White Paper

How Cisco **IT-LAN-SJ** Achieved High Availability

Table of Contents

Preface

In the 21st century the network is the critical enabler of employee productivity. Customers purchase products using the network. The network controls the supply chain and facilitates human resources, payroll, benefits, and training. And through IP telephony, phone calls share the data network infrastructure.

Cisco Systems® cannot function in this environment without an operational and highly available network. Availability is typically measured by how many minutes each week the network is down or unavailable.

- Three nines (99.9) = 10 minutes downtime every week
- Four nines (99.99) = 1 minute downtime every week
- Five nines (99.999) = 6 seconds downtime every week

Three-nines availability is no longer adequate. Cisco must achieve at least four nines to function effectively, but five nines is the availability and the measure to which companies aspire. Although many corporations have networks or equipment designed to achieve 99.999 percent availability, very few companies have reported achieving that level in a large-scale production environment.

Spanning 50 buildings throughout San Jose and serving desktops, data centers, laboratories, and manufacturing, the Cisco IT-LAN-SJ (San Jose) network consists of 900 switches, 200 routers, 250 console servers, 800 Cisco® Aironet® access points, and an assortment of content switching devices inside the Cisco firewall. Despite its size and complexity, in 2002 the San Jose network approached 99.999 percent availability. During the second calendar quarter of 2003, in areas where the network is 100 percent uninterruptible power supply (UPS) and generator backed, Cisco IT-LAN-SJ achieved 99.99853 percent availability.

This paper shares Cisco success in achieving high availability on the San Jose campus, how it is measured, availability results, and the steps Cisco IT-LAN-SJ took to strive for 99.999 percent availability. The paper concludes with a discussion of how the Cisco IT-LAN-SJ network aligns with those steps and the importance of planning to develop the most cost-effective approach to achieving high availability.

THE INFORMATION HEREIN IS PROVIDED ON AN "AS IS" BASIS, WITHOUT ANY WARRANTIES OR REPRESENTATIONS, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

Measuring Raw Availability

Since the beginning of Six Sigma, organizations have measured quality by establishing a baseline, setting goals, and developing process improvements. Today, a company's success often ties directly to the ability to keep its network fully optimized, operational, and highly available. However, a plan to achieve high availability must be realistic and take into account only those devices that directly affect user satisfaction.

Availability measurements serve two purposes:

- Measure the service provided to the network user
- Provide a tool to help improve the service provided to the network user

Availability measurements are not just a measure of service, they also provide a strategic tool to improve service. For wired network connections, the level of service made available to the network user is best estimated by the availability of access layer switches. These switches connect users' laptops with a Category 5 cable, typically running through structured cabling from a cubicle or office to the closest network closet. Whereas the availability of access layer switches directly affects end users, the availability of distribution and core devices is less important when measuring service. Redundant networks are designed so that an individual device in the core can be down without affecting users. But an access layer switch outage will always have an impact because typical end users physically connect their computers to only one switch. As a result, Cisco IT measures the service level provided to users by measuring the availability of access layer switches. These measurements will still reflect a redundancy failure in the core because the core failure would prevent pings from getting through the core to the access layer switches.

Although monitoring access layer switches may be the best way to measure the service level provided to the customers, monitoring availability to core devices still has operational value. If a network link in the core is dropping packets, it may be difficult to identify the link if you only have availability data for access layer switches. If the network operators have availability data for every network device, pinpointing the location of packet loss is much easier. For this reason, the availability of all network devices should be measured. The network team uses these availability reports for problem isolation. But because the core availability measurements do not reflect the level of service provided to users, Cisco IT excludes them in the metrics provided to management.

Wireless Connections

Cisco IT considers wired network connectivity a Priority 1 (P1) service, monitoring and immediately repairing all outages affecting wired network connectivity 24 hours a day, every day, and paging a network engineer after hours if necessary to restore service. (See p. 21 for a discussion on priority levels.)

Conversely, wireless connectivity is a Priority 4 (P4) service. Wireless network outages are repaired during business hours only. Wireless outages do not prevent users from working because they can plug into a physical network port if necessary. Because metrics show that most wireless use occurs during business-hour meetings, the effect of an extended after-hours outage is minimal.

Furthermore, pinging wireless access points does not provide a reliable measure of wireless service availability. Although an access point can be pinged, users may be unable to associate to the wireless network for many reasons, including radio interference, failed access point radio, software driver problems, and authentication server problems.

As a result, Cisco IT-managed wireless access points are not included in the Cisco IT-LAN-SJ Production availability group but are included in the Test availability group. (See "Groups and Subgroups" below.) Although Cisco continues to research ways to accurately measure wireless service availability, that topic will not be covered further in this document.

Measuring Raw Availability for a Single Device

Cisco IT-LAN-SJ availability is measured from network management servers in a San Jose data center with two pings generated to each managed device every 15 to 20 seconds. If the management server receives at least one reply, the device is considered up (available) during that time period. This is used to determine the raw availability for that device during that day.

Groups and Subgroups

Two Availability Groups: Cisco IT-LAN-SJ-Production and Cisco IT-LAN-SJ-Test

Cisco monitors and measures all devices related to network connectivity. However, to differentiate outages that directly affect users from those outages that have no effect, Cisco IT-LAN-SJ created two availability groups called Cisco IT-LAN-SJ-Production and Cisco IT-LAN-SJ-Test.

Cisco IT-LAN-SJ-Production—The Cisco IT-LAN-SJ-Production group measures service provided to customers by pinging access layer switches directly connected to customers. The only exception is the laboratory network where the demarcation point between Cisco IT and the laboratory is an access layer router. In the laboratory case the loopback addresses of the access layer routers are monitored.

The Production Group is divided into subgroups based on function and location as follows:

- Production Data Center 1 (PDC1)
- PDC2
- Development Data Center 1 (DDC1)
- DDC2
- DDC3
- DDC4
- DDC5 (closed in November 2002)
- Laboratories
- San Jose Metropolitan Area Network (MAN) desktops
- San Jose Site 1–3 desktops
- San Jose Site 4 desktops
- San Jose Site 5 desktops
- San Jose CallManager Network

Production data centers support Cisco business functions (Website, ordering, manufacturing, and enterprise resource planning [ERP]). Development data centers support Cisco hardware and software development. This categorization reports availability in a meaningful way. In addition to reporting overall availability for Cisco IT-LAN-SJ as a whole, reporting availability by subgroup allows management to understand whether an availability hit affected labs, which is a concern—or a production data center, which may impact revenue.

The creation and modification of the production availability groups and subgroups are carefully controlled with major updates made only by the technical lead after careful consideration. In addition, because an update made at the end of a fiscal quarter could skew the statistics for that quarter, major updates (such as the creation or deletion of subgroups) are made only at the beginning of each fiscal quarter.

Cisco IT-LAN-SJ-Test Availability Group—The Cisco IT-LAN-SJ-Test availability group consists of all other network devices managed by Cisco IT-LAN-SJ, and includes routers, nonaccess switches, Cisco PIX® security appliances, LocalDirectors, content services switches, out-of-band management devices, and wireless access points. Because all network devices are in an availability group, the Cisco IT-LAN team receives automated reports on availability, enabling them to identify and investigate connectivity problems, regardless of whether they directly affect the customer. The Cisco IT-LAN-SJ-Test availability group is also known as the "Test" availability group.

Cisco network engineers use the Cisco IT-LAN-SJ-Test availability group for diagnostic purposes only and do not report results to management. The Test availability group is divided into informally defined subgroups, and any network engineer on the team can create a test subgroup as needed. Following is a list of the current Cisco IT-LAN-SJ-Test subgroups:

- Cisco Lightweight Extensible Authentication Protocol (Cisco LEAP)—Monitors the authentication application used for wireless connectivity to measure wireless service availability.
- IPv6—Measures devices in the IPv6 deployment that have not yet been defined as a P1 service.
- All routers in IT-LAN-SJ.
- Site 5 infrastructure—Created by the network engineer responsible for that site for his or her use.
- WAN-SJ-Reliability—Measures uptime of WAN/MAN circuits in the area.
- WAN-SJ-Availability—Measures the percentage of uptime for at least one WAN/MAN circuit to each remote site.
- All wireless access points in IT-LAN-SJ.

Calculating Raw Availability for Groups and Subgroups

The raw availability of a *subgroup* is the average of the raw availability of all devices in that subgroup. The raw availability of a *group* is the average of the raw availability of all devices in that group, including all devices in all subgroups.

> Note: The raw availability of a group is *not* the average of the raw availability of its subgroups. This would give extraordinary weight to small subgroups, such as the Cisco IT-LAN-SJ-Production/DDC4 subgroup with its five access layer switches. The Cisco IT-LAN-SJ-Production/Site 4 Desktops subgroup is given more weight because it has 374 access layer switches. Whereas each device in the group carries equal weight in availability calculations, each subgroup does not carry equal weight.

Daily, Monthly, Quarterly, and Annual Calculations

The availability of each device, group, and subgroup is calculated daily from the ping statistics using an "availability day" that runs from 4 p.m. to 4 p.m. Pacific Time (midnight to midnight GMT). Monthly statistics for each group and subgroup are calculated by averaging the daily statistics for the month. Although this introduces some rounding error, it eliminates complexity introduced by devices being added and deleted from subgroups during the month.

Statistics are also generated on a fiscal quarter basis. Cisco fiscal quarters for 2003 are:

- Q1FY2003: July 28, 2002 through October 26, 2002
- Q2FY2003: October 27, 2002 through January 25, 2003
- Q3FY2003: January 26, 2003 through April 26, 2003
- Q4FY2003: April 27, 2003 through July 26, 2003

Because the fiscal quarters do not align with calendar-month boundaries, the quarterly availability statistics average the availability for the 91 days in the quarter. The quarterly statistics for the Production group and subgroups are reported up through the management chain, whereas monthly statistics are used within the team to maintain awareness of availability.

Measuring Adjusted Availability

The goal of availability measurements is to measure the service level provided to customers. Outages that affect users must be measured, but planned outages that have no effect should be measured differently and adjusted to report the true service level provided to the network users.

Consider the circumstances of outage A:

- Desktop network in building 11 down from 9 p.m. to midnight Tuesday night.
- The outage was a planned network upgrade.
- Users in that building were notified in advance.

The users in that building were only minimally affected. Although they could not work after 9 p.m. that evening, they were notified well in advance so that if they were performing critical work in that building—such as a tapeout—they could have requested a reschedule of the outage. Given the minimal effect, the availability measurement should be adjusted to exclude this planned outage.

Now, consider outage B:

- Production Data Center 1 (PDC1) network down 9 p.m. to midnight Tuesday night.
- The outage was a planned network upgrade.
- Users of that data center were notified in advance.

The users of that data center were affected. Even though advance notification and off-hours scheduling mitigated the effect somewhat, data centers perform business critical functions 24 hours a day, every day. In this case, raw availability is the best measure of effect on network users.

Finally, consider Outage C:

- Desktop network in building 11 down 2 p.m. to 5 p.m. Tuesday afternoon.
- The outage was unplanned.

Users in that building were affected, leaving potentially hundreds of Cisco employees unable to work for most of the afternoon. In this case, raw availability must be measured due to the adverse effect on network users.

Because of variable circumstances such as these, Cisco IT measures both raw and adjusted availability, with planned outages excluded in adjusted availability. For desktop networks and laboratories, adjusted availability is most relevant. However, for data centers, including the Cisco CallManager subgroup, both adjusted and raw availability numbers are closely evaluated.

This evaluation helps motivate optimal behavior on the part of network engineers. For example, simply reloading a switch performs code upgrades in desktop networks. This is the most labor-efficient process and does not impact adjusted availability, which is most relevant in desktop networks. Code upgrades in data center networks are performed using high-availability procedures to minimize the impact on raw availability, which is most relevant in data centers, but incurs a cost of additional labor.

Change Management Process

The most difficult but critical element of this strategy is determining which outages are planned. If this were a manual process, it would be vulnerable to cheating. To circumvent that possibility, Cisco integrated its change management process with availability measurements.

Fundamental rules of the Cisco IT-LAN-SJ network change management process:

- Change management requests must be submitted before the outage begins.
- Requests must include the timeframe of the change and all devices affected by the change.
- Management must approve each request.
- Users must be given proper notification.
- All emergency changes that cannot provide sufficient advance notice for users require operations duty manager approval.

Most changes occur after regular business hours and most approvals are made at a daily change management meeting that typically occurs at 8 a.m. Pacific Time. Changes with large impact—such as a data center outage—are rejected unless planned well in advance.

Note: For purposes of adjusted availability, a device listed as "impacted" by an approved change management is considered fully operational during the change window.

Avoidable and Unavoidable Outages

Adjusted availability measures the level of service provided to users. In addition to availability, Cisco IT-LAN-SJ categorizes outages as avoidable or unavoidable. Examples of unavoidable outages include:

- Power outages
- Natural disaster (in the area of the disaster)

By default, all outages are considered avoidable. The following are examples of avoidable outages:

- Hardware failures
- Software failures
- Human error
- Process failures
- Denial-of-service (DoS) attacks
- Outages of unknown cause
- Natural disasters (downstream from the disaster, where redundancy could have been provided)

Categorizing outages as avoidable versus unavoidable helps identify which outages can be prevented in the future and give management perspective when reviewing the top outages. Regardless of whether an outage is avoidable or unavoidable, if it is unplanned, it affects both raw and adjusted availability because the unplanned outage affects service.

Cisco IT-LAN-SJ-Production 2002 Availability

The following results demonstrate the difference between adjusted and raw availability in each subgroup.

2002 Results by Subgroup

Subgroup	Adjusted	Raw
Overall	99.992%	99.964%
DDC4	99.998%	99.964%
CallManager Network	99.998%	99.967%
PDC1	99.997%	99.995%
DDC5	99.997%	99.997%
PDC2	99.996%	99.991%
Site 5 Desktops	99.995%	99.992%
DDC1	99.995%	99.878%
Site 1–3 Desktops	99.993%	99.966%
DDC3	99.992%	99.909%
MAN Desktops	99.991%	99.969%
DDC2	99.991%	99.912%
Site 4 Desktops	99.991%	99.947%
Lab Cluster	99.973%	99.943%

Overall Results by Month

Month	Adjusted	Raw
January	99.998%	99.991%
February	99.985%	99.950%
March	99.994%	99.989%
April	99.992%	99.992%
May	99.994%	99.991%
June	99.987%	99.978%
July	99.999%	99.880%
August	99.999%	99.984%
September	99.998%	99.984%
October	99.995%	99.994%
November	99.997%	99.948%
December	99.970%	99.892%

Top 5 Unplanned Outages

Date	Daily Adjusted Availability	Outage Description
December 19, 2002	99.618%	Unplanned power outage in sites 3 and 4
December 20, 2002	99.644%	Extended power outage in building 13
February 21, 2002	99.747%	DDC2 and DDC3 outage due to hardware failure
June 28, 2002	99.764%	Simultaneous upgrade caused routing instability
April 23, 2003	99.880%	Senter Road power outage

Analysis of Top Five Unplanned Outages

December 19, 2002 unplanned power outage in sites 3 and 4—San Jose experienced a widespread power outage impacting about 25 Cisco buildings for approximately 3 hours. Although Cisco data centers all have UPS and generator backup, the desktop networks have many devices on either house power with no UPS, or are UPS only. The power outage represented the largest availability hit for 2002 but was considered unavoidable by Cisco IT-LAN-SJ. Although this outage was considered unavoidable, it was still counted against adjusted availability statistics because it impacted the service level provided to our users.

December 20, 2002 extended power outage in building 13—San Jose site 4 experienced a widespread power blip early in the morning, causing an electrical equipment failure in building 13 that took the power out in building 13 for most of the day. Although from an IT Networking perspective this was an unavoidable outage, it counted against adjusted availability statistics because it was an unplanned outage that affected service provided to our users.

February 21, 2002 DDC2 and DDC3 outage due to hardware failure—A router in Development Data center 3 suffered a hardware outage and redundancy failed due to an error in the design of the two data centers that were linked in a hierarchy violation at the time. This outage was considered avoidable. Physically and logically separating the data centers and rebuilding the data center networks to comply with the new Cisco standard data center design corrected the design flaw.

June 28, 2002 simultaneous upgrade caused routing instability—This avoidable outage, caused by a process error, was the result of two separate Cisco IT-LAN-SJ network engineers executing change requests to upgrade devices in two different layers of the network hierarchy simultaneously. Although both change requests included e-mail notification to the team, the fact that both changes were going to occur simultaneously was overlooked. The simultaneous upgrade resulted in network instability. Because the outage was caused by a process error, it was considered avoidable.

April 23, 2002 Senter Road power outage—This unavoidable outage was caused by a power outage at the Senter Road site, which is in the San Jose Metropolitan Area Network (MAN).

Top 5 Planned Outages

Date	Daily Raw Availability	Change Description
July 13, 2002	96.497%	Power work and network rearchitecture
Dec. 7, 2002	97.850%	Power work in three buildings
Nov. 2, 2002	99.167%	Building 8 planned power outage
Feb. 16, 2002	99.460%	Silvercreek planned power outage
Nov. 16, 2002	99.507%	Building 2 planned power outage

Analysis of the Top Five Planned Outages

July 13, 2002 power work and network rearchitecture—The facilities team needed an extended power outage in Development Data center 1 to expand the power capacity. Networking used that outage as an opportunity to rebuild the data center network and make it compliant with our standard data center design.

December 7, 2002 power work in three buildings—The facilities team needed an extended power outage in three buildings. Networking used the outage as an opportunity to rebuild the development data center networks in those buildings and make them compliant with the Cisco standard data center design. This was also the “long term fix” for the unplanned network outage to DDC2 and DDC3 that occurred on February 21.

November 2, 2002 Building 8 planned power outage—Facilities needed an extended power outage in building 8.

February 16, 2002 Silvercreek planned power outage—Facilities needed an extended power outage in the Silvercreek MAN site.

November 16, 2002 Building 2 planned power outage—Facilities needed an extended power outage in building 2.

Summary

Overall, Cisco achieved 99.992 percent adjusted availability in the San Jose LAN during 2002, despite the fact that three of the five worst outages were due to uncontrollable power outages. In addition, the networks in Development Data centers 1 through 3, and in labs were significantly improved during the year, which should result in a substantial improvement in availability during 2003.

The remainder of this document suggests recommendations to achieve 99.9 percent, 99.99 percent, and 99.999 percent availability, based on the Cisco IT-LAN-SJ experience. Although results will vary, Cisco IT-LAN-SJ has found these steps to be effective in improving availability.

Cisco IT has instituted most of these recommendations, but it is not cost effective to implement all of them in all areas. Decisions need to be made regarding which areas of the network are most critical and require high availability. For example, to achieve 99.999 percent availability, all devices should be on UPS and generator. However, because this would be a costly endeavor, Cisco IT chose to implement it only in data centers, not on desktop and laboratory networks.

Please see the end of this paper to identify which recommendations Cisco has implemented on each section of its San Jose network.

Steps Cisco Took to Achieve 99.9% Availability

Step 1
Measuring Availability

The first step in achieving maximum uptime is to monitor and continuously measure availability. Measuring availability should not be viewed just as an occasional metric tool for management, but also as a tool to improve service delivery. Measurements can be used strategically to identify and to correct the causes of large outages, and tactically to identify and to correct causes of small, localized outages.

Using Availability Measurements Strategically

Measurement reports are generated on a monthly, quarterly, and annual basis by a senior network engineer to maintain focus on service availability, both successes and areas requiring improvement. Following is the availability report for November 2002:

Date: Mon Dec 2, 2002 3:53:23 PM US/Pacific
Subject: November 2002 Availability Report for IT-LAN-SJ

November 2002 Availability Report for IT-LAN-SJ

Adjusted Availability: 99.997%
Raw Availability: 99.948%

Subgroup	*Adjusted*	*Raw*
DDC1	99.984%	99.984%
MAN	99.988%	99.988%
Site 4	99.998%	99.887%
CM	99.998%	99.886%
Site 1-3	99.999%	99.999%
Site 5	99.999%	99.999%
Labs	99.999%	99.963%
DDC4	100.000%	99.599%
DDC2	100.000%	100.000%
DDC5	100.000%	100.000%
DDC3	100.000%	100.000%
PDC2	100.000%	100.000%
PDC1	100.000%	99.994%

Top Unplanned Outages:

Nov 23:	99.949%	DDC1 power outage/UPS failure
Nov 9:	99.981%	Scotts Valley power outage
Nov 24:	99.988%	Site 1–4 power outage
Nov 28:	99.997%	Minor blip of unknown cause

Top Planned Outages

Nov 2:	99.167%	Building 8 planned power outage
Nov 16:	99.507%	Building 2 planned power outage
Nov 24:	99.902%	Building 5 planned power outage
Nov 21:	99.922%	DDC4 rearchitecture, building 12 laboratory rearchitecture

COMMENTARY: Except for the 99.997 percent blip on November 28, all outages were identified, explained, and deemed to be outside of IT-LAN-SJ's control. Excluding uncontrollable outages, availability would have been 100.000 percent. In addition, the high availability in the laboratory cluster is the result of the laboratory rearchitecture. In fact, the 99.999 percent laboratory cluster adjusted availability exceeds the production availability due to the deployment team's work in this area.

Report

This report shows the overall availability score for the Cisco IT-LAN-SJ-Production availability group. Quarterly reports are provided to executive management and allows them to see which areas are meeting the Service Level Agreement (SLA) and which areas are having trouble.

The report consists of several sections as shown below:

The overall summary

November 2002 Availability Report for IT-LAN-SJ

Adjusted Availability: 99.997%

Raw Availability: 99.948%

The summary by subgroup

Subgroup	*Adjusted*	*Raw*
DDC1	99.984%	99.984%
MAN	99.988%	99.988%
Site4	99.998%	99.887%
CM	99.998%	99.886%
Site1-3	99.999%	99.999%
Site5	99.999%	99.999%
Labs	99.999%	99.963%
DDC4	100.000%	99.599%
DDC2	100.000%	100.000%
DDC5	100.000%	100.000%
DDC3	100.000%	100.000%
PDC2	100.000%	100.000%
PDC1	100.000%	99.994%

Top unplanned outages

Nov 23:	99.949%	DDC1 power outage/UPS failure
Nov 9:	99.981%	Scotts Valley power outage
Nov 24:	99.988%	Site 1-4 power outage
Nov 28:	99.997%	Minor blip of unknown cause

This section lists the unplanned outages for the month with the largest impact to adjusted availability. To clarify the impact of the outage, that day's adjusted availability is also shown for the Cisco IT-LAN-SJ-Production group. The 99.949 percent availability for November 23 corresponds to unavailability of 0.051 percent. The 99.997 percent availability for November 28 corresponds to unavailability of 0.003 percent. In this case, the DDC1 power outage on November 23 had 17 times more impact to network users than the "minor blip of unknown cause" on November 28.

Top planned outages:

Nov 2:	99.167%	Building 8 planned power outage
Nov 16:	99.507%	Building 2 planned power outage
Nov 24:	99.902%	Building 5 planned power outage
Nov 21:	99.922%	DDC4 rearchitecture, building 12 laboratory rearchitecture

This section lists approved change requests that had the greatest effect on raw availability. Raw availability statistics for Cisco IT-LAN-SJ-Production for that day are included to give perspective. In this case, the three largest planned outages were due to power work on three buildings. In addition, on November 21 the rearchitecture of DDC4 and the laboratory network in building 12 was completed in two separate changes.

COMMENTARY: Except for the 99.997 percent blip on November 28, all outages were identified, explained, and deemed outside of IT-LAN-SJ's control. Excluding uncontrollable outages, our availability would have been 100.000 percent. In addition, the high availability in the laboratory cluster is the result of the laboratory rearchitecture. In fact, the 99.999 percent laboratory cluster adjusted availability exceeds the production availability due to the deployment team's work in this area.

The commentary section notes whether the network team could have avoided the unplanned outages. All outages are considered avoidable if the cause is unknown, such as the "blip of unknown cause" on November 28. The commentary also serves as an opportunity to provide positive feedback to the team. In this case, the recent rearchitecture of the lab network and the 99.999 percent adjusted availability for that subgroup was a direct result. By providing positive feedback in a report with high visibility to management, actions that improve availability are strongly reinforced.

Using Availability Measurements Tactically

In addition to providing strategic service level measurements, availability statistics function as a tool to improve the level of service to customers. Availability hits to individual devices need to be identified and investigated. To accomplish this, the Cisco IT-LAN-SJ team receives a daily e-mail listing all devices that failed to achieve 100 percent adjusted availability the previous week. Following is a portion of a sample report:

Group/SubGroup: IT-LAN-SJ-Production/DDC4
Availability Target: 99.985, Annotated Availability Target: 99.999

Resource	Annotated UTC Date	Adjusted Availability	Raw Availability	Area	Minutes Unavailable
ddc4-row3-sw1.cisco.com	27-MAR-2003	99.973	99.973	IS-HQ HQ	0
ddc4-row3-sw1.cisco.com	29-MAR-2003	99.975	99.975	IS-HQ HQ	0
ddc4-row5-sw1.cisco.com	29-MAR-2003	99.975	99.975	IS-HQ HQ	0
ddc4-row1-sw1.cisco.com	30-MAR-2003	99.975	99.975	IS-HQ HQ	0
ddc4-row11-sw1.cisco.com	30-MAR-2003	99.977	99.977	IS-HQ HQ	0
ddc4-row2-sw1.cisco.com	30-MAR-2003	99.977	99.977	IS-HQ HQ	0
ddc4-row3-sw1.cisco.com	30-MAR-2003	99.975	99.975	IS-HQ HQ	0
ddc4-row5-sw1.cisco.com	30-MAR-2003	99.975	99.975	IS-HQ HQ	0
ddc4-row11-sw1.cisco.com	31-MAR-2003	99.977	99.977	IS-HQ HQ	0

This report includes all devices that did not meet the "annotated availability target" on a particular date. To avoid huge reports, Cisco IT-LAN-SJ initially sets the "annotated availability target" low, for example, to 99 percent. Over time, as problems are fixed, the annotated availability target can be gradually raised. With availability monitored every 15 to 20 seconds, the 99.973 percent to 99.977 percent availability figures in this report represent one failed monitoring attempt for each device listed.

Step 2
Outage Alerts

Communication is a critical element to achieving high availability, informing support staff in real-time regarding outages. Priority levels are assigned to each Cisco IT-LAN-SJ device to initiate the appropriate response as shown below:

- Priority 1: Large access layer switches where redundancy is irrelevant because customers connect directly to the switch and lab gateways that do not have redundancy.

- Priority 2: Routers with redundancy and small access layer switches.

- Priority 3: Out-of-band management and other support networks.

- Priority 4: Wireless access points.

All devices in the Production availability group are (P1) or (P2). The Operations Command Center (OCC) monitors P1 devices 24 hours a day, everyday, and P2 devices during business hours. An outage page is triggered when a device is down for 2 minutes. The outage during those timeframes will be managed by the OCC, which pages on-call personnel and performs management escalations.

Priority 1–3 devices page out to on-call personnel 24 hours a day, everyday, although on-call personnel may choose not to respond immediately for P3 outages.

Priority 4 devices page out to on-call personnel during business hours.

A network outage in the vicinity of the monitoring/alert system will be detected by the OCC. In that circumstance the OCC can still manually page people using IP telephony backed up with Survivable Remote Site Telephony (SRST).

Step 3
Physical Hierarchy

To achieve 99.9 percent availability, Cisco required a fundamentally stable network. In order to achieve this, Cisco needed both physical and logical hierarchy.

Physical Layout of a San Jose Campus Building

Cisco buildings are organized by IDF, LDF, SDF, BDF, and NOC network rooms (definitions below). To understand how the physical hierarchy is implemented, the following discusses the physical layout of Cisco San Jose campus buildings:

Intermediary Distribution Frame (IDF)—Typical San Jose buildings have two to five floors. Each floor has two IDFs with Category 5 (Cat5) cable running from each wallplate to one of the IDFs. A small number of locations, mostly wallplates for phones in public areas, have Category 3 (Cat3) cable. Two IDFs allow all cable runs to be less than 100 meters in length to meet Cat5 specifications. With two IDFs on each floor, each building contains four to ten IDFs and each IDF has the following types of cable going back to the Building Distribution Frame (BDF):

- Cat5 copper (mostly used for consoles)
- Multimode fiber
- Single-mode fiber

Telecom style wiring exists in older buildings but is no longer used due to the full conversion to IP telephony throughout Cisco. Newer buildings on the San Jose campus were constructed without telecom style wiring.

Lab Distribution Frame (LDF)—Structured cabling from the BDF to the laboratory terminates in an LDF, most of which have the following types of structured cabling going to the BDF:

- Cat5 copper (distance may exceed 100 meters in a few cases)
- Multimode fiber

A few laboratories may also be equipped with single-mode fiber. Like IDFs, all LDFs should have structured cabling running to the BDF to enforce the physical hierarchy.

Building Distribution Frame (BDF)—The BDF is the network aggregation point for networks in a building (exception: see SDF). In San Jose, most BDFs are located on the second floor, although a few older buildings have BDFs on the first floor. The structured cabling of all IDFs and LDFs in each building terminates in the BDF. In addition, the BDF has the following structured cabling running to Network Operations Centers (NOCs) in that campus:

- Multimode fiber
- Single-mode fiber

If a NOC exists in the same building as a BDF, all the structured cabling runs to that NOC and is cross-patched to other NOCs as necessary. If a NOC is not located in a building, then the structured cabling runs directly from the BDF to two separate NOCs in that campus. The exception to this rule is if a campus has only one NOC.

Data center zonal cabinet—Cisco data centers contain compute servers that are typically organized in rows of racks. Most Cisco data centers have a zonal cabinet at the end of each row that usually includes an access layer switch and a console server. Structured Cat5 and multimode fiber cabling runs from each server rack to the zonal cabinet. Structured Cat5 and multimode fiber also runs from each zonal cabinet to the Server Distribution Frame (SDF).

Server Distribution Frame (SDF)—Buildings with data centers are served with a SDF. Every SDF is located in a building with a NOC with structured cabling that runs from data center zonal cabinets and terminates in the SDF. The SDF has structured cabling that runs to the NOC in the building and individual fiber patches cross-patched to another NOC in the campus for redundancy. The SDF typically holds data center gateways, console servers, and content switching devices.

Network Operations Center (NOC)—The NOC is a physical aggregation point for network equipment and structured cabling. The San Jose LAN campus is divided into the following sites for purposes of network aggregation:

- Sites 1–3 (lettered buildings A–P)
- Site 4 (numbered buildings 1–19)
- Site 5 (numbered buildings 20–25)

Sites 1–3 have four NOCs. Site 4 also has four NOCs. Due to a cost-risk-benefit analysis during construction, site 5 has one NOC.

Note: Cisco is considering installing only single-mode fiber in new installations. The major obstacles are data center hosts with network interface cards (NICs) that require the use of multimode fiber.

The Physical Hierarchy of the San Jose Structured Cabling

The structured cabling in Cisco's San Jose campus follows a core/distribution/access hierarchy model. There are a total of nine NOCs that form the core of the network on the San Jose campus. The BDFs and SDFs form the distribution layer of the physical network hierarchy and the IDFs, LDFs, and data center zonal cabinets form the access layer.

Cisco designs and implements networks in a physical hierarchy. This strategy encourages network engineers to deploy hierarchical networks by making it easier to do. In addition, a hierarchically designed network in a hierarchical structured cabling plant will result in simpler fiber patching (fewer jumpers) between network devices, improving reliability, and easing troubleshooting.

The Physical Hierarchy of the San Jose Network

The San Jose network consists of the following levels of hierarchy that approximate the traditional core/distribution/access model, moving from the edge to the core:

- **Access-layer switches**—Users connect their workstations directly into access layer switches. Cisco IT uses the Cisco 6500 Series Switch running Cisco Catalyst OS as the primary access layer switch. In some areas of low port density, Cisco Catalyst® 3550-24 PWR switches are used. In older deployments, Cisco Catalyst 3524 XL switches are used.

- **Access-layer gateways**—Each access layer switch directly connects into a pair of access layer gateways. These are typically Cisco 6500 Series switches or 7600 Series routers running native Cisco IOS® Software. Each building contains one pair of desktop network access layer gateways, also called BDF gateways. In addition, some buildings have additional access layer gateway pairs for specialized functions. For example, buildings with data centers have a separate pair of data center gateways in the SDF.

- **Cluster gateways**—Each grouping of 6 to 12 pairs of access layer gateways aggregate upward into a pair of cluster gateways. These are separated by function so that desktop access layer gateways aggregate into desktop cluster gateways, and data center access gateways aggregate into data center cluster gateways. These are typically Cisco 6500 Series switches or 7600 Series routers running native Cisco IOS Software.

- **Site backbone**—From a networking perspective, the San Jose campus has four sites:

  – Sites 1–3 (one site from a networking topology standpoint)

  – Site 4

  – Site 5

  – MAN

  Each site has a pair of backbone routers that are typically Cisco 6500 Series switches or 7600 Series routers running native Cisco IOS Software. The MAN backbone routers use FlexWAN modules instead of Gigabit Ethernet for much of their connectivity.

- **Regional backbone—**The San Jose campus uses six Cisco 6500 Series routers running native Cisco IOS Software to form a regional backbone. The four site backbones connect into the regional backbone. The regional backbone also connects to the corporate firewalls leading to the demilitarized zone (DMZ), as well as the Cisco WAN network.

Physical Hierarchy Summary

To achieve 99.9 percent or greater availability, a network must be fundamentally stable with a well-defined physical hierarchy. This prevents network additions from creating a chaotic network topology with too much redundancy in some locations—increasing routing complexity—and insufficient redundancy in others. A well-defined physical hierarchy makes it easier to provide the correct amount of redundancy and keeps the network fundamentally stable.

Physical hierarchy is also a prerequisite for logical hierarchy, a critical necessity for maintaining routing stability.

Step 4
Logical Hierarchy

In addition to physical hierarchy, logical hierarchy creates the foundation for a fundamentally stable network. The Cisco global network has more than 23,000 subnets entered into the address management database. Although Border Gateway Protocol (BGP) can handle a routing table of that size without difficulty, IGPs, which emphasize fast convergence over scalability, cannot. Regardless of the IGP routing protocol (EIGRP, OSPF, or IS-IS), a route table with 23,000 routes would result in instability.

Reducing the route table size requires a logical hierarchy, achievable with three components:

1. Physical hierarchy (see above).
2. Address space assigned hierarchically to align with the physical hierarchy.
3. Route summarization to take advantage of the hierarchical address space allocation.

Internet Routable and RFC1918 Addresses

Complicating the address space hierarchy is the requirement for two different types of address space. Internet routable space is used by user workstations because users access the Internet as part of their normal work. Because of the global shortage of Internet routable IPv4 space, RFC1918 space should be used whenever possible. Cisco uses RFC1918 address space for IP telephony, out-of-band-management, and most laboratory networks.

Site 4 Address Hierarchy Example

RFC1918 Space for Site IP Telephony

10.16.0.0/17 IP telephony—Site 4
---**10.16.0.0/19** Site 4, Desktop Cluster A, IP Telephony (Bldgs 1–7)
---**10.16.32.0/19** Site 4, Desktop Cluster B, IP Telephony (Bldgs 8–12)
---**10.16.64.0/19** Site 4, Desktop Cluster C, IP Telephony (Bldgs 13–19)
---**10.16.96.0/21** Site 4, Desktop Cluster A, IP Telephony (Bldgs 1–7)
---**10.16.104.0/22** Site 4, Desktop Cluster B, IP Telephony (Bldgs 8–12)
---**10.16.108.0/22** Site 4, Desktop Cluster C, IP Telephony (Bldgs 13–19)
---**10.16.112.0/20** Site 4, Desktop Cluster C, IP Telephony (Bldgs 13–19)

The address allocations above are good but not perfect. Although the entire IP telephony address space can be summarized in one route advertisement from the site 4 backbone to the regional backbone, inside site 4 the summarization is imperfect. For example, the IP telephony address space for Desktop Cluster A can be summarized in two route advertisements: 10.16.0.0/19 and 10.16.96.0/21. That's very good, one route advertisement would be better.

Within each desktop cluster the address space can be allocated hierarchically down to the building level:

10.16.0.0/19 Site 4, Phase A, IP Telephony (Bldgs 1–7)
---**10.16.0.0/22** SJC01 IP Telephony (2nd and 3rd floors)
---**10.16.4.0/24** SJC01 IP Telephony (1st floor)
---**10.16.5.0/24** SJC02 IP Telephony (1st floor)
---**10.16.6.0/23** SJC02 IP Telephony (2nd floor)
---**10.16.8.0/23** SJC02 IP Telephony (3rd floor)
---**10.16.10.0/23** SJC03 IP Telephony (2nd floor)
---**10.16.12.0/22** SJC03 IP Telephony (3rd and 4th floors)
---**10.16.16.0/24** SJC03 IP Telephony (1st floor)
---**10.16.17.0/24** SJC04 IP Telephony (1st floor)
---**10.16.18.0/23** SJC04 IP Telephony (2nd floor)
---**10.16.20.0/23** SJC04 IP Telephony (3rd floor)
---**10.16.22.0/23** SJC05 IP Telephony (2nd floor)
---**10.16.24.0/23** SJC05 IP Telephony (3rd floor)
---**10.16.26.0/24** SJC05 IP Telephony (1st floor)
---**10.16.27.0/24** SJC06 IP Telephony (1st floor)
---**10.16.28.0/22** SJC06 IP Telephony (2nd and 3rd floors)

This address allocation is still not perfect, but it does allow many route advertisements to be summarized at the building level. Cisco IT Networking summarizes at the cluster and site backbone layers of the physical hierarchy rather than at the access layer gateway level because each summary adds complexity. Summarization at the cluster and backbone level is sufficient to achieve excellent routing stability. Allocation of address blocks for summarization to each building, however, enables summarization in the future should it be necessary.

Internet Routable Space for Site

171.71.0.0/16 (Site 4: Bldgs 1–19)

-- **171.71.0.0/24** Engineering WAN Point-to-Point Network Links (Site 4)

-- **171.71.1.0/24** Site 4 Network

-- **171.71.2.0/24** Reserved for San Jose Growth

-- **171.71.3.0/24** San Jose Campus, Site 4, Miscellaneous Clusters

-- **171.71.4.0/22** Site 4 Phase A Desktop Cluster (Bldg 1)

-- **171.71.8.0/21** Site 4 Phase A Desktop Cluster (Bldgs 1–2)

-- **171.71.16.0/21** Site 4 Lab Networks (non-RFC1918)

-- **171.71.24.0/21** Site 4 Phase A Desktop Cluster (Bldgs 3)

-- **171.71.32.0/19** Site 4 Phase A Desktop Cluster (Bldgs 4–7) (Wireless 1–4)

-- **171.71.64.0/20** San Jose MAN Sites

-- **171.71.80.0/20** Site 4 Phase B Desktop Cluster (Bldgs 8, 9, 12)

-- **171.71.96.0/20** Site 4 Phase B Desktop Cluster (Bldgs 9, 10, 11)

-- **171.71.112.0/22** Site 4 Phase B Desktop Cluster (Bldg 11)

-- **171.71.116.0/22** Site 4 Phase C Desktop Cluster (Bldg 13)

-- **171.71.120.0/21** Site 4 Phase C Desktop Cluster (Bldgs 13–14)

-- **171.71.128.0/20** Site 4 Phase C Desktop Cluster (Bldgs 14–16)

-- **171.71.144.0/21** Site 4 Phase C Desktop Cluster (Bldgs 16–17)

-- **171.71.152.0/22** Site 4 Network

-- 171.71.156.0/22 -(*Unallocated Block*)

-- **171.71.160.0/20** Site 4 Network

-- **171.71.176.0/21** Site 4 Network

-- **171.71.184.0/21** Site 4 Wireless Network Bldgs 5–8

-- **171.71.192.0/21** Site 4 Wireless Network Bldgs 9–12

-- **171.71.200.0/21** Site 4 Wireless Network Bldgs 13–16

-- **171.71.208.0/21** Site 4 Wireless Network Bldgs 17–19

-- **171.71.216.0/21** Site 4 Phase C Desktop Cluster (Bldgs 17–18)

-- **171.71.224.0/21** Site 4 Phase C Desktop Cluster (Bldgs 18–19)

-- **171.71.232.0/22** Site 4 Phase C Desktop Cluster (Bldg 19)

-- **171.71.236.0/27** Network for NTG server

-- 171.71.236.32/27 -(*Unallocated Block*)

-- 171.71.236.64/26 -(*Unallocated Block*)

-- 171.71.236.128/25 -(*Unallocated Block*)

-- 171.71.237.0/24 *-(Unallocated Block)*

-- 171.71.238.0/23 -(*Unallocated Block*)

-- **171.71.240.0/22** SJC RBB and Site 4 BB Links

-- 171.71.244.0/22 -(*Unallocated Block*)

-- 171.71.248.0/21 -(*Unallocated Block*)

Again, in the example above, the address space is allocated hierarchically. The address space for each desktop cluster can be summarized in a handful of route advertisements. The entire 171.71.0.0/16 address block can be summarized with one route advertisement from the Site 4 backbone to the regional backbone. In addition, the 171.71.64.0/20 address block is summarized out of the MAN site backbone into the regional backbone. This results in two route entries in the core routing table.

Consequences of No Hierarchy

172.24.0.0/16 Cisco IT-LAN (Engineering) RFC1918 Address Space
-- **172.24.0.0/19** San Jose Campus
-- **172.24.32.0/20** Remote Sites (Western Region and Central Region)
-- **172.24.48.0/21** San Jose Campus: Site 4 (IT-LAN Engineering)
-- 172.24.56.0/21 -(Unallocated Block)
-- 172.24.64.0/22 -(Unallocated Block)
-- **172.24.68.0/22** Center for Network Application (CNAP or POC) Bldg 13
-- 172.24.72.0/21 -(Unallocated Block)
-- 172.24.80.0/20 -(Unallocated Block)
-- **172.24.96.0/21** Remote Sites (All Regions)
-- **172.24.104.0/24** Sites 1–3 Network
-- **172.24.105.0/24** Site 4 Network
-- **172.24.106.0/23** St. Paul, Minn (Ieng) Lab network
-- **172.24.108.0/26** Ann Arbor, MI console network
-- 172.24.108.64/26 -(Unallocated Block)
-- 172.24.108.128/25 -(Unallocated Block)
-- **172.24.109.0/24** Site 4 lab backbone
-- **172.24.110.0/24** Center for Network Application (CNAP or POC) Bldg 13
-- **172.24.111.0/24** Site 4 Lab Backbone
-- **172.24.112.0/23** Sites 1–3 Lab Backbone
-- **172.24.114.0/24** Site 4 Lab Backbone
-- **172.24.115.0/24** Site 5 and McCarthy Lab Backbone
-- **172.24.116.0/22** Franklin, Mass (Altiga) Console, laboratory
-- **172.24.120.0/22** Franklin Desktop Network
-- **172.24.124.0/22** India RFC1918 Address Space
-- **172.24.128.0/21** Reserved for San Jose Campus
-- **172.24.136.0/21** Remote Sites
-- **172.24.144.0/21** Reserved for San Jose Campus
-- **172.24.152.0/30** Site 4 Network
-- 172.24.152.4/30 -(Unallocated Block)
-- 172.24.152.8/29 -(Unallocated Block)
-- 172.24.152.16/28 -(Unallocated Block)
-- 172.24.152.32/27 -(Unallocated Block)
-- 172.24.152.64/26 -(Unallocated Block)
-- **172.24.152.128/25** MSSBU - lab space in Bldg 1
-- 172.24.153.0/24 -(Unallocated Block)
-- **172.24.154.0/24** Lab network for sjc1-gsr laboratory
-- **172.24.155.0/24** Saint Paul, MN - laboratory expansion
-- **172.24.156.0/23** Salem, NH Laboratory Nets
-- **172.24.158.0/24** Eng net loopbacks, TBR
-- **172.24.159.0/24** RTP Comvault
-- 172.24.160.0/19 -(Unallocated Block)
-- **172.24.192.0/18** Remote Site

At one point in Cisco's history, Cisco IT allocated 172.24.0.0/16 to laboratories based on function instead of geography or hierarchy. This was a mistake.

In the above address layout, 172.24.155.0/24 is in Minnesota. The adjacent 172.24.156.0/23 is in New Hampshire. These geographically separated address blocks cannot be summarized. As a result of this haphazard allocation, the 172.24.0.0/16 address block results in 26 routes in Cisco's core routing table. On the other hand, the 171.71.0.0/16 address block (San Jose Site 4 and San Jose MAN) results in two routes in Cisco's core routing table. The difference is that the 171.71.0.0/16 address block was allocated hierarchically.

Maintaining Logical Hierarchy

Address space is a strategic resource for Cisco. If not allocated efficiently, it would be impossible for Cisco to justify more address space from the Internet registries to enable corporate growth. To ensure that all address allocations are executed efficiently and hierarchically, Cisco IT Networking has implemented the following four mechanisms.

1. **All address allocations are recorded in one central tool**—It is critical to understand and document all current allocations to maintain logical hierarchy. One master of record must exist for all address and subnet allocations, which could be anything from a text file under RCS (Revision Control System) control to a database with built-in subnet calculation functions. The critical factor is to have one master record for all address allocations within the company, as well as any address space obtained during corporate acquisitions.

2. **A team of Classless Interdomain Routing (CIDR) block administrators allocate large blocks strategically throughout the company**—Cisco has four primary locations, which include San Jose; the Americas; Europe, the Middle East, and Africa; and Asia Pacific. A global design team supports all locations. Two people from each location and two people from the global network design team are CIDR block administrators. This committee of ten people handles all Cisco's strategic address space allocations. The CIDR block administrators have experience with hierarchy, summarization, BGP route advertisements to Internet service providers (ISPs), and conservation of address space. They also consult with the Internet registries when necessary.

3. **Each network team has a designated member to handle tactical allocations**—CIDR block administrators allocate large blocks of address space to each network team. One team member handles local address space allocations. That team member is experienced with the need for hierarchy, summarization, and conservation of address space, and provides a centralized strategy for address space management.

4. **The core routing table is monitored for route additions or deletions**—In a global network, mistakes can happen that result in incorrectly allocated address space, accidentally deleted summarization statements during network changes, overlooked summaries, etc. To detect these mistakes, Cisco sends an e-mail with all changes in its core routing table to a team of network engineers on a daily basis using an automated job. Following is a sample e-mail message:

```
Date: Thu Apr 3, 2003 7:30:04 AM US/Pacific
Subject: Route Diff

Comparing routes for San Jose Regional Backbone
From: Wed Apr 2 7:30:01 US/Pacific 2003
To: Thu Apr 3 7:30:00 US/Pacific 2003
Deleted: 10.96.224.0/24 - Buenos Aires IP Telephony
Deleted: 10.96.225.0/24 - Rio IP Telephony DHCP scope
Deleted: 10.96.255.216/30 - Lima <-> San Jose/RWC WAN Link
Deleted: 10.96.255.220/30 - Santiago <-> San Jose/RWC WAN Link
Deleted: 64.100.181.192/26 - Brasilia, Brazil Desktop
Added: 10.96.248.0/31 - Virtual Host for Se1/0 on mxc-wan-gw1
Added: 10.96.248.2/31 - Virtual Host for Se2/0 on mxc-wan-gw1
Added: 172.30.54.0/25 -
Added: 172.30.54.128/25 -
Added: 64.100.176.0/20 -
```

The network engineers glance through the e-mail to see if any "incorrect" routes are added or deleted, either from a missing summary or a simple typo. If anything unusual appears, they can then investigate the cause.

The tool, which looks at the route table, has access to the master record of address allocations. As a result, if the route advertisement matches an address space allocation, the description from the database is appended to the route entry. This greatly improves the readability of the report.

Hierarchy Summary

A physical hierarchy is a prerequisite for a logical hierarchy. Allocating address space in a logical hierarchy allows summarization. This hierarchy and summarization is necessary to create a fundamentally stable network.

Step 5
Outage Root Cause Analysis

An important goal of Cisco's Networking team is to not take the same avoidable outage twice. The procedure is straightforward:

1. Identify the cause of the outage.
2. Fix the cause of the outage in the affected building.
3. Determine if other buildings are vulnerable.
4. If vulnerable, modify the network to prevent the outage in those other buildings.
5. Update design documentation to reduce the possibility that new deployments are vulnerable.

Because of workload, the tendency of network engineers is to fix the root cause in the affected building and then move on to other tasks. Management must follow up to make certain that similar outages are prevented in other buildings, and verify that design documentation is updated so that new deployments will not be vulnerable to the problem.

Obtaining Management Visibility

The OCC at Cisco is staffed 24 hours a day, every day, and is responsible for the following functions:

- Identifying when a business-impacting outage is in progress, either through monitoring software or through a phoned-in problem report.
- Categorizing the severity of the outage.
- Notifying the appropriate on-call personnel to resolve the technical issue.
- Escalating to management as appropriate, based on the severity and duration of the outage.

After a short-term fix is in place, the OCC staff:

- Periodically follows up with the resolver to verify that the root cause is identified.

- Periodically follows up with the resolver to verify a long-term fix is executed, if appropriate.
- Sends out a twice-daily e-mail summarizing all P1 business-impacting outages. The e-mail goes to the P1-recap e-mail alias to which any Cisco employee can subscribe. Cisco IT managers who supervise on-call personnel are strongly encouraged to subscribe to the P1-recap e-mail alias.

Priority and Outage Severity Definitions

Monitored priority is a predetermined indication of potential business impact. Monitored P1 and P2 devices, applications, and databases have been identified as having a potential significant business impact to Cisco. Therefore, P1 and P2 incidents require immediate response from support when contacted by incident managers, with the expectation that P1 incidents will be recovered within 2 hours and P2s within 4 hours.

Priority 1: Requires immediate response and resolution within 2 hours. P1 applications are defined as necessary for revenue processing; are used by more than 60 people; or are used by the executive staff. These applications must have a 24-hour on-call support, and when down, will result in a P1 ticket being opened and notification pages sent. P1 network equipment supports more than 100 people, a partner site during business hours, or access to any P1 server or application. A P1 ticket can be opened if there is a network outage, and several devices are affected that individually would be classified as P2 sites.

Priority 2: Requires response within 2 hours and resolution within 4 hours. P2 applications are used by a smaller client base and can, by definition, experience longer downtimes without affecting Cisco's ability to process revenue. P2 network equipment supports fewer than 100 people or supports access to P2 applications and servers.

Priority 3: Requires response within 1 day. P3 applications are used by a specific client group, but are either not vital to the ability to do their jobs or an easy workaround is possible. The application can have a significant downtime with no effect on productivity. P3 network equipment includes home ISDN, home Frame Relay, and console server networks.

Priority 4: Requires response within 2 days. P4 applications are typically in development or used very rarely and have no effect on revenue.

Outage Severity Definition

Severity is a measure of real business impact. Incidents where P1 or P2 monitored resources show unavailable are not always an indication of severe business impact. Severity is used to differentiate the expected response to the problem, based on priority, from the effect (the severity of business impact) realized by Cisco. The severity of a case is determined at the time of the incident based on the actual circumstances. It is measured for all P1 and P2 incidents managed by incident managers using the definitions given below:

	Definition	Examples
Severity 1	• Immediate and severe business impact • No workaround available	• Data center power outage • Complete campuswide network outage
Severity 2	• Adverse business impact • No workaround available	• Degraded critical system • Global manufacturing affected • Multiple applications on Cisco.com unavailable
Severity 3	• Low business impact • Workaround available in degraded mode	• Production content or code deployment unavailable • Localized effect
Severity 4	• Minor or no business impact • Workaround available	• Application load balanced • Redundant network service • After business hours outage for office services

Most P1s are severity 3 or severity 4. A severity 1 or severity 2 incident is very rare and inevitably results in visibility to high levels of management.

Sample P1-Recap E-mail:

Date: Mon Apr 7, 2003 5:43:55 AM US/Pacific
Subject: P1 Recap for the Morning of Monday April 7

Today we had 5 new P1s, 2 P1 updates, no P1 exceptions, and 13 P2s

P1s in brief:
Multiple files written to ECS host drno infected by the Lovegate Virus as of 01:00 PT (10:00 CET), next Update 07 Apr 08:00 PT
Eworklli app down on host ework since 19:38 PT, Next update 07 Apr 12:00 PT
Batch processing job fin_box_ai_daily missed its 21:00 PT SLA and completed at 21:10 PT
ECS view server smbview2 was down from 00:43 PT to 01:10 PT
Application Universe on host jane was down from 19:15 PT to 19:29 PT

P1 updates in brief:
Johannesburg, South Africa WAN links were down from 06 Apr 03:26 PT to 07 Apr 02:14 PT, the POP mailserver still not accessible since 06 Apr 03:36 PT.

Progeon, India has been experiencing intermittent problems using SOLCAT application as of 23:00 PT on the 25th of March. Next update 10:00 on the 7th of April.

P1s in detail:
SEVERITY 4 case no. 817113 Multiple files written to ECS host drno infected with Lovegate virus as of 01:00 PT. There is minimal impact as clients are currently able to access server. Support in the process of deleting infected files. Next update 07 Apr 08:00 PT. This case remains open.

SEVERITY 4 case no. 816732 Eworklli application down on host ework. The impact is minimal as only the search function of online collaboration tool is down; main function of uploading/downloading docs is working. Support investigating, monitoring stability of app. Next update 07 Apr 12:00 PT. This case remains open.

SEVERITY 3 case no. 816587 Batch processing job fin_box_ai_daily missed its 21:00 PT SLA and completed at 21:10 PT, It was impacting customer invoice printing and Rapid Revenue reporting. Support monitored the job to completion. This case is recovered.

SEVERITY 4 case no. 816969: The ECS view server smbview2 was unavailable from 00:43 PT to 01:10 PT. The impact to the engineers' ability to compile software and hardware development was minimal due to time of day. Support rebooted the server to restore services. This case is recovered.

SEVERITY 4 case no. 816494 Application Universe was down on the host jane from 19:15 PT to 19:29 PT. There was minimal impact to batch job processing due to the short duration of the outage. The application came up on its own without support intervention. This case is recovered.

P1 updates in detail:
SEVERITY 4 case no.816124. Johannesberg, South Africa WAN links was down from 06 Apr 03:26 PT to 07 Apr 02:14 PT. The clients have network connectivity again, after recovering from power outage. The POP mailserver still not accessible. EMEA Transport and Sysadmins investigating. This case remains open.

SEVERITY 4 case no.707465: Progeon, India has been experiencing intermittent problems using SOLCAT application as of 23:00 PT on the 25th of Mar. No impact to clients' ability to transact with customer orders at one site in India as workaround is in place. Support performing more onsite testing and investigating WAN latency. Next update 10:00 PT on the 7th of Apr. This case remains open.

Management Accountability

IT managers at Cisco present essential information at an operations review to their superiors once every quarter. Each layer of Cisco IT management presents an operations review, culminating in a quarterly operations review presented to the CEO. These periodic reviews of availability and P1 metrics at all levels of the management chain maintain focus on outage root cause resolution. The key information presented at operations reviews include:

- Network or application availability metrics
- P1 outage metrics (including number and severity)
- Detailed information on any severity 1 and severity 2 outages

Root Cause Analysis Example

Understanding root cause analysis requires network engineers to identify the problem, identify the cause, and then take steps to fix the problem and ensure that it doesn't happen in the future. The following example demonstrates each step of root cause analysis using a real case.

- **Review the problem report**—Users in building 12, fourth floor, who connected their laptops to the Ethernet network were unable to gain network connectivity. Other floors in that building experienced no problems. IP phones were unaffected, wireless network was unaffected, users already on the network were unaffected, and users with static IP addresses were unaffected. No network equipment was reported as down.
- **Identify the cause of the outage**—The problem was caused by a workstation on that network that was incorrectly configured as a Dynamic Host Configuration Protocol (DCHP) server. New computers on the network were unable to receive a valid DHCP address because the invalid DHCP server was responding to DHCP requests with invalid information.
- **Fix the cause of the outage in the affected building**—The unauthorized DHCP server was removed and service in the building was restored.
- **Determine if other buildings are vulnerable**—Other buildings are vulnerable because it is easy for people to incorrectly configure a workstation as a DHCP server. This outage type is particularly insidious because it is not automatically detected by our network management system.
- **Prevent the outage in other buildings**—Cisco deployed VLAN access control lists (VACLs) on all access layer switches, which prevented DHCP replies (User Datagram Protocol (UDP) port 68) from any hosts other than authorized DHCP servers and IT routers that were using IP helper functions. This was possible because the Cisco access layer switches are typically Cisco Catalyst 6500s with policy feature cards.
- **Update design documentation to make certain that new deployments are not vulnerable**—Cisco IT updated the Production Desktop Network documentation to include the VACL configuration as part of the standard configuration. As a result, all new desktop network deployments were invulnerable to the "rogue DHCP server" problem.

Step 6
Critical Devices on UPS

99.9 percent availability translates to 8.766 hours of downtime each year. Unplanned power outages will cause some of this downtime, but since Cisco's San Jose power grid is reasonably stable, it is unnecessary to have all devices on UPS to achieve 99.9 percent availability. It is, however, recommended to have critical devices, such as core routers, on UPS to accomplish the following:

- Prevent a localized power outage in buildings with core routers from resulting in a widespread outage.
- Help protect critical devices from power-surge-induced hardware failures.

Step 7
Provision Redundancy

Redundancy is critical to achieve 99.9 percent availability. Cisco provisions each Layer 2 switch with two separate paths back to distinct Layer 3 gateways, and designs the network so that each Layer 2 domain cannot be segmented due to a single failure. Each Layer 3 gateway is also provisioned with two distinct paths back to the redundant core.

When constructing buildings, each BDF is typically connected to two distinct NOCs using diverse paths whenever possible. NOCs should be interconnected with diverse fiber paths, labeling the fiber cans with "Diverse Path A" or "Diverse Path B."

When building WAN and MAN sites, two leased lines are used for connectivity, provisioning diverse paths when it is cost effective. Each redundant WAN/MAN gateway is uplinked through one of the diverse leased lines.

Step 8
Change Management

Change management provides a necessary communication mechanism to:

- Prevent unplanned change impact due to overlapping outages on related systems.
- Create a record of changes so support engineers can determine if a service outage is the result of a recent change.

To implement a change management process, the Cisco team created a logged e-mail alias that network team members could populate with “who, what, where, when, why” information regarding their planned change. Anyone who executes changes must subscribe to the alias to help prevent change conflicts, and should read the e-mail messages, even if the messages are filtered. Cisco IT Networking copies all network changes to the Cisco IT-LAN-CM e-mail alias to which all network team members, as well as critical contacts outside of networking, subscribe. A tool is also available to search through the past change management activities.

Step 9
Emergency Spares

Cisco’s LAN team in San Jose keeps at least one spare for each part deployed in the production network. From edge to core, the Cisco Catalyst 6500 Series greatly reduces the number of spares that must be kept on hand. Emergency spares are separated from general inventory and clearly labeled, enabling recovery from outages without waiting for a Return Materials Authorization (RMA) number. A junior network engineer is given the responsibility to periodically audit the spares kit.

Step 10
Out-of-Band Management

To minimize network outages, it is necessary to build a separate out-of-band management network. Cisco IT-LAN-SJ’s out-of-band network has the following characteristics:

- It is a flat, nonredundant network
- It uses static routing to connect to the production network
- It has its own DNS server
- Each production network device’s console is connected to a console server on the out-of-band network

The existence of the out-of-band network greatly decreases both planned and unplanned outage times because it allows many problems to be repaired remotely.

Summary: Achieving 99.9 Percent Availability

Achieving this level of uptime is not difficult but does require a fundamentally stable network. Cisco’s IT-LAN-SJ team followed the following steps to achieve this level of availability:

- Measure availability and actively use the reports both tactically and strategically
- Build a network with physical hierarchy
- Build a network with logical hierarchy
- Follow through with outage root cause analysis and remediation
- Put critical devices on UPS
- Build a redundant network
- Communicate and record changes with a simple change management system
- Provision emergency spares
- Build an out-of-band management network

Most of these steps are relatively simple. Building a network with redundancy, physical hierarchy, and logical hierarchy may require extensive work; however, it is impossible to achieve high levels of availability in a large network without hierarchy and redundancy.

Steps Cisco Took to Achieve 99.99% Network Availability

While 99.9 percent availability translates into 8.766 hours of downtime each year, 99.99 percent availability translates into less than 53 minutes of downtime each year for each device. One 15-minute global outage will cause Cisco to miss the quarterly availability target. While a fundamentally stable network should achieve 99.9 percent availability, 99.99 percent availability requires a more robust network.

In addition to the steps listed above (see 99.9 percent section), Cisco IT-LAN-SJ found the following steps necessary to achieving this level of availability:

- Proactive redundancy checking
- All devices on UPS
- Critical devices on generator
- Automated router configuration audits
- Change management integrated with availability monitoring
- Standardized code versions
- Troubleshooting training
- Separating incident management from problem resolution

STEP 1
Proactive Redundancy Checking

To achieve 99.9 percent availability, the Cisco San Jose network was already built with redundancy. However, over time, some of the redundant links will fail or be accidentally misconfigured. If these link failures are not detected and fixed, it is possible that the second link will fail at some point resulting in an impacting outage. Imagine having to report a root cause analysis with the following message: “Two months ago our redundant link failed. This failure was not detected. Yesterday the other link failed, resulting in an outage.”

When 8.7 hours of downtime are allowed, these outages are acceptable. But when only 53 minutes of downtime are allowed each year, these outages must be prevented.

Cisco runs a Perl script each week to verify that each Layer 2 switch has two separate paths back to distinct routers; and each Layer 3 router has two separate paths back to the core.

While not perfect, given the network design where most Layer 2 switches are directly connected to Layer 3 gateways, almost all “undetected loss of redundancy” outages have been eliminated. The script also has the ability to specify certain devices as “known nonredundant devices”. To maintain visibility, the redundancy report lists all the “known nonredundant devices,” in a separate section. Following is a sample redundancy check e-mail:

Date: Tue Apr 1, 2003 2:21:36 AM US/Pacific
Subject: Redundancy Report

```
Redundancy Report

Devices in EMAN with a pager contact of it-lan-sj-duty and a priority of 2 or higher which do not have layer
2 redundancy to other devices with the same pager contact. Connectivity based on CDP data.

Terminal Servers, Distributed Directors, RSMs and Hybrid MSFCs are excluded from the report
2 pls1-00lab-sw1          lanswitch
2 sjcc-12mc-sw1           lanswitch
1 sjcm-21-sw2             lanswitch

Known nonredundant devices:
1 pmr-00-sw1              lanswitch
2 sjc1-00cn-sw1           lanswitch
2 sjc10-00cn-sw1          lanswitch
2 sjc11-00cn-sw1          lanswitch
2 sjc12-00cn-sw1          lanswitch
2 sjc12-42cn-sw1          lanswitch
2 sjc13-00cn-sw1          lanswitch
2 sjc14-00cn-sw1          lanswitch
2 sjc15-00cn-sw1          lanswitch
2 sjc16-00cn-sw1          lanswitch
2 sjc17-00cn-sw1          lanswitch
2 sjc18-00cn-sw1          lanswitch
2 sjc19-00cn-sw1          lanswitch
2 sjc20-00cn-sw1          lanswitch
2 sjc21-00cn-sw1          lanswitch
2 sjc22-00cn-sw1          lanswitch
2 sjc23-00cn-sw1          lanswitch
2 sjc24-00cn-sw1          lanswitch
2 sjc3-00cn-sw1           lanswitch
2 sjc4-00cn-sw1           lanswitch
2 sjc5-00cn-sw1           lanswitch
2 sjc6-00cn-sw1           lanswitch
2 sjc7-00cn-sw1           lanswitch
2 sjc8-00cn-sw1           lanswitch
2 sjc9-00cn-sw1           lanswitch
2 sjca-00cn-sw1           lanswitch
2 sjcb-00cn-sw1           lanswitch
2 sjcc-00cn-sw1           lanswitch
2 sjcd-00cn-sw1           lanswitch
2 sjce-00cn-sw1           lanswitch
2 sjcf-00cn-sw1           lanswitch
2 sjcg-00cn-sw1           lanswitch
2 sjch-00cn-sw1           lanswitch
2 sjci-00cn-sw1           lanswitch
2 sjcj-00cn-sw1           lanswitch
2 sjcj-trailer-sw1        lanswitch
2 sjck-00cn-sw1           lanswitch
2 sjcl-00cn-sw1           lanswitch
2 sjcm-00cn-sw1           lanswitch
2 sjcn-00cn-sw1           lanswitch
2 sjco-00cn-sw1           lanswitch
2 sjcp-00cn-sw1           lanswitch
<br>Report Generated: Tue Apr 1 2:21:36 US/Pacific 2003
```

Step 2
All Devices on UPS

Given that only 53 minutes of outage time are acceptable each year, all network devices must be on UPS to achieve 99.99 percent availability. Cisco designates 2 hours of UPS power for each network device. This is particularly important because the Cisco IP telephones provide 911 (emergency) service. Cisco policy requires evacuation of a building if the UPS fails because of the inability to dial 911 in those circumstances.

Step 3
Critical Devices on Generator

To prevent extended power outages in core buildings from causing widespread outages, Cisco IT-LAN-SJ puts core network devices on generator power.

Step 4
Automated Router Configuration Audits

Cisco uses the Router Audit Tool (RAT) from www.cisecurity.org to enforce our standard configurations. This has two major consequences:

- We have a documented standard configuration
- Our routers are compliant with our documented standard configuration

The discipline of having a documented standard configuration is beneficial to the network team. When root cause analysis results in recommended configuration changes, having a standard, automatically-audited configuration improves compliance to those configuration improvements.

Every week a "Bottom 10" report is generated listing the 10 routers least compliant to Cisco standards, based on RAT reports, as well as the 10 configuration rules most commonly violated. Following is a sample Bottom 10 report:

```
Date: Tue Apr 8, 2003 6:15:29 AM US/Pacific
Subject: RAT_Bottom_10_Report_For_it-lan-sj-duty

Bottom 10 report for it-lan-sj-duty custom configuration file
Hostname                  Score     Owner          Weeks-in-bottom-10-list
softoken-test.cisco.com   75        [removed]      23
pmr-gw1.cisco.com         85        [removed]      8
sjcd-00-cs1.cisco.com     85        [removed]      6
wlshb-gw1.cisco.com       85        [removed]      8
sjc12-00-gw2.cisco.com    86        [removed]      7
sjca-12-cs1.cisco.com     86        [removed]      7
wlshd-gw1.cisco.com       87        [removed]      7
sjce-00-gw1.cisco.com     89        [removed]      4
sjc16-00-gw2.cisco.com    89        [removed]      3
sjc15-00-gw2.cisco.com    89        [removed]      1

Most commonly failed rules for it-lan-sj-duty custom configuration file
133     tacacs-server timeout 3
40      udld enable
33      ip igmp snooping
27      no class-map match-any http-hacks
22      exec-timeout 300 0 (line vty)
22      ip ssh time-out 30
21      ip name-server 171.68.226.120
21      logging source-interface loopback0
19      no ip source-route
18      snmp-server community xxxxxx ro 90
```

Step 5
Change Management Integrated with Availability Monitoring

When 8.7 hours of downtime each year is acceptable, it is unnecessary to differentiate planned and unplanned outages. There is sufficient leeway to absorb the planned outages and still achieve 99.9 percent availability. To achieve 99.99 percent availability, however, it is necessary to distinguish between planned and unplanned outages. To do this, Cisco's change management system requires network engineers to provide the following information when scheduling a change:

- The timeframe of the planned change
- The devices affected by the change

While raw availability is calculated normally, for purposes of adjusted availability, devices listed in the change request are considered 100 percent operational during the change window. In addition to enabling accurate data regarding raw and adjusted availability, this system has the side benefit of forcing a high degree of discipline on network engineers when they plan outages. The failure of the network engineer to list all affected devices will result in an availability hit and possibly a P1 being opened by the OCC.

A standard naming convention is extremely helpful in change planning. The name of every network device in Cisco starts with the building identifier. For example, sjc12-31-sw2 is in San Jose, building number 12, 3rd floor, IDF number 1. It is the second switch in that room. Consider a planned power outage for building 12. A network engineer needs to make certain that every device starting with "sjc12-" is included in the change request. This greatly reduces the possibility of missing a device when planning a change. If a device is missed the device will experience an "unplanned outage" during the change window. A good naming convention can greatly decrease this type of error.

Integrating change management with availability calculations allows accurate measurement of raw and adjusted availability, which represents planned and unplanned downtime. Measuring both planned and unplanned downtime encourages the network team to use discipline when planning their network changes. It also encourages the team to minimize planned outages in data center environments because even planned outage time gets management visibility. A standard naming convention makes it much easier to identify devices impacted by a change.

Step 6
Standardized Code Versions

It is possible for Cisco IT-LAN-SJ to achieve 99.9 percent availability using "random" Cisco IOS Software versions because the failure to consciously pick versions that have undergone rigorous testing will result in only a few additional unplanned outages. This meets the 8.7 hours of acceptable downtime and still enables 99.9 percent availability without the extra work of choosing and upgrading to specific Cisco IOS Software releases.

However, 99.99 percent availability requires selection of specific Cisco IOS Software and Cisco Catalyst OS Software releases to achieve. The general rules are to:

- Pick a version with the required features.
- Pick a specific release with the largest number of bug fix rebuilds since the last feature was integrated.
- Avoid "deferred" images. (Deferred images are listed in a separate section on the www.cisco.com Cisco IOS Software upgrade planner Web page).
- Avoid "software advisory" images. (A warning will appear on www.cisco.com prior to allowing you to download an image with a software advisory).

Following are the Cisco IOS Software version "tactics" Cisco IT-LAN-SJ uses to choose specific software releases:

Cisco IOS Software Release 12.2T IOS Train Tactics—As of April 2003, Cisco IOS Software 12.2T is the latest technology train, where the latest features are introduced. Since many features were recently introduced, the technology train has a lower level of maturity. If Cisco IT does not require technology train features, then another Cisco IOS Software train (such as 12.2 mainline) is chosen.

Consider a Cisco 2621XM Multiservice Router that requires basic IPv6 functionality. Because of the IPv6 requirement, you must run the Cisco IOS Software 12.2T train. As of April 2003, the following 12.2T versions are available:

Version	Description
12.2(15)T	First release of new 12.2(15)T features
12.2(13)T3	Third rebuild of 12.2(13)T features
12.2(13)T1	First rebuild of 12.2(13)T features
12.2(13)T	First release of new 12.2(13)T features
12.2(11)T6	Sixth rebuild of new 12.2(11)T features
12.2(11)T5	Fifth rebuild of new 12.2(11)T features
12.2(11)T3	Third rebuild of new 12.2(11)T features
12.2(11)T2	Second rebuild of new 12.2(11)T features
12.2(11)T1	First rebuild of new 12.2(11)T features
12.2(11)T	First release of new 12.2(11)T features
12.2(8)T8	Eighth rebuild of new 12.2(8)T features
12.2(8)T5	Fifth rebuild of new 12.2(8)T features
12.2(8)T4	Fourth rebuild of new 12.2(8)T features
12.2(8)T3	Third rebuild of new 12.2(8)T features
12.2(8)T2	Second rebuild of new 12.2(8)T features
12.2(8)T1	First rebuild of new 12.2(8)T features
12.2(8)T	First release of new 12.2(8)T features
12.2(4)T5	Fifth rebuild of new 12.2(4)T features
12.2(4)T3	Third rebuild of new 12.2(4)T features
12.2(4)T1	First rebuild of new 12.2(4)T features
12.2(2)T4	Fourth rebuild of new 12.2(2)T features
12.2(2)T	First release of 12.2(2)T features

Note: You will notice that some versions and rebuilds are missing. There are two reasons for this:

- Some rebuilds fix specific bugs with specific platforms. If a rebuild is for a Cisco 3640-specific bug, the rebuild will not be compiled for the Cisco 2621.
- Cisco periodically removes old images from Cisco.com—typically when they are 6 to 9 months old and a more recent rebuild is available.

Because each rebuild has bug fixes but no new features, the first tactical decision is to remove all but the most recent rebuilds from consideration. This leaves the following versions under consideration:

Version	Description
12.2(15)T	First release of 12.2(15)T features
12.2(13)T3	Third rebuild of 12.2(13)T features
12.2(11)T6	Sixth rebuild of 12.2(11)T features
12.2(8)T8	Eighth rebuild of 12.2(8)T features
12.2(4)T5	Fifth rebuild of 12.2(4)T features
12.2(2)T4	Fourth rebuild of 12.2(2)T features

None of these releases have a deferral or software advisory against it. Since all of these releases have the required features, the releases with the highest rebuild numbers would probably be best, for example 12.2(8)T8 or 12.2(11)T6.

Cisco IOS Software Release 12.2 Mainline Tactics—The Cisco IOS Software 12.2M train's primary purpose is stability. Virtually the only code changes in Cisco IOS Software 12.2M are bug fixes. Almost no new features are integrated into the mainline train. Consider a Cisco 2621XM where the features you need are included in the Cisco IOS Software 12.2M train.

As of April 2003, the following versions are available. Only the most recent rebuilds in each release are included:

Version	Description
12.2(16)	First release of 12.2(16)
12.2(13b)	Second rebuild of 12.2(13)
12.2(12c)	Third rebuild of 12.2(12)
12.2(10b)	Second rebuild of 12.2(10)
12.2(7c)	Third rebuild of 12.2(7)
12.2(6i)	Ninth rebuild of 12.2(6)
12.2(5d)	Fourth rebuild of 12.2(5)
12.2(3d)	Fourth rebuild of 12.2(3)
12.2(1d)	Fourth rebuild of 12.2(1)

As with the Cisco IOS Software Release 12.2T train, the rebuilds are bug fixes only. However, the releases are fundamentally different from the Cisco IOS Software Release 12.2T. Mainline trains, such as Cisco IOS Software Release 12.2M, rarely integrate new features.

Release vs. Rebuild: A release generally includes a larger number of bug fixes and undergoes full regression testing. A rebuild includes a handpicked set of additional bug fixes. To enable quick release of bug fixes, rebuilds do not undergo full regression testing.

A good rule of thumb for mainline releases is to use one of the last two releases. In this case that would mean one of the following:

Version	Description
12.2(16)	First release of 12.2(16)
12.2(13b)	Second rebuild of 12.2(13)

The advantage of Cisco IOS Software 12.2(16) is that it includes all of the most recent bug fixes and has undergone full regression testing. The advantage of Cisco IOS Software Release 12.2(13b) is that Cisco IOS Software Release 12.2(13) underwent regression testing, and since then only a handpicked set of bug fixes have been integrated.

Cisco IOS Software 12.1T Technology Train Tactics—Cisco IOS Software 12.1T is the "old" technology train used to create the Cisco IOS Software 12.2 mainline code. Cisco IOS Software 12.1T features are included in Cisco IOS Software 12.2 mainline with much greater maturity because Cisco IOS Software 12.2M has undergone only bug fixes for an extended period of time. Because the features of Cisco IOS Software 12.1T are available in the more mature Cisco IOS Software 12.2 mainline, using Cisco IOS Software 12.1T code versions is not recommended.

Cisco IOS Software Release 12.1M Mainline Train Tactics—For improved quality, Cisco recommends the "old" mainline train because it has been several years since a major feature was integrated into this code base. Starting with Cisco IOS Software 12.1(13), this code has earned the label of "General Deployment (GD)", which means that it is considered to have the highest level of reliability.

Once code reaches General Deployment (GD) status, every release undergoes full regression testing. This is why starting with Cisco IOS Software 12.1(13) there are no "rebuild" releases with a Cisco IOS Software 12.1(13a) naming scheme. In 12.1 mainline, the most recent version is 12.1(19) (as of April 2003).

Cisco IOS Software 12.1E Enterprise Train Tactics (Version 12.1(14)E and Earlier)—Cisco IOS Software 12.1E is known as the "enterprise train," which is a Cisco IOS Software train optimized for enterprises. Although it has some new features needed by enterprises, it minimizes those new features to maximize quality. As of April 2003, the Cisco IOS Software 12.1E train is the primary train supporting the Multilayer Switch Feature Card (MSFC) on the Cisco Catalyst 6500, making it critical for Cisco IT-LAN-SJ which uses Cisco Catalyst 6500s as the edge to core platform.

As of April 2003, the following Cisco 12.1E IOS Software releases are available on Cisco.com. For clarity, only the most recent rebuilds of each feature release are shown:

Version	Description	Based on Mainline Version
12.1(13)E5	Fifth rebuild of 12.1(13)E feature release	12.1(13)
12.1(12c)E5	Fifth rebuild of 12.1(12c) feature release	12.1(12c)
12.1(11b)E7	Seventh rebuild of 12.1(11b) feature release	12.1(11b)
12.1(11b)EX1	First rebuild of 12.1(11b)EX feature release	12.1(11b)
12.1(8b)E13	Thirteenth rebuild of 12.1(8b)E feature release	12.1(8b)
12.1(8b)EX5	Fifth rebuild of 12.1(8b)EX feature release	12.1(8b)
12.1(8a)E5	Fifth rebuild of 12.1(8a)E feature release	12.1(8a)
12.1(5c)EX3	Third rebuild of 12.1(5c)EX feature release	12.1(5c)

Note 1: There are two ways to integrate a bug fix into the Cisco IOS Software 12.1E train:

- The bug fix can be directly integrated into a Cisco IOS Software 12.1E release or rebuild.
- The bug fix can be integrated into Cisco IOS Software 12.1 mainline. Each Cisco IOS Software 12.1E release is based on a mainline release.

For example, a bug fix integrated in Cisco IOS Software 12.1(11b) mainline will also end up in Cisco IOS Software 12.1(11b)E. But a bug fix integrated directly into Cisco IOS Software 12.1(11b)E2 would not necessarily be integrated into any Cisco IOS Software 12.1 mainline release, which would be appropriate when the bug is specific to a 12.1E feature.

Note 2: There are two separate trains—Cisco IOS Software 12.1E, the enterprise train, and Cisco IOS Software 12.1EX, which consists of temporary offshoots of the Cisco IOS Software 12.1E train to introduce major new features. For example, a copy of Cisco IOS Software 12.1(8b)E was used to create Cisco IOS Software 12.1(8b)EX. Network Analysis Module (NAM) support was initially added in 12.1(8b)EX, then the NAM support was reintegrated into the enterprise train in Cisco IOS Software 12.1(11b)E.

This mechanism of temporarily creating new trains allows major new features to undergo rigorous testing prior to introduction into the primary enterprise train. Meanwhile minor new features are added directly to the enterprise train.

When picking a specific version to deploy, the rules are similar to the technology train:

- Avoid versions that are deferred or in software advisory status.
- Avoid EX releases unless you need the specific feature integrated into that release.
- Only consider the latest rebuild of each feature release.

This leaves the following versions to consider:

Version	Description	Based on Mainline Version
12.1(13)E5	Fifth rebuild of 12.1(13)E feature release	12.1(13)
12.1(12c)E5	Fifth rebuild of 12.1(12c) feature release	12.1(12c)
12.1(11b)E7	Seventh rebuild of 12.1(11b) feature release	12.1(11b)
12.1(8b)E13	Thirteenth rebuild of 12.1(8b)E feature release	12.1(8b)
12.1(8a)E5	Fifth rebuild of 12.1(8a)E feature release	12.1(8a)

If this were a technology train, Cisco IOS Software 12.1(8b)E13 would be a clear choice for stability, based on the number of rebuilds. The enterprise train, however, limits new features to improve quality. As a result, all of these versions would probably be robust. It is usually wise, however, to avoid the first few rebuilds of a new release if possible.

Cisco IOS Software 12.1E Enterprise Train Tactics (Cisco IOS Software 12.1(19)E and Later)—Starting with Cisco IOS Software 12.1(19)E, the Cisco IOS Software 12.1E train will stop integrating new features and will become a “bug fix only” train, behaving like a mainline train. Follow the rules for Cisco IOS Software 12.1 mainline and Cisco IOS Software 12.2 mainline (the latest release is probably the best).

Cisco Catalyst OS Tactics

Cisco Catalyst OS versions are numbered in the following format: Cisco Catalyst OS 1.2(3). In this example, the release train is “1,” the feature release within that train is “2,” and the bug fix release is “3.” Any time a new feature is added the feature release number is incremented.

Cisco Catalyst OS 5.X—As of April 2003, the latest 5.X Cisco Catalyst OS release is 5.5(19). No new features have been integrated since Cisco Catalyst OS 5.5(1). As of Cisco Catalyst OS 5.5(7), this code is considered GD. As a result, this is extremely mature code and the latest release will be effective. The only problem is that there is a high probability that you will need features in a later train.

Cisco Catalyst OS 6.X—As of April 2003, the latest 6.X Cisco Catalyst OS release is Cisco Catalyst OS 6.4(2). Although this is only the first bug fix of the Cisco Catalyst OS 6.4(1) feature release, only two minor features were integrated into Cisco Catalyst OS 6.4(1). As a result, the latest Cisco Catalyst OS 6.4 code has a high degree of maturity. It is Cisco's intention to close Cisco Catalyst OS 6.X for new features and move toward GD status for this train.

Cisco Catalyst OS 7.X—Cisco Catalyst OS 7.X is the current release train being used for new features. As a result there are a relatively low number of bug fix releases between each feature release. As of April 2003, the following are the most recent bug fix releases of feature releases:

Version	Description	Release Date
7.5(1)	First release of 7.5(1) features	Dec 31, 2002
7.4(3)	Second bug fix of 7.4(1) features	Dec 6, 2002
7.3(2)	First bug fix of 7.3(1) features	Aug 2, 2002
7.2(2)	First bug fix of 7.2(2) features	June 4, 2002
7.1(2)	First bug fix of 7.1(1) features	Feb 9, 2002

If you need features in the Cisco Catalyst OS 7.X train, it is best to treat it like a technology train. Go with the version with the highest number of bug fixes and avoid versions with old release dates. For example, Cisco Catalyst OS 7.3(2)'s release date of August 2, 2002 indicates that it is not actively being maintained. Any bugs identified in Cisco Catalyst OS 7.3(2) will probably result in the bug fix being integrated into the latest version, Cisco Catalyst OS 7.5.X, for example.

In this case, Cisco Catalyst OS 7.4(3) would probably be the best choice for a switch, which requires Cisco Catalyst OS 7.x features.

Cisco IOS Software Release Categories

- **Early Deployment (ED) Releases**—Cisco IOS ED releases are vehicles that bring new development to the marketplace. Each maintenance revision of an ED release includes not only bug fixes, but also a set of new features, new platform support, and general enhancements to protocols and the Cisco IOS Software infrastructure. Every 1 to 2 years, the features and platforms of the ED releases are ported to the next mainline Cisco IOS Software release.

- **Limited Deployment (LD) Releases**—This is the phase of Cisco IOS Software maturity between first customer shipment (FCS) and general deployment for main releases.

- **General Deployment (GD) Releases**—At some point during the release life cycle, Cisco will declare a major release to be ready for GD certification. Only a major release can achieve GD status. It meets the GD certification milestone when Cisco is satisfied that the release has been:

  – Proven through extensive market exposure in diverse networks;

  – Qualified by metrics analyzed for stability and bug trends;

  – Qualified through customer satisfaction surveys; and

  – Proven a reduction in the normalized trend of customer-found defects in the release over the previous four maintenance releases.

A customer advocacy GD certification cross-functional team composed of Cisco Technical Assistance Center (TAC) engineers, Advanced Engineering Services (AES) engineers, System Test Engineering, and Cisco IOS Software Engineering is formed to evaluate every outstanding defect of the release. This team gives the final approval for GD certification. Once a release attains GD status, every subsequent revision of the release is also GD.

Consequently, once a release is declared GD, it automatically enters the restricted maintenance phase. While in this phase, engineering modification of the code, including bug fixes with major code rework, is strictly limited and controlled by a program manager. This ensures that no adverse bug is introduced to a GD-certified Cisco IOS Software version. GD is achieved by a particular maintenance version.

Subsequent maintenance updates for that release are also GD releases. For example, Cisco IOS Software Release 12.0 received the GD certification at Cisco IOS Software Release 12.0(8). Thus, Cisco IOS Software Releases 12.0(9), 12.0(10), and so on are GD releases.

For additional information on the Cisco IOS Software lifecycle, see:

http://www.cisco.com/go/IOS

Cisco IOS Safe Harbor

The goal of Cisco IOS Safe Harbor is to provide improved network stability, reliability, and performance with respect to Cisco IOS Software. Safe Harbor involves testing the feature sets and protocols in a particular Cisco IOS Software Release 12.1 E image on the Cisco Catalyst 6500 platform to provide high quality code for the financial services business. This combination of features, hardware, and image is tested in a laboratory environment that simulates the financial services business network environment using regularly updated topologies and configurations provided by the financial customer. For details of the Cisco Safe Harbor program, see: http://www.cisco.com/univercd/cc/td/doc/solution/systest/safehbr/.

Cisco IOS Software Category Summary

When picking Cisco IOS Software releases for reliability, General Deployment and Limited Deployment releases are best. Some Cisco Cat6K IOS Software releases undergo additional safe harbor testing.

"Recommended" Versus "Acceptable"

Cisco IT-LAN-SJ recognizes the concept of a recommended version and a list of acceptable versions. Network engineers use the recommended version if they deploy a new device. Acceptable versions are versions other than the recommended, but that do not require immediate upgrade. If a critical bug is identified in an acceptable version, then the version is removed from the acceptable list, which requires any devices running that version to be upgraded promptly.

Periodically Review Code Versions

Cisco IT-LAN-SJ chooses new recommended versions under two circumstances:

1. When a critical bug is found in the current recommended version—In this case, the previous recommended version becomes unacceptable, requiring prompt upgrades.
2. Every 3 to 6 months the recommended versions are reviewed and updated. In this case the previous recommended version will usually be moved to acceptable status.

Crash upgrade projects, where large numbers of devices need to be upgraded in a short time, are demoralizing. These crash upgrade projects are caused when the recommended version goes directly to unacceptable due to a critical bug. The goal is to minimize crash upgrades by having two to three acceptable versions and gradually upgrading devices to the latest recommended version—preferably during other required work.

Exceptions That Require Different Versions

How to unify Cisco IOS Software releases when a small number of devices require new technology train features is a constant struggle. Should Cisco IOS Software releases be unified by running all routers on the technology train? Or should 90 percent of routers be run on mainline train, and only the exceptions run on the technology train?

Consider a case where you have 100 routers, 10 of which require 12.2T features.

The two choices are:

1. 100 routers on Cisco IOS Software 12.2T
2. 90 routers on Cisco IOS Software 12.2M. 10 routers on Cisco IOS Software 12.2T

If the Cisco IOS Software 12.2T Routers need to be upgraded every quarter, solution number 1 results in 100 upgrades every quarter. But if Cisco IOS Software 12.2M Routers require upgrades every three quarters, solution number 2 will result in 40 upgrades every quarter. By accepting the cost of having two standards, the time spent executing Cisco IOS Software upgrades is reduced by 60 percent. While having two versions does impose an additional support cost, the cost is relatively minor. As a result Cisco IT-LAN-SJ uses mainline code where possible. Only the few routers that require technology-train features run the Cisco IOS Software Release 12.2T train.

Step 7
Troubleshooting Training

An ironic problem of achieving 99.99 percent availability is that there are not enough outages to keep troubleshooting skills sharp. When availability is poor, no special troubleshooting training is needed. But when availability reaches 99.99 percent, it is necessary to conduct periodic troubleshooting exercises. Cisco IT-LAN-SJ holds separate administrative and technical weekly meetings. Periodically, the technical meeting consists of engineers repairing a laboratory network that has been deliberately broken. Although not a perfect solution, this troubleshooting training helps to keep troubleshooting skills sharp despite the "problem" of not having enough network outages.

Step 8
Separating Incident Management from Problem Resolution

During a network outage, Cisco IT serves two functions:

- Resolving the network outage
- Managing communications and escalations regarding the incident

Cisco IT separates these functions into two separate groups. Cisco IT-LAN-SJ is responsible for resolving the network outage, and the OCC staff manages the incident.

The OCC is staffed 24 hours a day, every day with a team whose primary function is to detect P1 and P2 service outages (either through our network management system or through a customer problem report). The OCC staff does not attempt to resolve the issue. Instead, the OCC pages out to the appropriate support teams. A LAN problem in San Jose would be paged out to the Cisco IT-LAN-SJ duty person.

The OCC will open up a conference bridge and have the appropriate duty people join the conference bridge. If needed, the OCC staff will contact vendor support (including Cisco TAC) and connect them with the conference bridge. The OCC staff will determine the severity of the problem and send notifications to management. At predetermined intervals based on the severity of the incident, the OCC staff will escalate the incident to management. Management will determine whether additional technical personnel are needed to resolve the incident.

After an incident, the OCC staff will follow up to verify that the root cause is identified and that a long-term-fix (if appropriate) is implemented to prevent recurrences of the problem.

Putting notifications and escalations in the hands of the OCC staff frees the network engineers to concentrate on resolving the technical problem. It also ensures that notifications and escalations will occur in a consistent manner. The OCC also facilitates the prevention of outages by following up on root cause analysis and long-term fix activities. The end result of the separation of incident management from problem resolution is improved service and decreased outage time.

Steps Cisco Took to Achieve 99.999% Availability

- Achieving 99.9 percent availability (8.7 hours of downtime each year) requires a good, stable network.
- Achieving 99.99 percent availability (53 minutes of downtime each year) requires an even more robust network.
- Achieving 99.999 percent availability (315 seconds of downtime each year or less than 1 second each day) requires an essentially perfect network.

For Cisco IT, where the availability of each device is determined every 15 to 20 seconds, each device is allowed to miss one availability measurement every 3 weeks. This is an extremely difficult level of availability to reach.

To achieve 99.999 percent availability in a LAN, Cisco IT recommends all the steps required for 99.9 percent and 99.99 percent availability, plus the following three steps:

Step 1
All Devices on Generator Emergency Power

It is impossible to achieve less than 1 second of downtime on each device every day while suffering unplanned power outages. In areas where Cisco IT-LAN-SJ targets 99.999 percent availability, Cisco puts every device on UPS and on generator backup to avoid the effects of a power outage.

Step 2
Automated Switch Configuration Checking

To achieve 99.99 percent availability, the Cisco IT-LAN-SJ team developed a router standard configuration and automated configuration checking with the RAT from www.cisecurity.org.

99.999 percent availability requires a switch standard configuration that must be proactively audited, preferably in an automated fashion. Cisco IT-LAN-SJ also uses RAT with a modified configuration file to audit switch configuration files.

Step 3
Semi-Annual Manual Auditing

Even the most intelligent automated redundancy and configuration audit tools cannot address all possible contingencies. To achieve 99.999 percent availability, Cisco IT-LAN-SJ is starting to manually audit all connectivity, topology, network maps, and configurations at least once every 6 months. In particular, it is critical to verify that the logical and physical hierarchy deployed to achieve 99.99 percent availability remains in place.

Cisco-Specific Tactics That Improved Production Availability

In addition to the steps outlined in the previous availability sections, separating the production and alpha networks, and using your existing support organization will help to improve production availability.

Separation of Production and Alpha Networks

As a networking company, the goals of the Cisco IT Networking organization are to:

1. Provide a reliable network for the company

2. Be an example enterprise network for our customers

3. Be our first, best, and toughest customer

Goal number 1, to provide a reliable network, requires Cisco to run tested code and platforms in an effort to achieve high availability. However, Goal number 3, being our own first, best, and toughest customer, requires Cisco to run prerelease code on prerelease hardware to make Cisco products better for our customers. At first glance, these goals appear mutually exclusive.

The solution is to run two parallel networks—the production network and the alpha network. The production network is patched to two network jacks in every office or cubicle. The alpha network is patched to one network jack, usually orange, in approximately 40 percent of the San Jose campus. Cisco attempts to put developers on the alpha network for the product they are developing. Engineers are encouraged to patch into the alpha (orange) network jack by periodic automated audits, the results of which are sent to management.

The production and alpha networks are both connected by static routing at a demarcation point. Whereas the production network has stringent change management procedures, the alpha network has minimal change management procedures—even allowing changes during business hours if it's necessary to enable development. The only requirement is to send an e-mail message to the affected building telling employees to repatch to the production network for a few hours.

This separation of production and alpha networks allows the production network to attain excellent availability while enabling Cisco to test products internally prior to release.

Technical Assistance Center Support

As part of being Cisco's first customer, Cisco IT uses the same support mechanisms as do our customers, including procuring equipment internally through www.cisco.com and using the Cisco Technical Assistance Center (TAC) to debug an issue. This strategy works on both a cost-effective level and a tactical level because TAC and Cisco IT-LAN have different skill sets. Cisco TAC engineers are professional troubleshooters, trained to debug whatever network they encounter. Cisco IT-LAN is trained to build a specific reliable network and concentrate on preventing problems. Cisco IT-LAN also uses Cisco Advanced Services (see http://www.cisco.com/en/US/products/svcs/ps11/serv_category_home.html) to assist with network design and Cisco IOS Software version selection.

Cisco IT-LAN-SJ's Compliance with the Above Recommendations

The steps to achieve 99.999 percent availability can be cost prohibitive if integrated without planning. Although Cisco IT has executed many of the steps above, not all have been implemented in all areas due to cost-benefit considerations. For example, some areas of our network, such as laboratory networks, are considered less important than other areas such as data centers. Therefore, the cost-benefit calculation of high availability versus cost is different in each area of the network. A summary of the steps taken by the Cisco IT-LAN-SJ in each area follows. In addition, we repeat the adjusted availability achieved in each area for reference.

The attached chart provides an overview of the 2002 adjusted availability for each subgroup managed by the Cisco IT-LAN-SJ team, as well as the steps that have been deployed to achieve high availability in each area.

Calendar Year 2002 Adjusted Availability

Subgroup	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	Call Manager Network	Site 1–3 Desktop	Site 4 Desktop	Site 5 Desktop	MAN Desktop	Lab
2002 Adjusted Availability %	99.997	99.996	99.995	99.991	99.992	99.998	99.997	99.998	99.993	99.991	99.995	99.991	99.973

99.9% Steps

Measure Availability	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Outage Alerts	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Physical Hierarchy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Logical Hierarchy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Root Cause Analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Critical Devices on UPS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Provision Redundancy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Change Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Emergency Spares	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Out-of-band Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

99.99% Steps

Subgroup	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	Call Manager Network	Site 1–3 Desktop	Site 4 Desktop	Site 5 Desktop	MAN Desktop	Lab
Proactive Redundancy Checking	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
All Devices on UPS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes
Critical Devices on Generator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Automated Router Configuration Audits	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Change Management Integrated with Availability Monitoring	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Standardized Code Versions	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Troubleshooting Training	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Separate Incident Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

99.999% Steps

All devices on generator	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
Automated switch configuration audits	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Semi-annual manual auditing	No	No	No	No	No	No	No	No	No	No	No	No	No

Availability has continued to improve overall to 99.995 percent. Following is the 12-month rolling average (July 2002 through June 2003):

Subgroup	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	CM Network	Site 1–3 Desktop	Site 4 Desktop	Site 5 Desktop	MAN Desktop	Lab
July 2002 to June 2003 Adjusted Availability %	99.999	99.997	99.997	99.998	99.999	99.998	99.998	100.000	99.996	99.994	99.998	99.996	99.987

Number of devices per subgroup in June 2003 (November 2002 for DDC5)

Subgroup	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	CM Network	Site 1–3 Desktop	Site 4 Desktop	Site 5 Desktop	MAN Desktop	Lab
Number of devices	26	10	72	11	10	5	23	17	166	374	78	39	39

Monthly Adjusted Availability Statistics for January 2002 through June 2003

Subgroup	Overall	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	CM Network	Site 1–3 Desktop	Site 4 Desktop	Site 5 Desktop	MAN Desktop	Lab
Jan 2002	99.998	100.000	99.999	99.996	99.999	99.997	99.999	99.998	99.999	99.998	99.998	99.996	99.999	99.998
Feb 2002	99.985	99.992	99.999	99.999	99.931	99.946	99.991	99.996	99.993	99.995	99.991	99.993	99.997	99.980
Mar 2002	99.994	99.998	99.992	99.999	99.989	99.990	99.997	99.994	99.995	99.991	99.999	99.988	99.995	99.979
Apr 2002	99.992	99.989	99.999	99.987	99.994	99.993	99.999	99.999	100.000	99.998	99.997	99.989	99.960	99.968
May 2002	99.994	99.998	99.999	99.994	99.999	99.999	99.998	99.998	99.998	99.969	99.994	99.997	99.990	99.892
June 2002	99.987	99.991	99.975	99.980	99.993	99.993	99.994	99.997	99.990	99.989	99.975	99.985	99.985	99.984
July 2002	99.999	99.999	99.999	100.000	100.000	100.000	99.999	100.000	100.000	100.000	99.999	99.997	99.999	99.999
Aug 2002	99.999	99.997	100.000	100.000	99.999	99.999	99.998	100.000	100.000	100.000	100.000	99.999	100.000	99.994
Sep 2002	99.998	100.000	99.986	100.000	99.996	99.995	100.000	100.000	100.000	99.998	100.000	100.000	99.998	99.998
Oct 2002	99.995	100.000	100.000	100.000	99.996	99.997	100.000	99.988	99.999	99.999	100.000	100.000	99.996	99.961
Nov 2002	99.997	100.000	100.000	99.984	100.000	100.000	100.000	100.000	99.998	99.999	99.998	99.999	99.988	99.999
Dec 2002	99.970	99.998	99.999	99.999	99.994	99.999	99.999	–	100.000	99.979	99.945	99.997	99.984	99.925
Jan 2003	99.997	100.000	100.000	99.996	99.999	99.999	99.989	–	100.000	99.996	99.997	99.996	99.999	99.999
Feb 2003	99.999	100.000	99.999	99.997	100.000	100.000	100.000	–	100.000	99.999	99.999	100.000	99.999	99.999
Mar 2003	99.995	99.998	99.996	99.998	99.995	99.998	99.998	–	99.998	99.993	99.993	99.997	99.997	99.996
Apr 2003	99.998	99.999	99.999	99.999	99.999	100.000	99.999	–	100.000	99.999	99.998	99.998	99.997	99.994
May 2003	99.997	100.000	99.984	99.996	99.999	99.998	100.000	–	99.999	99.997	99.999	99.996	99.990	99.985
June 2003	99.998	100.000	100.000	100.000	100.000	100.000	99.999	–	100.000	99.996	99.998	99.998	99.999	99.992

CISCO SYSTEMS

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 6317 7777
Fax: +65 6317 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.com Web site 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

DR/LW4827 0703

Printed in the USA