Cisco on Cisco Best Practices
Cisco High Availability WAN

HOW CAPNET ACHIEVED HIGH AVAILABILITY

High Availability Case Study

This case study describes how Cisco IT achieved high availability networking and reduced operating costs as a result. Making improvements across all the following functional areas proved to be crucial to success:

- **Network design**—Consistent architecture-driven designs
- **Network operations**—Consistent processes for changes and upgrades
- **Network management**— Configuration templates and proactive fault and performance management
- **Network support**—Training, sparing, and troubleshooting
- **Network infrastructure**—Standardization across a few platforms

By focusing on these areas, the CAPNet team successfully boosted availability to 99.998 percent. We not only achieved our availability goal, but also reduced the CAPNet staff from six engineers to just one for the entire worldwide network.

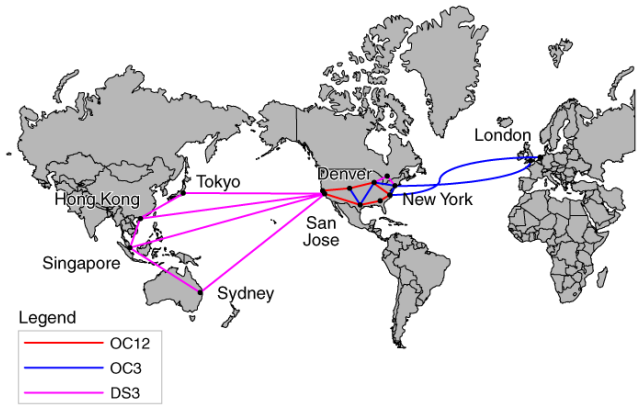
CISCO ALL-PACKET NETWORK

Cisco all-packet network (CAPNet) is a global backbone network that serves tens of thousands of Cisco employees and contractors at 15 locations on four continents (Figure 1).

> *"The CAPNet represents the heart of Cisco's converged global communications infrastructure, carrying voice, video, and data for Cisco employees between hundreds of Cisco locations and partner locations worldwide. Availability of this network is paramount to sustaining Cisco's business operations."* Lance Perry, Vice President, Worldwide IT Infrastructure, Cisco Systems.

Cisco employees and contractors rely on CAPNet daily for business-critical applications, interoffice communications, and connectivity to Internet touch points at Cisco facilities worldwide. Because CAPNet is the backbone of the Cisco global network, even a brief outage can disrupt the workflow of thousands of employees. Therefore, high availability is a priority for the CAPNet team.

Figure 1 CAPNet Worldwide Network



Gigabit Ethernet, OC12, OC3, and DS3 circuits connect Cisco sites in major cities in Europe, North America, Asia, and Australia. Each site has at least two diversely routed circuits on redundant hardware to maximize fault tolerance. CAPNet bandwidth ranges between 45 Mbps to 622Mbps, depending on the location.

How Is High Availability Specified?

High availability is typically specified as the percentage of time a network is available, expressed as a number of nines:

- 3 nines (99.9%)—10 minutes downtime per week
- 4 nines (99.99%)—1 minute downtime per week
- 5 nines (99.999%)—6 seconds downtime per week

Cisco's business applications require at least four nines availability, but the goal for CAPNet is five nines or better. Many enterprise networks are capable of five nines, but few achieve this availability without careful attention to all factors that contribute to network downtime. To achieve five nines, enterprises must assess and improve network design, operations, management, and support. The payoff is big—a highly available network that decreases operating costs, increases employee productivity, streamlines supply chain activities, and provides the infrastructure necessary for applications such as video conferencing and IP Communications.

THE ROAD TO FIVE NINES

The Cisco WAN developed gradually over time to accommodate growth, acquisitions, and network enhancements. Different sites used different equipment, different Cisco IOS® Software releases, and nonstandard configurations. Networks of acquired companies were occasionally merged with CAPNet without careful planning and integration. Operational and support procedures had gaps that extended the duration of outages. These and other problems led to unplanned downtime that affected availability.

At the same time, Cisco was investing heavily in IP Communications (data, voice, and video), because IP data networks had matured to the point where they could, and should, be as reliable as telephone networks. The CAPNet team realized that is was time to strengthen the underlying infrastructure that would make IP Communications successful.

At the start of the high-availability effort, the CAPNet service level agreement (SLA) was at three nines (99.975%), thanks to resilient technologies such as redundant routers and circuits that were deployed in the network infrastructure. Downtime was usually not the result of hardware or circuit failures. Subtle or intermittent problems such as flapping routes, inconsistent equipment configurations, or gaps in the support procedures were generally the culprit.

The CAPNet team tackled these problems in phases. First they established reliable availability measurements that could quantify the improvement progress. Then they identified the key design and procedural gaps and executed upgrade programs. The initial goal was four nines, which they achieved by closing the major gaps. The final goal was five nines or better, which required careful attention to all factors that affect network availability.

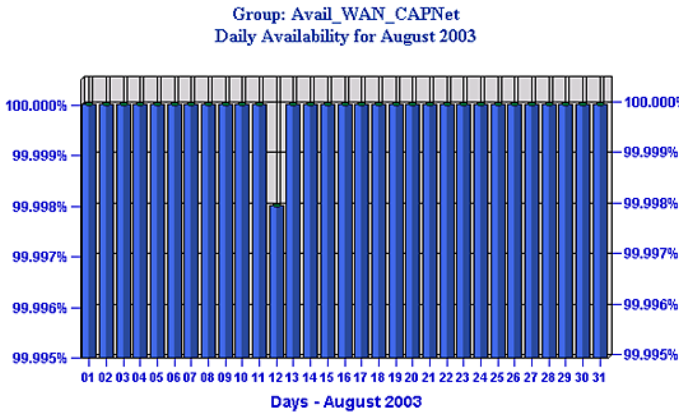
This is a success story—telling how the CAPNet team achieved high-availability targets and reduced operational costs, all in a real-world global network environment. And the CAPNet team did it all without adding personnel; the existing team planned and implemented all improvements. In fact, as availability improved, network support decreased, and the team had more time to devote to other programs.

MEASURING CAPNET AVAILABILITY

CAPNet monitors availability using EMAN, an internal network management system. This system continuously collects availability data for CAPNet nodes, computes availability percentages, and reports the results.

EMAN displays availability data in bar graphs that show performance by time or location. For example, Figure 2 shows daily CAPNet availability for August 3003.

Figure 2 Availability Graph for August of 2003



The EMAN system provided the CAPNet group with good availability measurements from the start, but the team did improve the measurement accuracy over the course of the program. The most important accuracy change was measurement of composite host availability, instead of device availability, as described in this section.

Why Measure Availability?

Cisco IT uses availability metrics to determine how well CAPNet is performing, to help identify the cause of specific outages, and most importantly, to establish availability trends over time. Is availability getting better? Is availability getting worse? Knowing trends is especially important as you execute availability improvement programs because they quantify your progress.

Consistent availability measurements over time also help the CAPNet team track the effects of changes to hardware, software, circuits, topology, and operational practices. CAPNet also uses availability measurements to verify service levels for system users.

How Does CAPNet Measure Availability?

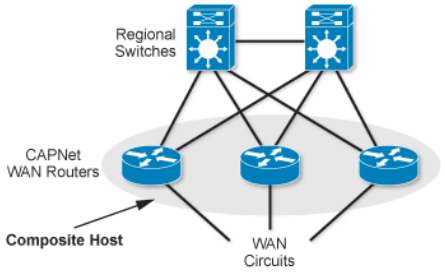
CAPNet measures availability by pinging each CAPNet site every 15 seconds, 24 hours a day, seven days a week. If any host at the site responds, the site is considered available for that time interval. CAPNet measures site availability rather than individual device or link availability, because a single failure of a device or link does not isolate a site. CAPNet does monitor device and link availability, but these metrics do not affect CAPNet availability reports.

Composite Hosts

CAPNet measures site availability using composite hosts, which are an EMAN feature that groups all WAN routers at a site into a single logical host. Testing the availability of the composite host then yields the site availability. EMAN also treats the composite host as an availability subgroup, so you can later view network availability data by site.

For example, Figure 3 shows a composite host that groups three WAN routers.

Figure 3 Composite Host at CAPNet Site



In this example, redundant hardware and mesh connections make the site resistant to single device or link failures. Because traffic quickly reroutes around a failure, one or two individual hosts or WAN circuits can fail without affecting availability. Availability measurements do not directly test other equipment at the site, such as regional switches or out-of-band management circuits (not shown).

Aggregate Availability

Aggregate network availability is the composite of the availability metrics for all sites, or availability subgroups, in the global CAPNet network. Each site has one availability subgroup and that subgroup has a single composite host. CAPNet contains 13 availability subgroups—one for each hub outside San Jose. An EMAN availability collector in San Jose measures availability worldwide.

Table 1 lists sample availability for all CAPNet sites (availability subgroups) over a 12-month period.

Table 1 Availability for April 2003 to March 2004

Availability Subgroup	Availability
Atlanta	99.998%
Chicago	99.999%
Dallas	99.999%
Denver	100%
EMEA	99.91%
Hong Kong	100%
Kanata	99.99%
New York	99.999%
RTP	99.999%
Redwood City	100%
Singapore	99.999%
Sydney	99.998%
Tokyo	100%
Total Network	**99.9916%**

The total network availability is simply the average of all availability subgroups. No one subgroup is considered more important than another.

Availability Measurements

The CAPNet team collects raw availability data for each hub, circuit, and device.

- Hub site

  The composite host is considered available if at least one of the devices within the composite is responding. This is the metric that the CAPNet team uses for availability.

Host availability measurements make no distinction between raw and adjusted availabilities. Because CAPNet is a backbone service, the CAPNet team never plans downtime that would disrupt service.

- WAN circuit (raw and adjusted for planned maintenance)

  Each circuit is monitored for availability using ICMP to the interface IP address (EMAN virtual host) at the end of the circuit furthest from the EMAN collector in San Jose. This data helps verify that WAN circuits conform to their SLAs.

  WAN circuits are generally characterized by an adjusted availability value, which subtracts planned maintenance from raw downtime. CAPNet minimizes the risk of unplanned outages by using on-site spares and on-site support.

- WAN router

  Each device is monitored for availability by reviewing outage records on the on-call log (see Network Support section). This activity helps identify devices that are down too often.

Availability Test

The EMAN collector sends two pings to the appropriate IP address every 15 seconds. A device is considered available for the 15-second interval if it replies to at least one of the two pings for that interval. Therefore, the average device availability equals the number of successful ping intervals divided by the total number of possible ping intervals. During a 24-hour day there are 5,760 15-second ping intervals.

Loosing just one ping interval reduces the availability to less than four nines (99.982%) for the day. Table 2 shows how ping loss corresponds to monthly availability.

Table 2 Affect of monthly ping loss on availability

Number of lost ping intervals	Monthly downtime	Availability
1.728	26.1 seconds	99.999%
17.28	4.3 minutes	99.990%
30[1]	7.5 minutes	99.982%

The longest theoretical outage that could go unnoticed is less than 15 seconds (down immediately following one ping interval but back up before missing the next). Using a 15-second interval strikes a balance between adequate and intrusive monitoring traffic.

Benefiting from Availability Measurements

CAPNet promises to deliver 99.99% availability, which leaves little margin for error. A momentary routing change that may go unnoticed by the average user can cause missed availability that CAPNet cannot tolerate. A solid availability measurement system was the cornerstone for the CAPNet's high availability program.

MOVING TO FOUR NINES

Now that the CAPNet team had good availability measurements, they were ready to conduct a strategic assessment of the overall network and operational infrastructure. This assessment identified likely improvement projects and assigned priorities each. For this phase of the availability project, the following design and standardization areas were high priorities:

- IP addressing plan for route summarization
- Standard hardware and software
- Configuration management process

Route Summarization Problem

The Cisco WAN developed gradually over time to accommodate growth, acquisitions, and network enhancements. As a result, IP addresses were not grouped by region, routing tables were large, and route summarization was not practical. A network flap in one region could propagate over a wide area, which reduces availability.

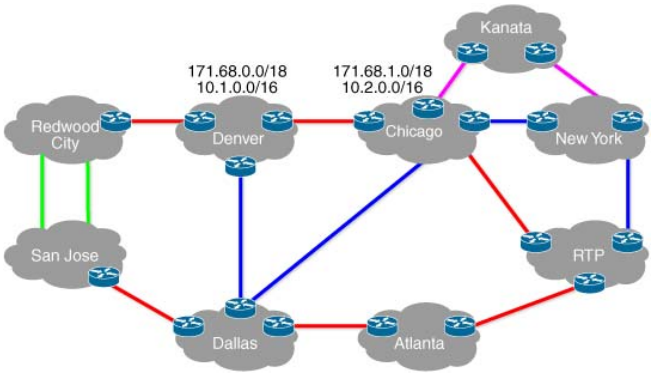
Cisco IT chose to implement route summaries because they:

- Reduce the size of the routing tables. Consequently, memory and CPU resources are conserved.
- Enforce a hierarchy of routes and limit routing instabilities to a small area. If an address within a summary range changes or a link changes state, the change is not advertised outside of the summarized area.

To implement route summarization, CAPNet and the regional IT groups had to adopt a new IP addressing plan for the entire network. This new plan grouped network addresses by regions so they could be summarized at the WAN interface. Figure 4 shows the US CAPNet and summary addresses for selected areas.

[1] One ping interval loss per day

Figure 4 Summary Routes for CAPNet Sites



Many sites advertise just two summary addresses, one for site administration and IP phones, and another for Internet-routed addresses. For example, the Denver site has two summary addresses:

- 171.68.0.0/18—addresses from 171.68.0.0 to 171.68.63.255
- 10.1.0.0/16— addresses from 10.1.0.0. to 10.1.255.255

Hardware Standardization

The CAPNet team's next project was selecting and deploying standard hardware. Consistent hardware configurations are critical to scaling CAPNet globally while still maintaining high availability. Every one-off configuration potentially complicates support, prolongs outages, and increases the total cost of ownership for Cisco IT.

Minimizing the number of supported hardware platforms simplifies operations and minimizes the chance of platform incompatibilities. Hardware standardization includes the base chassis, all line cards, and populated chassis slots.

CAPNet uses the standard hardware platforms listed in Table 3.

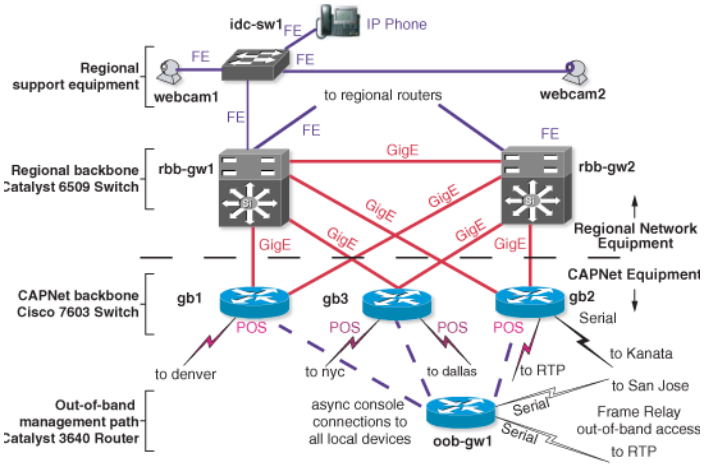
Table 3 Standard Routers for CAPNet

Router	Function	Key Feature
7206VXR	Backbone router	DS3 interfaces
7603	Backbone router	OCx interfaces
3640	Out-of-band router	Frame Relay interfaces

CAPNet works with regional network groups to assemble these standard components into building blocks that can be reused in each site. These building blocks not only use standard hardware components, they also adopt standard port usage and naming conventions.

Figure 5 shows a typical CAPNet site.

Figure 5 Typical Equipment Configuration at CAPNet Site



This site has the following primary components:

- Cisco 7603 routers

  These three CAPNet routers connect to regional backbone switches using Gigabit Ethernet circuits. Redundant routers and circuits ensure that this site remains available during router or circuit failures. The number of routers can vary from site to site, but all sites have at least two routers with redundant circuits.

- Cisco 3640 Multiservice Platform

  This router supports the out-of-band Frame Relay management path. This path makes it possible to open a console session with local equipment even if all WAN circuits fail.

- Cisco Catalyst® 6509 switches

  The Catalyst 6509 switches in the regional backbone are not part of the CAPNet, but are shown here because they are important in site standardization. These routers form the regional gateway to the CAPNet backbone.

- Cisco Catalyst 3550 switch

  This switch supports a local IP phone, local console access, and Web cameras. Web cameras are useful when using *remote hands* to resolve problems that require onsite personnel. This is regional equipment, but it helps the CAPNet support personnel.

Cisco IOS Software Standardization

After selecting and deploying standard hardware, the CAPNet had to select and deploy standard Cisco IOS® Software releases. Working with Advanced Services and other design and operations groups within Cisco, CAPNet aggressively deploys as few as

possible Cisco IOS Software releases across the various sites and equipment.

Standardizing on Cisco IOS Software releases does not entirely eliminate incompatibilities, but it does minimize interoperability issues between CAPNet devices and those of other operations groups.

Cisco IOS Software standardization also has the following benefits:

- Takes advantage of the experience and testing of other groups
- Improves network operations by reducing the number bugs the team must identify and track
- Ensures that critical services such as routing, QoS, and multicast work correctly end-to-end

The CAPNet team chooses Cisco IOS Software releases from the Global IOS Standards list that Cisco IT publishes. This list defines two categories of releases, *recommended* and *acceptable* by platform type and function.

The Cisco IOS Software current and previous releases in use by CAPNet are posted on an internal Cisco Website that is available to the networking team. For example, Table 4 shows the current and previous Cisco IOS Software releases as of 3/23/2004.

Table 4 Standard Cisco IOS Software Releases for CAPNet Routers

Router Model	Router Function	Current Cisco IOS	Previous Cisco IOS
7206VXR	Backbone router	12.2(13)T5	12.2(8)T4
7603	Backbone router	12.1(19)E1	12.1(13)E8
3640	Out-of-band router	12.2(13)T5	12.2(8)T4
7206VXR	DR/VPN router	12.2(15)T7	N/A

Note: The feature set is 3DES with Secure Shell (SSH) Protocol support.

Operational groups within Cisco IT, including CAPNet, are considered compliant with the Global Cisco IOS Software standards if they use either the *recommended* or *acceptable* releases. The CAPNet team does not automatically update from acceptable to recommended; updates are usually conducted when network users require new features that are only available in later releases.

Device Configuration

Now that CAPNet had standard hardware and software deployed, the team wanted to apply and enforce standard configurations. CAPNet adopts standard configurations to reduce incompatibilities caused by inconsistent or incorrect configurations. Standard configurations for everything from AAA authentication, access lists for SNMP, NTP, and logging help minimize support and interoperability issues while maximizing performance and reliability.

CAPNet uses the EMAN Auto Configuration Tool and standard global templates to apply basic configuration (for example, password encryption and timestamps) AAA Authentication, multicast, SNMP and NTP configurations.

EMAN reapplies the standard configuration to each device daily, overwriting (and reporting) any ad-hoc configuration changes that might have been made. The use of the Auto Configuration Tool has elevated the configuration consistency to a new level, one that was not previously possible. Before the introduction of this tool in Q4 2002, the CAPNet team relied on manual set up and periodic inspection of configurations to maintain consistency. This was time consuming and configuration errors were easily overlooked.

Benefiting from Four Nines

The road to four nines was paved with routing improvements and hardware, software, and configuration standardization. Problems in these areas can accumulate over time as a network grows because different sites are deployed at different times with different hardware, software, and IP subnets. Fixing these problems alone pushed CAPNet availability well over four nines. Maintaining four nines and pushing forward to five nines, however, required attention to operations, management, and support processes. The next section describes that effort.

MOVING TO FIVE NINES

The steps taken to achieve four nines capitalized on the easy opportunities for improvement. Moving to five nines required refinement of operational and support procedures.

CAPNet identified the following programs as priorities:

- Network design—Facility and circuit planning, and technology adoption.
- Network management—Host definitions and out-of-band management
- Network operations—Best practices for Cisco IOS Software upgrades and network changes

- Fault management and network support—Monitors, alerts, and event procedures

NETWORK DESIGN

CAPNet is a wide area network composed of SONET/SDH, DS3, and Frame Relay (for out-of-band access to Internet Data Centers [IDCs]) circuits that connect Cisco facilities in the Americas, EMEA the Asia Pacific region, and Japan. CAPNet sites are located at facilities owned or leased by Cisco and carrier-owned IDCs on four continents.

A carefully planed and comprehensive architecture and design that includes redundancy and fault-tolerance is the foundation for this highly available network. Performance, reliability, and value to Cisco (cost and showcase) are the critical factors considered in the design.

Facility Planning

Consider the following points when choosing physical facilities:

- Site—Choose a physical site suitable for all equipment, such as a secure room with equipment racks that has environmental controls.
- Power—High availability requires reliable power sources. All equipment should be on uninterruptable power supplies (UPS), and backbone equipment requires UPS with generator backup.

Carrier Circuit Planning

High-availability WAN circuits require SLAs with multi-homing, circuit diversity, low latency, circuit protection, and other availability practices. CAPNet designers team with circuit providers to get the necessary services. For various reasons, the desired bandwidth, circuit diversity or latency are not always available for every circuit. Sometimes costs, available fiber paths, carrier capacity, or other factors demand a compromise. In those cases the compromise is documented so that both the operations team and the carrier are aware of the compromise and during an outage can take appropriate steps to quickly mitigate the issue and return normal service.

Resilient Technology Adoption

Resilient technologies make the network tolerant to hardware and circuit failures. Keep in mind that simplicity is important when adopting resilient technologies; choose only those technologies that you need for your applications.

Redundant Hosts and Circuits

Each CAPNet site is connected by a minimum of two diversely routed circuits on redundant hardware to maximize fault tolerance. With this configuration, a host or circuit can fail without interrupting traffic because traffic quickly reroutes to redundant hosts and circuits.

IP Event Dampening

CAPNet is just now deploying IP Event Dampening on the Cisco 7200 platforms (running Cisco IOS Software release 12.2T). IP Event Dampening works like BGP route dampening. If a route flaps (because of a circuit flap or other reason), the route is temporarily suppressed. In a network like the CAPNet, with excellent Layer-3 redundancy, IP Event Dampening brings stability because it prevents traffic loss during route flaps.

The CAPNet team plans to deploy IP event dampening on their Cisco 7600 platforms as soon as there is support for that feature in a Cisco IT tested and approved Cisco IOS Software release.

NETWORK MANAGEMENT

Simplicity and consistency are essential to managing a network for high availability. Make sure hosts are clearly identified and always reachable

EMAN Management System Host Configuration

Each CAPNet device is entered into EMAN Host Management. This housekeeping task provides the foundation for monitoring and alerting, which is discussed in the Network Operations section.

It is extremely important that the EMAN Host Management information for each device be accurate and consistent. The following fields are standard for CAPNet hosts:

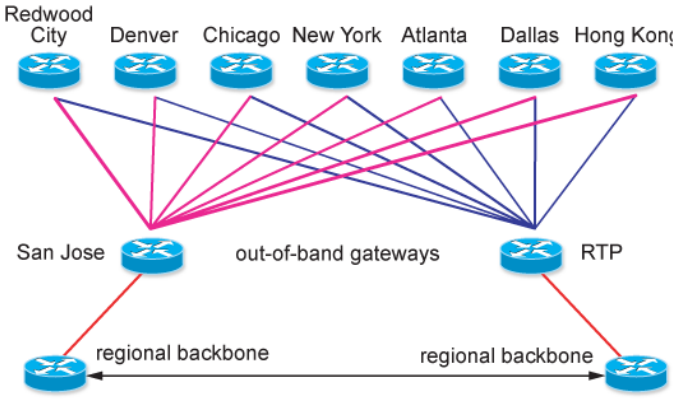
```
Area = As appropriate for location
Street = As appropriate for location
City = As appropriate for location
Support Group = IT
PGM Group = CAPNet
Duty Pager = capnet-duty
Contact = capnet-core@cisco.com
Collect Syslog Messages=Yes
Read-Only Community String = See std. config
Rear-Write Community String = See std. config
Collector Name = IS-HQ (and others as
appropriate)
Priority Level = P1/P2 (as appropriate)
Report Type = WAN
Alerts Enabled? = Yes
Download Config? = Yes
Business Support = CAPNet
Router Service Type = CAPNet Router
Comments = A brief description of the device
function and what redundancy (if any) is
available
```


Out-of-Band Management Path

An out-of-band management path ensures that network support staff can reach colocation sites even if all WAN circuits are down. This is a critical availability factor, because if support personnel cannot reach a site that has problems, it takes longer to resolve the problem and restore service.

Each colocation site has redundant Frame Relay Permanent Virtual Circuits (PVCs) to a Cisco 3640 Multiservice Platform, which connects to console ports of each production device at the site. Using this path, support staff can open a console session for any device and analyze the problem remotely, without dispatching personnel to the site. Figure 6 shows CAPNet's out-of-band management network.

Figure 6 Out-of-Band Network



Every site is reachable from two independent out-of-band paths, one from San Jose and another from RTP. Consequently, each site is reachable even if all WAN circuits and one of the out-of band circuits are down. If a site is completely unreachable, there is a serious WAN outage, not just a site problem.

The Frame Relay circuits must be truly independent of the primary WAN circuits. They use diverse circuits from diverse locations so that they are not likely to fail at the same time as the primary circuits.

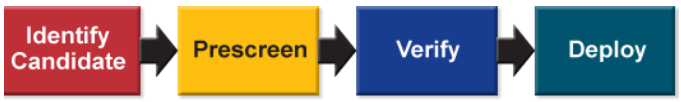
NETWORK OPERATIONS

The CAPNet team improved network operations by adopting best practices for Cisco IOS Software upgrades and change management.

Cisco IOS Software Upgrade Best Practices

The CAPNet team adopts a new Cisco IOS Software release only when users require a new feature, and then only after the IT Transport Design and Engineering team approves the release for company-wide deployment. When necessary, the CAPNet team selects an upgrade candidate and proceeds with the Cisco IOS Software upgrade process (see Figure 7).

Figure 7 Cisco IOS Software Upgrade Process



Even though the images listed in the global Cisco IOS Software standards document have been tested and deployed by other transport groups at Cisco, CAPNet operations still prescreens and verifies each new Cisco IOS Software image before deploying it. Prescreening consists of:

- Bug scrubs through Cisco.com and Advanced Services
- Review of Cisco IOS Software Release Notes for show stoppers

CAPNet then verifies the Cisco IOS Software candidate using lab and pilot tests. Lab tests verify basic functionality and compatibility, and pilot tests verify router operation in a limited production environment. Assuming the candidate passes all tests, it becomes the new standard and is scheduled for deployment across all CAPNet sites.

Cisco IOS Software Image Storage

All CAPNet routers have sufficient Flash (either on-board or slot flash) to store at least two Cisco IOS Software images (see Table 5).

Table 5 Storage Locations for Cisco IOS Software Images

	7603	7206VXR	3640
Primary image	sup-bootflash	slot 0	bootflash
Secondary image	slot 0	slot 1	slot 0

It is a CAPNet practice to store the current Cisco IOS Software image and its immediate predecessor on all routers. It's important to have an image ready for a quick downgrade or to replace the primary Cisco IOS Software image if it becomes unusable. If an image being upgraded is no longer a viable alternative to the current primary image, then store two copies of the current primary image on the router. This ensures that an alternate boot image is always available if the primary image becomes unusable.

Cisco IOS Software Image Upgrade

Upgrading Cisco IOS Software images throughout CAPNet is a periodic task, so it must be performed correctly to avoid outages. To ensure smooth upgrades, CAPNet posts detailed upgrade procedures on the internal Website. These procedures include:

- Cisco IOS Software staging—the process of loading a new image in the backup location.
- Cisco IOS Software upgrade scheduling—the process of scheduling a maintenance window through the formal Cisco Change Management system. This system is a Web-based tool that simplifies the process or creating, approving, and tracking change requests.
- Cisco IOS Software activation—the process of activating new images and verifying that the new image works correctly. This includes notification of support personnel so they know to expect changes.

Change Management Best Practices

CAPNet handles other changes to the network, such as new hardware or circuit additions, in a similar manner. The change is scheduled through the Change Management system, taking into account Cisco network freeze periods, and then deployed in a systematic manner. This is a practice across Cisco IT, not unique to CAPNet.

FAULT MANAGEMENT

Even highly available networks experience failures and downtime. Hardware components fail, software has bugs, WAN circuits drop, and network personnel make errors. Monitoring network performance and alerting support staff does not reduce the number of failures, but it can reduce their effects. A robust system of monitoring and alerting that quickly identifies problems and notifies operations personnel goes a long way towards minimizing the length and effect of any outage.

Activity Monitor

EMAN Enterprise Monitor is an internal Cisco IT network management system that provides a robust set of tools for monitoring network activity and sending alerts for significant changes.

CAPNet uses EMAN Enterprise Monitor to capture the following network information:

- Device and virtual host ICMP availability
- Traps for significant events:
  - Interface state
  - Router reload
  - Router coldstart
- Real-time monitoring for:
  - Interface state
  - Router CPU levels
  - Router memory
  - Latency monitor (each circuit has a contracted latency)
- Syslog messages
  - EIGRP stuck in active (SIA)
  - Duplex mismatches
  - Other events

Monitoring interface traps, real-time monitoring, and virtual hosts might seem redundant. However, in an environment with redundant hosts and circuits, this level of monitoring minimizes the chance of missing something. A router restart or an intermittent circuit flap might not create an availability hit, but it would generate a trap. Such unnoticed faults could affect performance and reliability for the network. Basically, it is better to get one page too many than one page too few.

The CAPNet team added a custom view in EMAN for real-time monitoring. This view gives the duty engineer a quick look into the current status and exceptions for all real-time monitoring events.

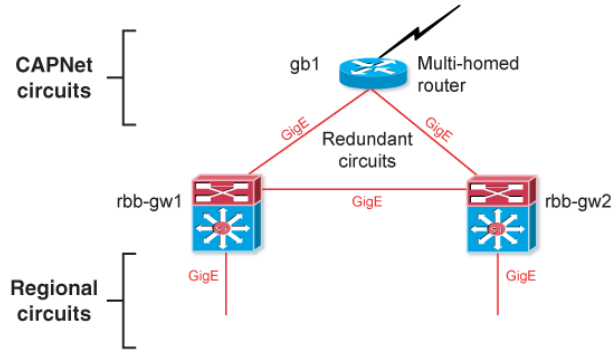
Monitoring Hosts that Have Redundant Circuits

Accurate availability measurements depend on correct interface usage and home address configuration. Otherwise, hosts can appear to be down when they are not.

Each individual CAPNet hostname is single-homed to the address on the Loopback 0 interface, and that loopback address is used for monitoring individual devices. The use of the loopback interface provides a stable, always up, interface for monitoring hosts and performing remote commands from EMAN. Using a loopback interface also simplifies maintenance and support activities. Single-home hostnames are better than multi-home hostnames when doing round-robin DNS for monitoring, because you can frequently get false positives in EMAN's Enterprise Monitor (a host showing down when it is really up).

Figure 8 shows how multi-homing can lead to incorrect availability data.

Figure 8 Multi-home Hosts with Redundant Circuits



If gb1 is monitored using multi-homed hostnames, it would appear to be down during a planned one-hour maintenance window for rbb-gw2 because the interfaces connecting gb1 to rbb-gw2 would be down, even though the router has redundant connectivity to rbb-gw1. You could get around this problem by including gb1 in the change management for rbb-gw2, but that inclusion would mask any real problem with gb1 that might occur during the maintenance window.

Network Alerts

EMAN can be configured to send alerts for any data that it monitors. These alerts can be sent to an individual or to a duty pager alias. The CAPNet team uses alert groups to customize the alerting for different parts of the network and different alert priorities (see Table 6).

Table 6 Alert Group Notification

Alert Group	Action	Example
High	Notify on-call engineer immediately, 7x24	Circuit down
Moderate	Notify on-call engineer during business hours and send email during off-hours	Out-of-band circuit flap
Low	Notify by email only	Duplex mismatch

The use of multiple alert groups ensures that critical issues are addressed as soon as possible (7x24). Other less critical but still important issues are handled within an appropriate timeframe without needlessly over-burdening the on-call engineer.

NETWORK SUPPORT

CAPNet uses on-call engineering for network support, with secondary help from Cisco Advanced Services. The on-call engineer is available 7x24 to resolve network problems. The on-call engineer tracks problems using an on-call log and posts summary information in EMAN.

On-Call Engineering

The CAPNet duty (on-call) rotation consists of eight engineers doing a one week 7x24 rotation. Therefore, each engineer has one week on and eight weeks off. The on-call engineer is responsible for handling all emergency issues, which are usually generated in real-time by the EMAN alert service in the form of a duty page. Occasionally, the CAPNet on-call engineer receives an alert from network operations (usually not directly related to the CAPNet).

CAPNet posts its on-call duty schedule on the IT Operations Support Duty Scheduler, along with other Cisco IT support groups. This scheduler is a calendar-like Web page that shows the primary and backup engineer on duty for each day.

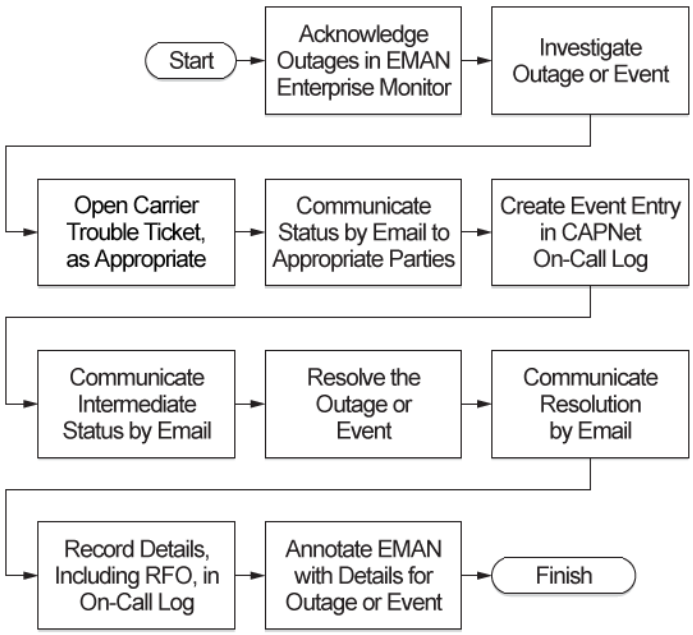
Duty Turnover

CAPNet Duty rotates weekly with a new shift beginning every Monday morning at 8:00 a. m. Pacific time. At that time, the current duty engineer transfers on-call duty to the next engineer in the rotation, either by phone or instant message. The current CAPNet duty engineer is responsible for duty coverage until the successor provides positive confirmation of the duty turnover. Open cases and trouble tickets at the time of the duty change are to be turned over to the new CAPNet duty engineer, except where it is not desirable or practical to do so.

Event Procedure

The CAPNet duty engineer follows a standard procedure that identifies the problem, communicates progress, and documents the outcome (see Figure 9).

Figure 9 Event Procedure Flow Diagram



CAPNet On-Call Log

Every incident that the on-call engineer handles is recorded in an on-call summary log. This log tracks and calculates the outages/events by problem classification, problem sub-classification, start time, end time, outage/event duration, time to resolve, and reason for outage (RFO). Table 7 summarizes the problem and sub-classifications.

Table 7 Problem Classifications

Problem Classification	Problem Sub-Classification
COS-CatOS	COS-Other COS-Undetermined/Intermittent COS-Version Interoperability
EV-Environmental	EV-Power--Equipment EV-Power--Room EV-Power--Site
HE-Human Error	HE-Misconfiguration HE-No CM Approved HE-Redundancy Failure ...
HF-Hardware Failure	HF-Cabling HF-Cisco System Component HF-Non-Cisco Equipment
IL-Increased Latency	IL-Increased Latency - Carrier Reroute IL-Increased Latency - Circuit Congestion
IOS-IOS	IOS-CPU Load IOS-Multicast IOS-Routing ...
NA-N/A	NA-Engineer Troubleshooting NA-Not a Network Related Problem NA-P3 Site NA-Problem with Monitoring
TF-Transport Failure	TF-LAN TF-WAN Circuit Down- General Carrier Outage TF-WAN Circuit Down- No Backup ...
UD-Undetermined	UD-Undetermined

Problem Tracking

Tracking outage and event details over time is critical for operational success. With a duty rotation transitioning from person to person, there is no other reliable way to identify trends or chronic issues. Each quarter, CAPNet reviews tracking data and identifies areas for operational improvement.

For example, problem classifications in the on-call log easily identify the following problems:

- Chronic hardware or Cisco IOS Software issues
- Periodic problems with a carrier or individual circuit
- Environmental issues, like power and HVAC problems
- Human errors, such as misconfigurations

Problems like circuit or hardware failures might not preventable, but the on-call log makes it easier to identify those issues that can be improved. In short, it is impossible to fix a problem unless the problem has been identified. The on-call log is a critical tool that CAPNet uses to identify and fix on-going or chronic problems and maintain operational excellence.

The on-call log also provides an easy copy-and-paste source for annotating EMAN pages, which provide outage and event information for individuals and groups that do not have easy access to the on-call log. To ensure that EMAN annotations provide consistent and complete information, the CAPNet uses an annotation template that includes the following information:

- Hosts and circuits affected

- Time down
- Time up
- Problem description
- Reason for outage (RFO)

Proactive Fault Management

The on-call CAPNet duty engineer is responsible for reviewing the EMAN network availability metrics daily and for annotating items that do not meet the availability targets. CAPNet receives daily reports detailing configuration changes, number of routes in the routing tables, autoconfiguration success or failure, and configuration exception reports. CAPNet also receives syslog alerts for events such as EIGRP SIAs and Ethernet duplex mismatches.

Investigating missed availability, even though it may not bring the site or device below the SLA, is also strongly encouraged. Proactive investigation of minor problems might uncover a weakness before it becomes a service-affecting outage.

Cisco Advanced Services

CAPNet uses Cisco Advanced Services as a technical resource for:

- Bug scrubs
- Product development
- Hardware and software resource
- Troubleshooting experts
- Design experts

Spare Components

CAPNet maintains spare components at each site. If a hardware failure occurs, field personnel can quickly swap the hardware component and restore normal operations with full redundancy.

Cameras and Remote Hands

Each CAPNet colocation site has Web cams that face the equipment rack. The on-call engineer can use these cameras to view the equipment and help remote personnel resolve problems. Cisco IT has contracts for onsite support at all co-location sites, so onsite assistance is readily available.

CAPNet Documentation

Easily found and accurate online documentation is an important aid for the on-call engineer helping to quickly address and remedy problems when they arise. The following online documentation is maintained by the CAPNet team:

- CAPNet Duty Procedures
- CAPNet Carrier Contacts Page
- CAPNet Network Maps
- CAPNet IOS Standards
- CAPNet BGP
- CAPNet Dashboard Global Duty Schedules
- TAC Case Procedures

All documents are easy to access on Cisco IT's internal Website.

CONCLUSION AND RECOMMENDATIONS

In many respects, the road to high availability is paved with good operational practices and common sense. The adoption of best practices can often increase operational overhead in the short term, but if implemented properly, will reduce overhead significantly in the long term. Focus on the areas of network design, configuration, monitoring and alerting, on-call support procedures, and documentation. Without focusing on these areas, operational excellence is difficult to achieve and even more difficult to maintain.

When starting a high-availability program, look for opportunities to implement a few easy improvements first. If you have too many hardware platforms and Cisco IOS Software releases deployed, try changing to standard hardware platforms and software releases. Remember however, that you can't get to five nines using technology and standardization alone. Many failures occur because of weak operating, management, and support procedures. Cisco provides many resources to enterprises, including best practice white papers for important processes.

The benefits of high availability by far outweigh the costs. Highly available networks improve company image, decrease operating costs, increases employee and vendor productivity, and support modern IP Communication applications, such as video conferencing and voice over IP.

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

www.cisco.com/go/ciscoit

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**