconds for the two generators spin up and synchronize, and once they have, then the power from both generators is transferred into the UPS system in the building. Either generator could supply enough power for the data center, but we run on both generators; that way, in case one generator has a mechanical failure, the other one is already running and could easily take up the rest of the load. So they share the load. Meanwhile they two generators are recharging the UPS battery banks from the generator as well. Now, when the power comes back on we don’t automatically transfer that back to the public power grid; instead, we wait until we’re satisfied by the utility. We call the power utility and wait until they assure us that the power is on for good, and that there’ll be no more power outages or testing. At that point we decide it’s all clear then we’ll manually switch the power back to the grid power.”

*Q: Have we ever gone to diesel generator backup?*

Ian: “Yes, we have. During the rolling blackouts in California in 2001, there were frequent power outages without much warning; so we learned to know proactively. When we did have warning – when the blackout was scheduled for one of our data centers, we would switch to our generators in advance. We get alerted when this happens, since we have a controller system that pages the plant’s team and lets us know that power is lost in a location, and that the generator is up to speed, and that power is transferred over to the generator.

Dick: “You’ll notice that we’ve got lights – one to tell us whether or not we are on batteries, and the other to tell us whether or not we are on generator power. A couple of years ago we had rolling blackouts in California, and we encountered a little problem that, theoretically, shouldn’t have happened. We had a blackout and we went automatically onto battery backup, then switched onto generator power and everything went smoothly. When the power came back on and our data center started up, it automatically came off the generators and went back to the UPS -- and got a ground fault. One of our two UPS backup battery systems, which isn’t in use normally, had been wired badly, and the protection circuits took us right back off the backup power and immediately everything in the data center lost power. We lost a few machines because of that. We didn’t lose any Cisco gear, but it took us awhile for us to get [www.cisco.com](http://www.cisco.com) back on the air, and that means millions of dollars in revenue lost or at least delayed.”

**Figure 34. Red and Blue Generator lights**

**Ian:** “We had a major power problem in another data center, which we traced to an error with the power controller system. We had a power outage, and went to generator power. About 15 minutes after the system reported that we were on generator, all our data center systems failed. It turned out that the generators had not been on at all, and the data center had really been on backup battery power until it was exhausted.

“Since then we’ve installed red and blue lights in all the data centers, directly connected to the circuitry for the generator and for UPS. The red light tells us when we’re using UPS, and the blue light tells us when we’re on the generator.”

**Dick:** “We learned some expensive lessons that day. We learned to hold our vendors a little more accountable to their standards. We worked with our Workplace Resources organization a lot more closely in the days following that event, to make sure the grounding everywhere is entirely up to standard.

**Ian:** “Now, we can look at the light to see when we’re using UPS. But we only have staff on two or three sites on a 24-hour basis, so we can’t be there to see what the light is telling us. So we’ve installed IP Web cams pointing at the lights, and our command center team can go online and look at the lights at any data center to see what’s happening. That costs a few thousand dollars per location, and does a whole lot of good.”

## Power Distribution

**Figure 35. Power Distribution Cabinets**



**Ian:** “Power distribution is important, and we’ve learned some lessons over time. The power distribution in the newer side of the building 12 data center is different from that in the older side. In the older side we used our standard practice of running power cables under the floor to power distribution units – they look like large circuit-breaker boxes – and then directly to the system racks.

“These power distribution units (PDUs) are more than circuit breakers though, they also condition the power like a large surge suppressor, to make sure that there are no spikes or power variations coming from individual systems. As we kept adding new units requiring new power, it strained our power distribution system. So in the new side of the data center we took more of the floor space and created multiple power zones. We take large power runs from three different PDUs down in these cabinets, with each circuit marked by identifying numbers, and then run the physical circuits under the floor to each frame.”

**Dick:** “This new power distribution architecture makes sure that power drops are spread throughout the room, rather than in one or a few locations. When we add a new box we plug it in just under the floor to cables connecting to one or more of the nearby power cabinets. We have three power cabinets for each row. It takes up more room, but we really need it. And because much of equipment requires dual power sources, we make sure that we plug the backup power supply into a completely separate cabinet. We don’t

plug directly into the cabinet, but into cabled power outlets under the floor. They're clearly labeled so that we know what circuit each one is connected to."

**Ian:** "This new power distribution system allowed us address two problems. One problem was the need for more power drops in less space. We've started migrating from larger servers to smaller servers; now we're getting servers in smaller form factors—in 1-rack-unit systems, or in larger units with 42 server blades in a rack, so power density needs have increased. The second problem is that more systems seem to have redundant power supplies, duplex power supplies for some servers, or N+1 power supplies for some multiserver systems. This increased the need for more power drops, and also required us to provide separate isolated power drops to the same server.

"What's the point of having backup power sources to the same server if they are all plugged into the same power bar? So now we have at least two power sources from two separate PDUs to each system, so if we get a circuit failure or a PDU failure, the system's redundant power will still support it."

## Under the Floor

### Cabling Standards

**Figure 36.** Cabling Under the Floor



**Dick:** "When I lift the floor tiles you can see the network. In this environment we have the network connections cabled out to one side, unlike the more distributed network in the Build room. It's still a somewhat distributed network approach, except that all the network connections are distributed by plugging them into labeled jacks underneath the floor.

“On the minus side you have to plan very carefully in advance and you have to bring enough cable drops under the floor to meet all your future requirements for network connections. On the plus side you don’t have to pull cable from the racks all the way to the back to the data center distribution frames on the side of the room. So that means that we have our network connections all underneath these floor tiles and it’s not all over the room.”

**Ian:** “The cabling under the floor has gone from complex to kind of boring, which is just the way we like it. We’ve standardized the cabling at different levels under the floor. The network cabling tray will be up on raised trays closest to the top. Power will be down on the floor so there is vertical separation from the network cabling. In addition, network cabling will go down one row of tiles and power is pulled down another row, so there’s more separation. That way if you’re adding a new run of network cabling or power cables by pulling the cables under the tile, you don’t end up pulling on or snagging other cables.

### Power Grounding Grid

**Figure 37.** Close View of Power Grounding Grid



**Dick:** “There’s a signal reference grid here, this copper grounding grid. It is a 2-foot by 2-foot grid, and the cable which is maybe  $\frac{1}{4}$  inch or  $\frac{1}{2}$  inch in diameter throughout this entire data center. We did that because a vendor was having a signal reference problem on the floor and telling us that the subfloor is a discontinuous entity and it’s not a very good place to ground. So we built this grounding grid. Unfortunately, it didn’t fix the problems we were having. That vendor’s equipment is still having problems. We got a very good grounding system out of it though.

“Also you’ll notice a shine on the concrete floor underneath. Over time the concrete slab will degrade and get dusty because it’s got lime in it, so we sealed all the floors with a nice lacquer finish.”

**End**

### **Data Center Power**

You can go back to the Data Center Storage and Servers section, move ahead to learn how the IT data center is protected against heat, fire, and earthquakes, or you can go to any other part of the tour.

## 8. Overheating, Fire, and Earthquake Protection

### Temperature Control

**Dick:** “Another thing you get concerned about running a data center is the temperature inside the data center. Hosts are sensitive to heat, and need to be kept cool. But our standard temperature control system in the data center only measured the heat in the room at one place—inside the air conditioning unit, on the intake side. That’s fine, it tells you when it’s hot in the room, but it only lets you know the temperature of the entire mix of air in the room.

“We still monitor that because if the entire room gets up to pretty high temperatures we want to know. If the air conditioner intake area is hot, the whole room is really hot. But it doesn’t let you know if a single host, or a group of hosts, is overheating in one small area of the room. Another option is to use temperature sensors inside the boxes and the CPUs, but that doesn’t tell you about the temperature of the whole environment in each enclosure.”

**Ian:** “We’ve done a lot of work refining our data center temperature sensing network. Our Workplace Resources facilities group – they’re responsible for maintaining the buildings – has always monitored temperature, power, and other environmental measures, but they do it from a “facilities” point of view, from the view of the whole room, the whole floor, and the whole building. IT needed to develop a different strategy about things like temperature because we’re concerned with temperature at the frame and at the host.”

**Figure 38. Temperature Sensors in a Rack**



**Dick:** “Our Data Center IT (DCIT) team came up with a nifty concept, which is ‘let’s test the environment where the equipment is, not from just one place.’ So we put temperature sensors inside some cases, near the top, plug them into the network, and monitor them periodically. That allows us to monitor temperatures at remote data centers around the world from one location. We set a range for normal temperature, and when the temperature in any case goes outside that range, an alert is sent to us on a Webpage that we monitor, and lets us know that something is wrong so we can investigate. It costs about \$150.00 for each IP-enabled temperature sensor that you can connect into the network to test the entire environment. We’ve put it in 5 to 10 different slots in the data center to give us localized feedback about the temperature.

**Ian:** “When the temperature at any of these units goes past a threshold, an alert is sent to our operations command center team. The team will see the floor plan of the data center and a map of the temperature sensors’ data, updating every five minutes. If all the sensors are high, they know it’s a systemic problem related to the air conditioning in the data center. On the other hand if only one of them is high, it could be a local system overheating or some other local problem with air flow, like a floor tile that was pulled up and not replaced, because cooled air flows under the floor.

“Without the temperature sensor network we would never have known about local overheating until one or more resources in a data center started failing. This has really helped us, because we’ve had instances where the air conditioning systems in remote data centers would start to overheat and sometimes the only thing we’d know was that our systems would start failing. We now coordinate better with Workplace Resources and they with us. That has saved us from having temperature-related system problems about two or three times a year, for the last two or three years.

**Figure 39. Server Racks Facing Each Other**

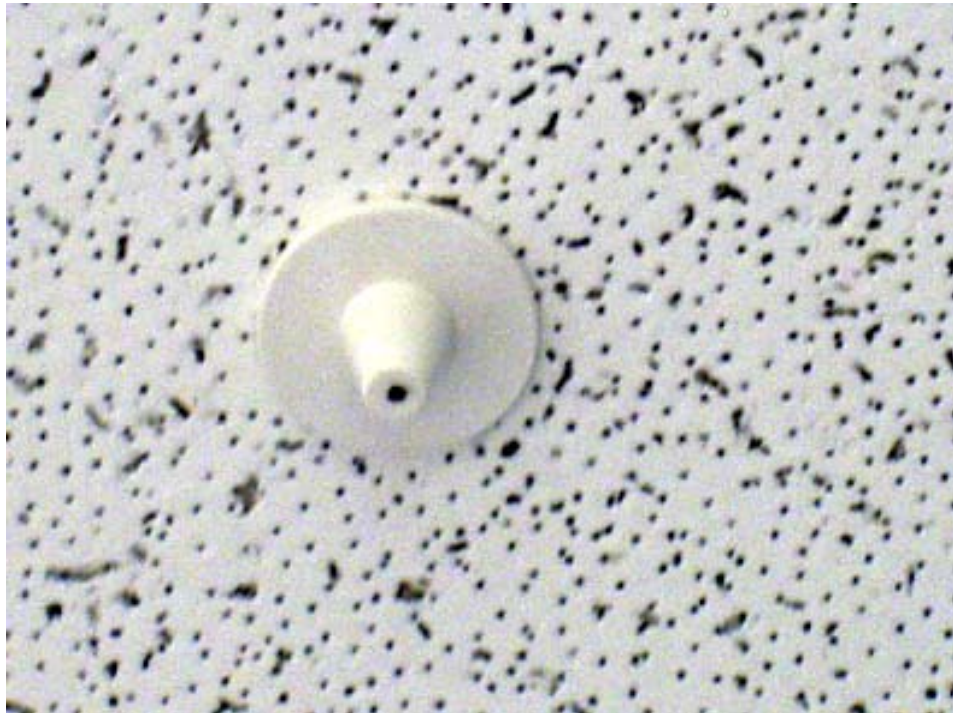


**Ian:** “The server racks face each other in pairs of rows, which helps us control temperature. Cooled air from the air conditioning units is pumped under the floor and comes up through special floor tiles. Servers pull in the cool air from the front, and push it out the back. Here in each row the backs face each other and we immediately duct the warm air up and out.

“Some people have made the mistake of having all their systems face the same way, which results in the first row getting cool air and blowing out warmer air to the back, which the next row takes in and blows even warmer air out the back, until you get a heat gradient from front to back. The air toward the back of the data center is extremely warm, and equipment in the back can fail more quickly. So we face our rows of servers front to front, and back to back, and that way it keeps the temperature relatively even throughout the data center.”

## Fire Suppression

**Figure 40.** Smoke Detector and Air Sensor on a Ceiling Tile



**Dick:** “We have smoke detectors all over the ceiling. Really, they’re not sensing the air for heat at all, they’re sensing the air for a high level of particles that would indicate smoke. We have to be careful in this room because just sweeping the floor can fill the air with particles and cause the smoke detectors to go off.”

**Figure 41. FM200 and Water Nozzles in the Ceiling**



**Dick:** “We have two forms of fire protection: FM200 and water. We have several stages of alarm, and when we get to the stage where smoke is detected, we trigger the FM200.

“FM200 is just a gigantic fire extinguisher, and works a lot like Halon. FM200 primarily absorbs heat from a fire event and secondly chemically interferes with the combustion process. It literally removes heat energy from a fire to the extent that the fire cannot burn any more. People could remain in the room and breathe if the system discharged, but we always advise occupants to leave the space because of the fire condition. We moved from Halon to FM200 because Halon was found by the EPA to deplete the ozone layer, and FM200 doesn’t.

“We also have dry pipes for sprinklers. They don’t have water in them now. When the FM200 gets triggered, these pipes fill with water, but even then you have to have a fire beneath the sprinkler for it to drop water. The only time you’ll see water in the data center is if you get to the point where the FM200 has already gone off, you’ve got water in the pipe, and there’s a hot fire.

“We try to make sure that water is our last resort, we really don’t want to have water in the data center because water will corrode and destroy circuitry in all these machines. We expect that the expensive machines underneath will be entirely destroyed. But if a fire ever gets to that point, we know that the fire protection is to stop or at least slow the fire, to protect the people in the building, which is more important than the investment in the equipment.”

*Q: Has there ever been an FM200 or Halon release that you are aware of?*

**Dick:** “Not in Cisco’s environment. I’ve been in a Halon release once; a lot of data managers could tell you they’ve been in one, or at least seen a Halon or FM200 release. It looks like a whirlwind. It comes up from spouts underneath the floor all at once and with a lot of force. If you think you’ve got a clean data center, it proves you wrong. All the dust balls under the floor are blown all over the room.”

*Q: Do you ever get false alarms?*

**Ian:** “Not to my knowledge. There’s a lot of work to make sure we don’t get accidental discharges of FM200. We’ve found that what’s most important is to keep the dust level down, to prevent accidental smoke alarms going off. These alarms are very sensitive to smoke and to dust.

“One way to keep dust down is by using the Build room. We get all our boxing activities out of the way in the Build room. Unpacking boxes stirs up a lot of cardboard and plastic dust. We also hire a company that comes in twice a year or once a quarter to vacuum under our floor tiles with a HEPA filter. They clean out all the dust; otherwise, you can lift a floor tile and stir up enough dust to set off the smoke alarms.”

**Figure 42. Sticky Dust-Trapping Mats in the Doorway**



**Ian:** “And you’ll see sticky mats that you walk over in the doorway to help take the dust off your feet. There’s also more dust mitigation through the concrete floor. Concrete gets a chalky lime layer after a few years, which is a source of dust, so we’ve sealed the floor and that helps control dust production.”

## Earthquake Protection

**Dick:** “One thing that you’ll notice here on the data center floor is that almost all the boxes are on a moveable platform. We spent about a million and a half dollars on the San Jose campus to focus on seismic isolation.

**Ian:** “We’ve been concerned about the impact of an earthquake on our data center here in San Jose, because this is a seismically active area.”

**Dick:** “In the old days, if we had an earthquake, a big one, the boxes were either tied to the floor, bolted to the floor, or freestanding. Back then they were connected to the electrical system with heavy bussing tags so you didn’t have to worry about them traveling too far but still you had to worry about them tipping over, and about whether the disk storage would be damaged.

“Because of these seismic isolation platforms, we don’t worry about this in production anymore. In the engineering data center environment, they generally stay on racks that are on rollers. But with this moveable frame, they can handle an 8.2 earthquake or 8.3 Richter scale earthquake. In 1989 we had a 7.1, which was big enough. This insurance policy is basically saving us from the kind of havoc that occurs when you get a big earthquake.”

**Ian:** “The earthquakes around here tend to have a horizontal displacement thrust, so the idea is the system stays still and the building moves underneath. It can move about 8 inches in any direction, which should allow us to survive an 8.3 earthquake. These platforms are just pairs of parabolic plates with a single large ball bearing placed between them. The bearing rolls around between the plates, but stays in the parabolic center.”

**Figure 43. Servers on Seismic Isolation Platforms**



**Dick:** “The hosts or frames are held to the seismic plate with these nylon straps when the whole thing is moving. You want to make sure you’ve got enough cable underneath because it’s going to move a few inches in any direction and if you don’t have enough free play in the cable, they’ll get pulled out.”

**Ian:** “The idea is to help prevent the transfer of shock to the electronics. Many people bolt their systems solidly to the walls or on the floor. They’re trying to prevent things from moving, but an earthquake can still transmit a lot of shock to hard drives and other equipment, and can damage or destroy them. We’re trying to allow things to move so that we don’t transfer shock.

“Insurance will replace your sheared cables and you can plug parts and memory back in, but insurance companies cannot replace all the data you’ve lost on your disk drive. Most of our critical systems, Enterprise Resource Planning systems primarily, are being continuously mirrored to our backup data center in RTP. Every five minutes we send chunks of data over the wide area network to hot standby databases in RTP, so our most critical systems should never be more than five minutes away from our last business transaction.

“We have 800 terabytes of information stored in this data center, most of it stored as RAID 0 or RAID 1. This local backup is designed to survive single or dual disk failures. If you lose several disks in an earthquake, if you lose even a single digit percentage in your disk drive, you could end up losing whole volumes of irreplaceable data. We’re playing a game of probabilities here, trying to reduce the number of disks that will need to be recovered from tape. Recovery can take a long time.”

*Q: How long would it take to recover a lot of data from tape?*

**Ian:** “It all depends on how much data is lost. If we lost multiterabyte volumes it could take days to replace, and it would be costly. If we had to replace multiterabyte volumes, we’d have to dedicate multiple teams working simultaneously to coordinate all that recovery. And because we back up to tape less frequently, the data would not be completely up to date, and some data would never be recovered.”

**End**

### **Overheating, Fire, and Earthquake Protection**

You can go back to the Data Center Power section, move ahead to hear Dick and Ian conclude the tour, or you can go to any other part of the tour.

## 9. Conclusion

**Figure 44. Dick Corso in the Data Center**



**Dick:** “The key message is, we changed our management process over time, and learned from our mistakes. We got more diligent. We created more consistency. We were able to give a lot more visibility into problems that had always existed but were not always measured. Because of this consistency and the improvements from increased visibility, we were able to take on more responsibility—all the Cisco data centers. In spite of the increase overall of monitored elements, we have created a trend toward decreased incident volume. And we have been able to standardize our processes so well that we could safely and comfortably outsource our OCC to an external vendor, and to distribute the functions between San Jose and Bangalore.

“Standardization and reliability have gone a long way in this organization. We’ve standardized and become much more reliable in the way the OCC team is managed, and the way the data center IT 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.

“All those things put together create a robust environment that everybody depends on day to day. 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. The success story that I can tell you 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.”

**Figure 45. Dick and Ian in the Data Center**



### **End Conclusion**

We hope you have enjoyed this part of the Cisco IT Data Center tour. You can contact your Cisco sales person to arrange an Executive Briefing Center visit, and request a live tour of the Cisco main production data center and operations control center.

For additional Cisco IT case studies on a variety of business solutions,  
go to Cisco IT @ Work

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

**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.



## Corporate Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS  
(6387)  
Fax: 408 526-4100

## European Headquarters

Cisco Systems International  
BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

## Americas Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

## Asia Pacific Headquarters

Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 317 7777  
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on  
**the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or 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. (0406R)