Cisco IT
Data Center and
Operations Control Center
Tour

Technology in the OCC:

Telephony, Monitoring, and Backup

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?*

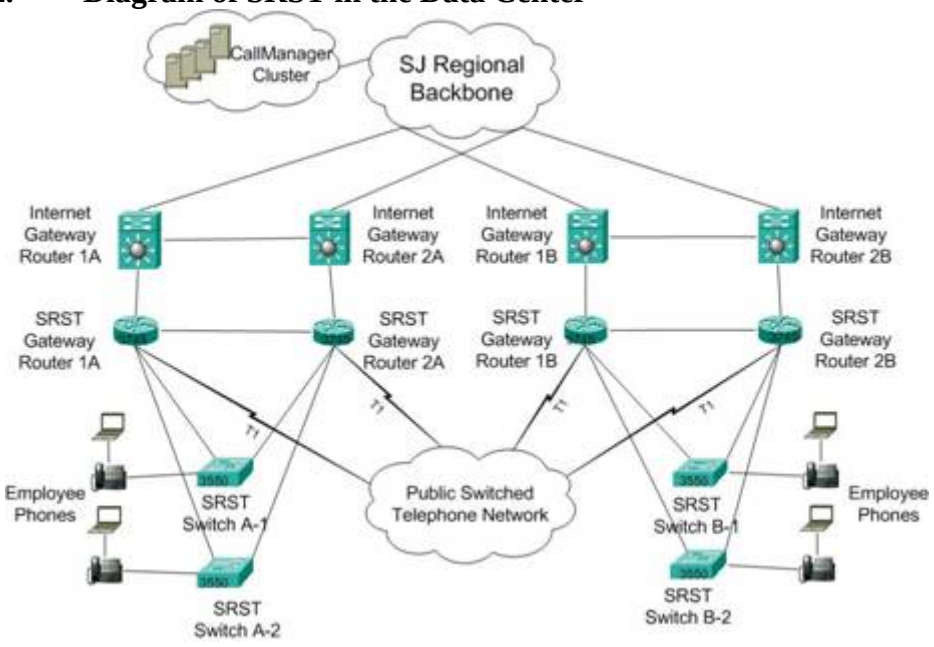
Figure 1. Dick at an IP Phone in the OCC

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 2. 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 3. 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 4. 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 5. 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 6. 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.

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

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.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
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
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
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
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.**

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