

# Cisco IT Data Center and Operations Control Center Tour



## 4 Root Cause Analysis and Change Management

### Root Cause Analysis

**Figure 1. 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 2. 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 3. 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.

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)