WHITE PAPER

NETWORK AVAILABILITY:
HOW MUCH DO YOU NEED? HOW DO YOU GET IT?

This white paper addresses the growing importance of communications networks, explains the key factors that influence network availability, and outlines some of the best practices, for both enterprises and network service providers, that help achieve this.

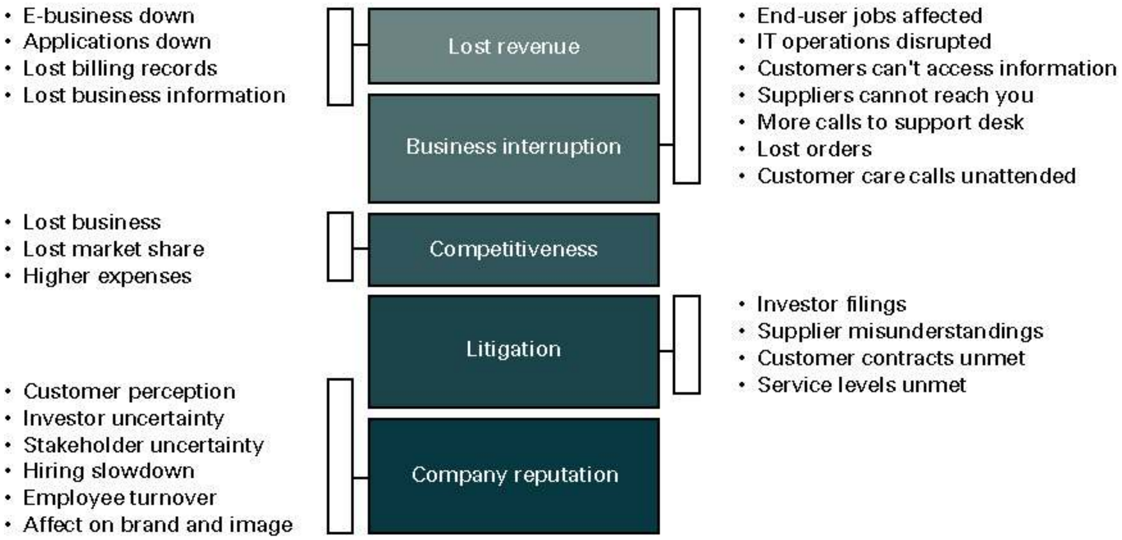
Businesses today are more dependent on network communications than they were only a few years ago. A recent survey found, for example, that more than 90 percent of advertisements in a national magazine include a Website address and it is surprising to receive a business card that doesn't include an e-mail address. Many businesses have implemented software applications that rely on networks for functions such as order entry, customer support, supply chain management, and employee benefit administration. Virtual private networks (VPNs), for example, are widely used to connect branch offices with headquarters and major suppliers and key customers are increasingly included in these networks as well. VPNs simplify remote-access requirements, and also replace difficult-to-manage legacy networks. There has been an increase in telecommuting and mobile workers, and more businesses have at least some functions that operate 24 hours a day. Using Internet or private networks using Internet Protocol (IP) technologies to carry ordinary telephone calls is commonplace, with IP-based private branch exchange (PBX) systems and telephones in offices of every size.

Disaster recovery plans that focus only on computer centers and the data they house may be inadequate; telecommunications networks must be considered as well. Failures in wide-area network (WAN) facilities are becoming a larger percentage of all failures, because of an increase in the number of online, networked business applications in use and the growing trend for major parts of enterprise networks to be outsourced.

The Gartner Group defines a resilient business as one that can "bounce back from any kind of setback, whether a natural disaster, an economic change, a competitive onslaught, cyber-espionage, or a terrorist attack." In a January 28, 2002 report, Gartner stated that only about a third of the enterprises they surveyed had plans in place to cope with the complete loss of physical assets and employee workspace. As recent world events make clear, business continuity plans must include LAN, WAN, and telephone facilities, along with data centers.

Disaster recovery plans often focus on complete failures, but even partial network failures can have a major impact on business effectiveness and employee productivity. The Meta Group studied typical revenue-per-hour figures for various industries, and found that the real cost of network failures to an enterprise is not the WAN charges from the network service provider, but the lost of business continuity, employee productivity, revenue, and customer good will. As business applications become more critical to a company's success, the reliability of the underlying network services becomes critical (see Figure 1).

Figure 1
Impacts of Network Failures



RELIABILITY VS. AVAILABILITY

Network availability is often confused with network reliability. Reliability is the ability of a device or system to perform its function without failure when called upon to do so. Availability means the system is ready for immediate use. Airplanes, for example, must be very reliable, while in the air, but aren’t expected to fly 24 hours a day. Reliable components certainly contribute to having a reliable network, but network availability is also controlled by other factors, including how rapidly a network can recover from a failure.

Mean time between failure (MTBF) is a common unit to measure reliability. MTBF is the average expected interval between failures of a product in steady state, for example., after the infant mortality and before the wear-out periods of its life. As an illustration, Cisco circuit cards are typically designed and tested for an MTBF of at least 100,000 hours, or as high as 200,000 hours for simple designs with few components.

Mean time to repair (MTTR) is the second key factor that determines network availability. MTTR is the average time it takes the operations staff (internal staff, service provider staff, or both) to diagnose, isolate, remove, and replace the failed part, and then restore full functionality to the network. Dispatch and travel time, if required, are included. “Repair time” doesn’t always involve people. Some products have been designed to detect a problem, switchover to a different piece of hardware or a different instance of software, rebuild a routing table, reboot a processor, and restore the system to service, all automatically.

Actual network availability is defined as MTBF divided by the sum of the MTBF and the MTTR. A network element, for example, that has a MTBF of 100,000 hours and typically takes 4 hours to restore when a failure occurs has an availability of 99.996 percent (see Figure 2).

Figure 2

Calculating System or Network Availability

$$\begin{aligned}\text{Availability} &= \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \\ &= \frac{10{,}000}{10{,}000 + 4} \\ &= \frac{10{,}000}{10{,}004} \\ &= 99.996\%\end{aligned}$$

The equation can also be worked in reverse. Assuming a 4-hour MTTR, a network service provider who offers a service level agreement (SLA) with a promised network availability of 99.99 percent is indicating that it expects a failure to occur, on average, about every 45,000 hours (equivalent to slightly more than 5 years).

Some documents, especially when discussing parts or products, describe availability in terms of defects per million (DPM). The two approaches result in different numerical results, but have essentially the same principles behind them.

ACHIEVING NETWORK AVAILABILITY

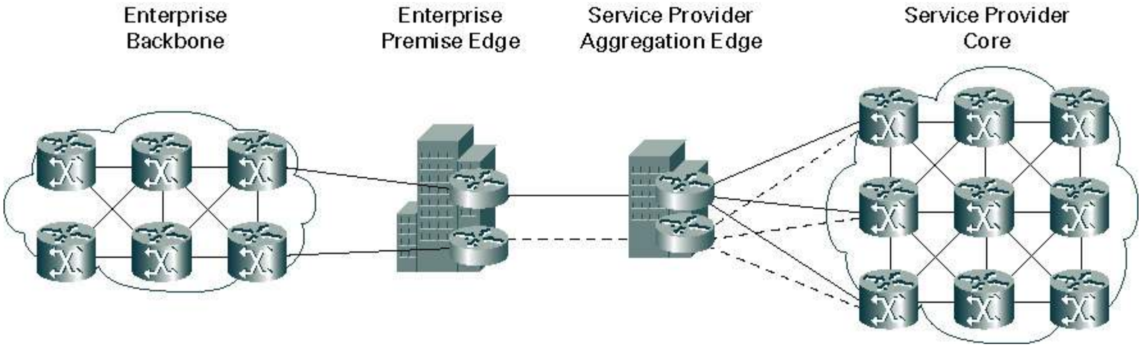
High network availability results from attention to three key points:

1. Choice of high-availability network elements, hardware, and software
2. Creation and maintenance of a high-availability environment (including security)
3. Use of network design and operations practices that emphasize high availability

Efforts in all three of these areas must consider the entire network, including LAN and campus networks, corporate data centers, and the data centers and WAN services provided by carriers or other network service providers (see Figure 3). This end-to-end perspective is the only way to minimize the chances and frequency of failure, to minimize the duration of inevitable outages, and to achieve employee productivity and customer service and satisfaction.

Figure 3

Taking the End-to-End View of Network Availability



The discussion that follows addresses both the enterprise and network service provider portions of the end-to-end network.

HIGH-AVAILABILITY PLATFORMS

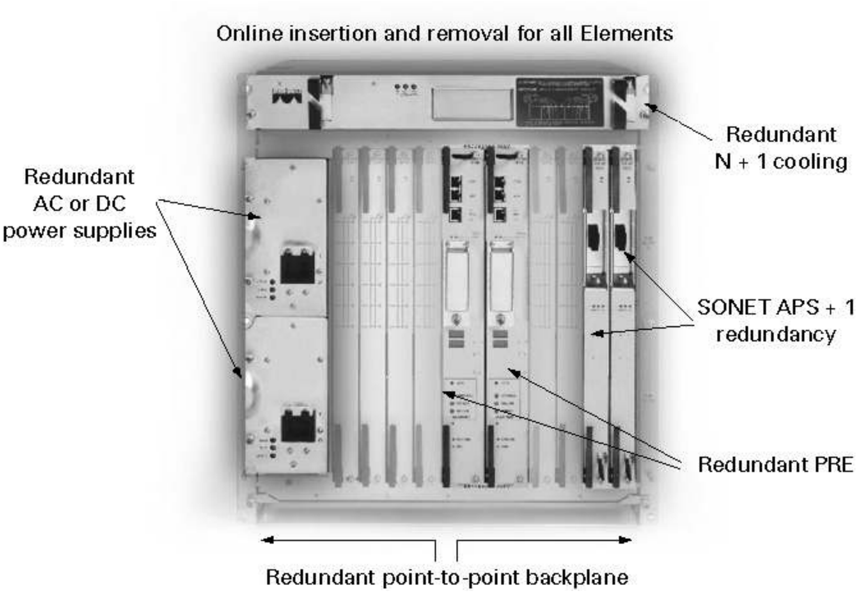
Hardware platforms can be made more reliable by both careful design and careful testing. While the product design process seeks to increase the MTBF of the product, it should also strive to decrease the MTTR. Employing redundant components, such as processors, power supplies and cooling fans can be doubly important-redundancy may not only prevent a service outage, but may also provide a means for low-risk maintenance and upgrade activities by the operations staff. Redundant designs can have one active and one redundant element (1:1), or one redundant element for every N elements that are active (1:N). Some system designs employ 1:N load-sharing redundancy, where all N+1 elements are active and carrying traffic, but only N are actually required—the load of any failed element can be handled by the remaining N elements. Redundancy is only as effective as the switchover process, which must detect the problem and move the load to the redundant element—with no loss of traffic—all within a very short amount of time. Systems with load-sharing redundancy designs are generally preferred to those with an active-plus-standby approach.

An example of the interaction of platform design and activities of the operations team involves the loading of new versions of software. Cisco® product designs allow the new Cisco IOS® Software image and configuration file to be loaded onto the standby route processor (RP) and parsed while still off-line, thus minimizing the reboot time when the new software is reloaded into all the line cards.

Many modular Cisco products allow for harmless insertion and removal of cards while the system is in service, thus minimizing the chance of an accidental, operations-caused network failure. Many larger Cisco products have optional 48-volt DC power supplies, for use in telephone company central offices, data centers, or other locations where 48-volt, battery-based uninterruptible power supply (UPS) installations are available.

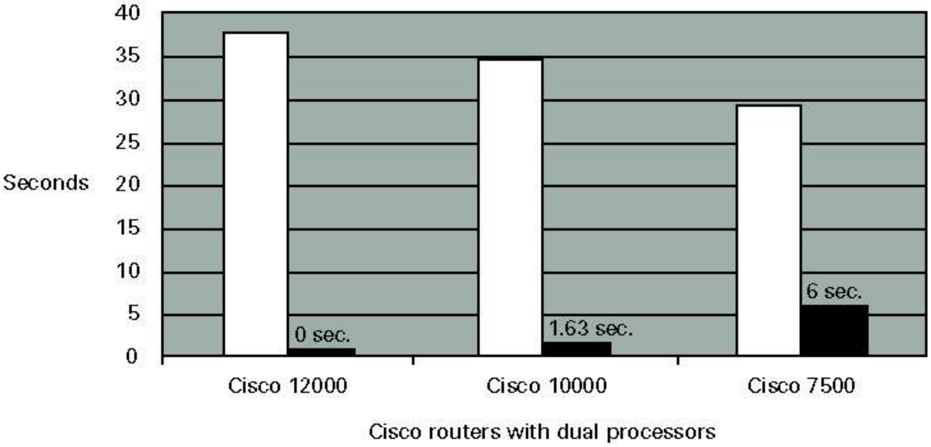
The Cisco 10000 Series Internet Router is an example of a practical implementation of many of these principles. Modular and redundant design is used extensively, with every element of the hardware designed for a minimum of 100,000 hours MTBF. Parity checking and error-correcting codes guard against memory errors, and both active and standby components are continuously monitored for proper operation. Every card slot has redundant point-to-point connections to the backplanes, and the entire unit complies with stringent service provider environmental requirements. Figure 4 shows the front view of a Cisco 10000 Series Router.

Figure 4
Cisco 10008 Internet Router Front View


Online insertion and removal for all Elements
Redundant N + 1 cooling
Redundant AC or DC power supplies
SONET APS + 1 redundancy
Redundant PRE
Redundant point-to-point backplane

The Cisco Route Processor Redundancy Plus (RPR+) feature allows a route processor failover to occur without resetting or reloading the line cards, thus reducing downtime, although session state is lost. When the Cisco IOS Software Stateful Switchover (SSO) feature is also used, however, session state is maintained. The active route processor synchronizes or checks information with the standby route processor so that if the standby route processor needs to take control, no packets are lost and no information corrupted. Independent lab tests (conducted by Mier Communications, Inc.) show that the SSO feature can significantly improve the availability of network applications such as VPNs. Figure 5 shows "before and after" tests conducted on several Cisco router models equipped with dual route processors. While actual results vary by hardware platform, the Cisco 12000 Series Internet routers reached zero time with SSO activated.

Figure 5
Cisco Router Failover Time Test Results



Source: Mier Communications, March 2002

Frame Relay Fast Restart is another platform improvement that increases availability. It greatly reduces the time needed to reactivate Frame Relay interfaces when a route processor switchover occurs. Restart time reductions can be as significant as 85 percent. Testing the designed product is a critical component to ensure reliability and availability. Cisco follows the Telcordia (formerly known as Bellcore) Reliability Manual (document SR-TSY-000385) for more complex products, and the Telcordia Methods and Procedures for System Reliability Analysis (document SR-TSY-00171) for simpler products. Telcordia has also published a set of standards that equipment installed in telephone company central offices must meet: the Network Equipment Building Standards (NEBS). These standards address issues such as resistance to earthquake, vibration, and falls, ranges of temperature and humidity in which the equipment must continue to operate, fire resistance, and electronic emissions. Cisco has an entire building devoted to the environmental and standards testing of its products. These test facilities have shake tables, temperature and humidity chambers, fire test stands, large anechoic chambers to test electronic emissions and interference, and knowledgeable staff. The Cisco test facilities have been reviewed and approved by various organizations such as Underwriter's Laboratories and the European Standards Testing Institute (ETSI).

While some equipment vendors' top priorities are low product prices, Cisco stresses high quality and reliability, knowing this policy will result in both better network service and in lower total cost of ownership over time.

THE IMPORTANCE OF SOFTWARE

While hardware failures may cripple a network, network managers are increasingly finding that software or its configuration is a greater source of risk.

> **"In the 21st century, it won't matter who has the best hardware, but the best software. That's how the defects per million figures are going to come down."**
>
> —AT&T's Chief Technology Officer, as quoted in Telephony Magazine

To minimize software-related failures, product designers must consider code design to prevent faults, means of rapidly detecting faults when they occur, means of isolating or containing a fault, and techniques for recovering from the fault.

How can software faults be prevented? Avoiding logic and coding errors and extensive testing to find and fix errors that creep in is essential. The development and testing procedures Cisco has established have qualified for ISO 9000 designation. Design staff and management constantly anticipate problems (such as a shortage of memory or a buffer overflow) that can make all the difference in the final result. Cisco IOS Software is the most stable and utilized software in the networking industry. The latest releases have a measured availability of more than 99.9999 percent. While Cisco takes pride in the quality of the Cisco IOS Software, the company also knows that "zero bugs" is difficult to achieve. To help its customers' networks be as reliable as possible, Cisco publishes information about known software problems and suggested ways to avoid or work around them until permanent fixes are implemented on its Website at Cisco.com.

Many techniques can be employed, some in software and some in hardware, to detect software faults in operating equipment. A fault detection agent can monitor key operating or performance values, such as free memory. System managers can detect the abnormal ending of a process. "Watchdog" timers can run out without being reset, causing a process to be terminated or a hardware reset to be initiated. Watchdog functionality can also guard against infinite loops, software deadlocks, or prioritization problems that might be difficult to detect by other means. They may be implemented in hardware, in software, or in both.

Many common software problems relate to memory usage. Cisco software engineers aim to design system software that can detect, report, and often fix problems including memory use growing in a static memory area, static memory allocations occurring in a dynamic memory area, memory not de-allocated by a stopped task or application, and tasks that are about to run out of stack space.

Check pointing allows a software component to store a consistent copy of its internal state in temporary storage so that it can be read back on restart after a software process crash. This function can also be used to synchronize the internal state between primary and backup redundant software processes. Check pointing can be done in immediate mode (where the process requesting check pointing is suspended until the checkpoint operation is completed) or in delayed mode (where an independent background process handles the check pointing operation without suspending the calling process). Checkpoint data can be stored on the same card where the calling process is running (the fastest approach) or on a different card entirely (facilitates online insertion and removal of cards).

Fault containment contains the effects of any fault to the least possible number of components. Avoiding the use of shared memory space, breaking complex software into many independent processes, and carefully inspecting and restricting any API calls are widely used techniques. (This discussion uses different elements of a single system as illustrations, but the general principles apply to preventing software corruption, of routing tables for example, from spreading across a network.)

The error recovery process includes the actions taken after an error has been detected in order to minimize disruption to the operation of the overall system. Critical design elements include minimizing the time required to switch over to different hardware, to reset a card, to rebuild a node, or to resync two sets of software, and various approaches to avoid database corruption. Another example is designing a system such that if a single line card crashes, only the software for that line card-not the entire system-is reloaded. This is a typical Cisco product design feature.

Software can also play a major role in overall network availability at a higher level than within individual devices. Cisco recently announced the Globally Resilient IP initiative to help ensure that software and design protocols deliver zero packet loss end-to-end across an entire network. This goal is accomplished by ensuring that Layer 2 connectivity is continuous, that packets are continuously forwarded, that IP network services (address translation, for example) are stateful, and that network services such as Multiprotocol Label Switching (MPLS) properly allocate bandwidth and handle node, link, or path failures. Dozens of specific software (and in some cases, related hardware) features are involved, but the goal is the same for each of them.

Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) are two other examples of Cisco IOS Software features that enhance reliability at the network level. These protocols enable a set of routers to work together to present the appearance of a single virtual router or gateway to a set of IP hosts. By sharing an IP address and a Media Access Control (MAC) address, two (or more) routers acting as a single virtual router are able to transparently continue the routing functions in case of a router failure, a power failure, scheduled maintenance, or other reasons. These features allow hosts on a network to use static configuration for their default gateway, and to continue to forward IP packets to a consistent IP and MAC address at all times, further enabling the transparent changeover of routing devices.

Having the network service provider use the same software that is used in the enterprise network minimizes compatibility issues, allows easier scaling of the network, facilitates adding or changing services on the network, and simplifies keeping up with the constantly evolving network requirements and features.

BEST PRACTICES FOR HIGH AVAILABILITY—ENVIRONMENT

As data networks become increasingly business-critical, the need to protect the physical environment of data centers and other equipment locations becomes more apparent. Most enterprises have some sort of disaster recovery (also called business continuity) plans in place, and recently, many such plans are being reviewed and strengthened. Environmental considerations such as power, air conditioning, access security, and other matters, while only one element of a comprehensive plan, have become more important than ever.

Service providers who want to offer highly available services must address these same issues. A visit to the data center or central office of a prospective service provider can reveal a great deal about its approach to reliability and security and the level of service likely to be delivered.

During a visit to a service provider, look for multiple power feeds to the building and an adequately sized UPS and generator set. Fire detection and suppression systems are critical, as are sensors for water detection under the raised floors, and physical bracing of equipment racks to cope with earthquakes, tornados, and other natural disasters. Air conditioning systems need to be redundant and have adequate capacity for a fully built-out center. Most data communications equipment operates normally at temperatures up to 40° Celsius (104° Fahrenheit), but Cisco experience has shown that hardware failures increase approximately by a factor of two for every 10° C increase beyond that.

There is an important relationship between network security and network availability. A network that has been compromised may not be available for its regular users, or may not deliver expected performance in other ways. While the physical aspects of the building are the starting point, it is also important to know what sorts of identification is required for visitors, if they must be escorted, what entrance and exit records are kept, and how extensively video surveillance systems are used.

Many security-minded network service providers have implemented the Cisco context-based access control (CBAC) feature in their networks. CBAC provides secure, per-application access control across network perimeters. It is significantly more secure than traditional access control lists (ACLs) because it takes the application type into account when deciding whether to allow a particular session across the network perimeter. Detection of suspicious network traffic is much easier and is especially useful in controlling Java applet downloading and in detecting and preventing denial-of-service attacks. Another interesting feature of Cisco ACLs is the ability to set them up to automatically change at certain hours. With this feature, for example, network security parameters can be different on weekends than from 8 am to 6 pm weekdays.

The service provider should also have implemented IP address filtering and rate limiting of unexpected traffic. IP address filtering (described in detail in the IETF's RFC1918 and RFC2827) prevents IP addresses that should be used only within an enterprise from traversing its network, and filters out any traffic with inappropriate source addresses (that are not part of the organization's assigned IP address range). Both of these types of traffic are suspicious, and filtering them discourages potential hackers from using the network to spawn malicious attacks.

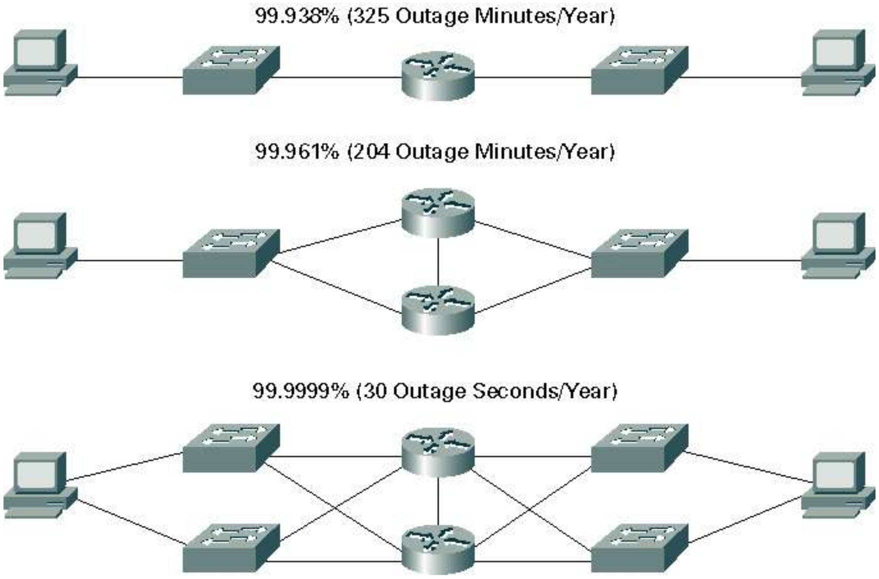
BEST PRACTICES FOR HIGH AVAILABILITY—NETWORK DESIGN

In helping its customers achieve higher network availability, Cisco network design practices take the end-to-end perspective, including the LAN and enterprise backbone, the enterprise premises edge, the service provider aggregation edge, and the service provider core. In each of these areas, similar principles apply:

- Increase modularity (and thus redundancy);
- Reduce complexity (more on this later);
- Strive for consistency (in operations procedures, for example)

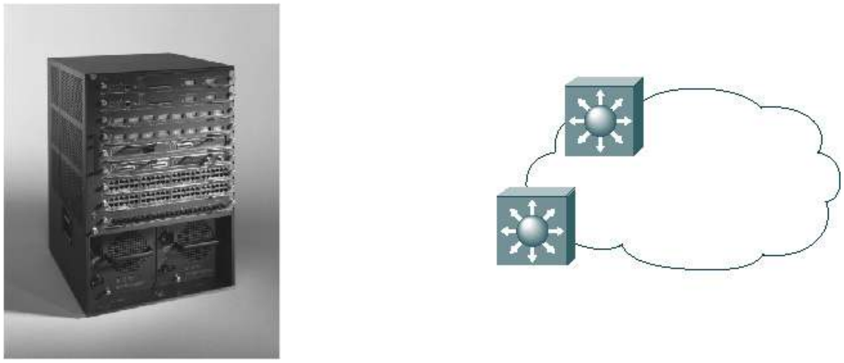
Avoiding any "single point of failure" is a major goal in network design. There should be few instances where there is only one of anything: routers, switches, servers, cache engines, etc., or paths connecting all of these. Servers should be dual-homed to multiple Ethernet switches. The impact of redundancy can be dramatic. Figure 6 illustrates a campus environment and traces an end-to-end connection from one user to another. The simplest design has many single points of failure and has a calculated availability of 99.938 percent, or about 325 minutes (more than 5 hours) of outage each year. Adding redundancy significantly improves this failure rate, down to about 30 seconds per year, in the last example design.

Figure 6
End-to-End Availability (4 hour MTTR in all cases)


99.938% (325 Outage Minutes/Year)
99.961% (204 Outage Minutes/Year)
99.9999% (30 Outage Seconds/Year)

Another factor to be considered in providing redundancy is whether to specify equipment that has redundant modules in it, to specify redundancy at the chassis level, or to do both (see Figure 7). The former approach may allow easier in-service card swaps or upgrades, but may also lengthen fail-over times. Ensuring that the spare module is working properly can sometimes be a problem (for example, are there background diagnostic software routines constantly running on the spare module?). Chassis-level redundancy can avoid the active-standby issues, but because this choice requires that fail-over communication be via a protocol; upgrades can be more complex to coordinate, and often require the network to reconverge.

Figure 7
Module Redundancy vs. Chassis Redundancy



Including load balancing in the design is important, whether Web and other application servers are located internally or at a network service provider's data center. The most effective load balancing techniques use switches that are content-aware (they understand the applications in use and user-specific items such as sessions and cookies) and does a far better job than a conventional Ethernet switch. Load-balancing capabilities allow for graceful degradation of network performance rather than quick collapse when traffic loads exceed predicted levels or traverse the network in unpredicted directions.

In addition to load balancing between servers, the best server network designs often include several extra servers and load-balancing systems that can automatically replicate suddenly popular data onto them. This capability in effect temporarily increases the number of servers handling a particular set of data. An example of this is a quick surge of traffic to corporate news pages immediately following a factory fire, plane crash, or other high-profile disaster. This kind of unexpected surge in traffic is sometimes called a “flash crowd” phenomenon, because not only is it an unexpected traffic peak, but it also develops rapidly.

A good network design also considers the physical routing of connections from the enterprise to the service provider. Having two cables both routed through the same conduit doesn’t offer much protection against physical damage.

At the service provider level, the points of connection to the enterprise network (often called points of presence, or POPs) should be dual homed to multiple data centers, or better yet, connected to all of the network service provider’s data centers via a mesh-style network.

IN NETWORK DESIGN, SIMPLICITY MEANS RELIABILITY

Reducing network complexity is another way for a network service provider to achieve higher network availability. Minimizing the number of vendors supplying network equipment is one approach to this. The more vendors there are, the more complex the IT environment becomes.

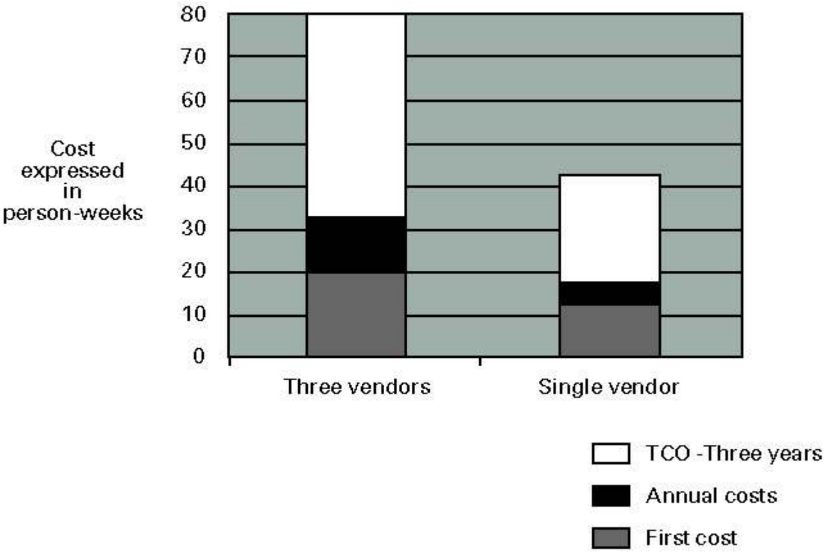
Thanks to industry standards, network components from almost any vendor can be made to work together. But the ease of doing that—and the likelihood of keeping the end-to-end network working—is a different matter.

In a recent survey of its readers, *InformationWeek Magazine* learned that more than 90 percent of those surveyed felt that network and IT complexity made the network more difficult to manage and is wasteful, stressful, and expensive. The same percentage agreed that simplifying any aspect of IT leads to greater business benefits.

Having equipment from multiple vendors in a network compromises service availability in two ways. First, operations staff is more likely to make mistakes with each additional brand of equipment they are expected to know about; it’s hard to be an expert on everything at once. Second, when something does go wrong, it often takes longer to identify the problem, fix it, and restore the customer to service.

Studies of several large enterprise and service provider networks drew the same conclusions about the affect of network complexity on both initial cost and total cost of ownership. Figure 8 summarizes the key findings of one study, (*The Business Case For a Primary Vendor*, The Registry, Inc.), expressing the results in person-weeks. It is true that complexity can arise from sheer scope and geography of the network, number of services and protocols supported, etc., and from the effects of multiple vendors, but vendor diversity is the easiest to control. The study confirmed that operations expenses, over a three-year period, could effectively be cut in half by the adoption of a primary vendor strategy.

Figure 8
Cost Impact of Multiple Vendors



Source: The Registry, Incorporated

These same principles also apply to network service providers. A service provider that has chosen one primary vendor for its network infrastructure has a procurement policy emphasizing greater reliability and service for their customers. On the other hand, those with numerous vendors may be indicating that they place greater importance on buying each component of their network based on what is new or on sale than they do to overall network operations, reliability, and customer satisfaction.

BEST PRACTICES FOR HIGH AVAILABILITY—NETWORK OPERATIONS

Robust, well-designed equipment, an excellent network design with good attention to redundancy and flexibility, and a solid physical environment are essential, but errors by the network service provider's operations staff can easily undo these efforts. The Gartner Group reports that no less than 40 percent, and in some cases as much as 80 percent, of network unavailability can be attributed to human error. (See report in CNET News, 1-26-01.)

Managing operations starts with finding and retaining a knowledgeable staff. This task is no easier for a network service provider than it is for a large enterprise. However, people with some experience and skills (Cisco career certifications, for example) can be easier to find in the marketplace than others. And as noted above, the fewer types of equipment installed in a network, the simpler the hiring and testing process becomes.

Once hired, operations staff must be trained, both to fill in gaps in their general knowledge and about specifics of the network they're now working on. Enterprises and service providers with multivendor networks frequently find they are faced with conflicting objectives; seldom do budgets (and time) allow for all employees to be sent to every available training class. This reality often results having individual specialists for particular pieces of technology—John knows about this equipment but not that, Fred is the expert on this other gear, and Mary is the only one who can configure "the new box." This situation is not only inefficient, but can lead to mistakes (when John has to work on Mary's equipment) and to delays (resolving many network problems may now take a minimum of two technicians, who are further delayed by needing to translate terminology and knowledge from the frame of reference of one vendor to that of another).

One way vendors like Cisco help network managers achieve operations excellence is by paying close attention to the maintenance aspects of products during design. An example that seems simple—but has far-reaching implications—is keeping track of configurations and configuration changes in all the devices in a network. Unlike most vendors, Cisco uses text-based configuration files, which are easy for network management applications to capture and store, and to review and analyze later.

Minimizing the need for operations staff to perform numerous manual tasks is another way Cisco indirectly helps improve network reliability. Many Cisco IOS Software features, for example, ease configuration work. The Cisco AutoQoS function, initially implemented for voice-over-IP (VoIP) applications, provides a centralized Web-based tool to manage network-wide quality of service (QoS) policies. With minimal keystrokes and manual effort, Cisco AutoQoS can automatically detect the presence of Cisco IP phones, and determine and apply the appropriate router and switch configuration settings for key variables such as link fragmentation and interleaving, header compression, best traffic shaping for the available Committed Information Rate (CIR), encapsulation, and queuing parameters. Cisco AutoQoS also monitors QoS performance, generates appropriate alerts and reports, and provides data to SNMP servers.

Cisco offers element management and network management systems to the operations staff, enterprise and service provider alike. The CiscoWorks product offers the enterprise manager a complete “toolkit” with a range of solutions from the basics (CiscoWorks LAN Management Solution) to the more specialized (for example, CiscoWorks Voice Manager, CiscoWorks Wireless LAN Solution Engine, CiscoWorks IP Telephony Environment Monitor, and CiscoWorks VPN/Security Management Solution). CiscoWorks offers several security-oriented products, such as the Cisco Secure Access Control Server and the Cisco Secure Intrusion Detection Director.

Network service providers have an extensive array of network management systems installed. These applications are often called Operations Support Systems (OSS), or sometimes OA&M (for Operations, Administration, and Maintenance). The systems are frequently deployed in accordance with the Telecommunications Management Network (TMN) framework created by the International Telecommunications Union (ITU), a United Nations agency. The TMN divides the required functions into element management, network management, and service management layers. The TeleManagement Forum (TMF), however, took a different approach, and coined the acronym FCAPS, to describe not the levels, but the specific functions needed in OSS applications. FCAPS stands for Fault, Configuration, Accounting, Performance, and Security Management). Table 1 shows examples of how these two common approaches to categorizing OSS applications relate to each other.

Table 1. A Functional View of TMN Applications and FCAPS

	Fault Management	Configuration Management	Accounting	Performance Management	Security Management
Service Management	Testing, reporting, and notification	Installation and deployment	Pricing	Reporting	Profiling and fraud management
Network Management	Event correlation and filtering; fault testing and isolation; trouble tickets	Connection and installation management	Correlation and storage	Aggregation, trending and characterization; capacity plng	Pattern analysis; breach response and recovery
Element Management	Alarm localization, logging, and correction	Loading, administration, and status	Collection and validation	Collection and analysis; capacity plng.	Alarm and audit trail management
Network Elements	Failure detection, reporting	Configuration validation and enforcement	Usage data generation and storage	State change detection and reporting	Access control; intrusion detection, reporting

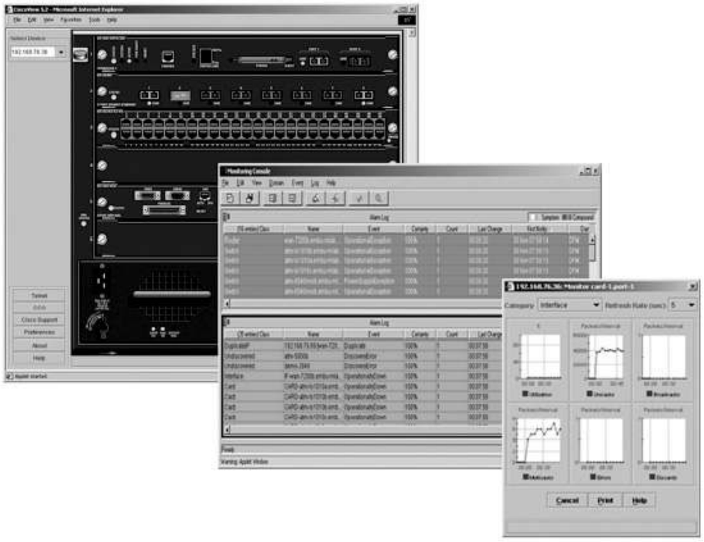
The Cisco Element Manager System is a range of device-specific element managers based on a highly scalable, tested, and field-validated common infrastructure (many are based on what was previously referred to as the CEMF, or Cisco Element Management Framework).
This consistent system approach has delivered a wide range of carrier-grade element managers across Cisco service provider product lines. The

Cisco Element Manager System provides a common set of graphical user interface (GUI) applications and administration tools for network operations center (NOC) operators to increase NOC productivity and reduce operations and training costs. This system allows for new service delivery with fewer highest-level engineers such as those with the Cisco CCIE® certifications. With real-time inventory discovery capabilities and standard interfaces to simplify integration with existing OSS units, Cisco element managers help ensure quicker deployment of Cisco networking equipment, and provide comprehensive element service assurance applications for faster turnaround of network problems. They provide NOC element layer administration and troubleshooting tools to reduce operational costs and increase productivity for service provider network operations—with OSS integration capability for element information access and high availability as mandatory customer expectations.

The common look and feel of the Cisco Element Manager System—across multiple network technologies such as routing, switching, DSL, Voice/IP, cable modems, and wireless networks—helps simplify tasks while also reducing personnel training costs. A user can change from one application to another without the need to come up to speed. For example, a user can move from viewing an alarm on a core router to looking at a status screen for an Asynchronous Transfer Mode (ATM) switch to reviewing a performance summary for a dial-access server quickly and easily (see Figure 9).

Figure 9

Typical Web-Based CiscoView Screens



Examples of Cisco Element Manager System features include:

- Map viewer (provides an overview of all managed network elements)
- Auto discovery (finds devices on the network)
- Deployment wizard (facilitates faster, more accurate equipment deployment)
- Event browser (helps identify and resolve network trouble reports)
- Event manager (provides fault analysis and reporting)
- Performance manager (monitors and displays device performance data)
- Access manager (provides secure access to network elements and information)

- Object group manager (groups network elements by organization or geography)

Cisco also offers products referred to as domain management systems, which look across a set of devices and network elements related to a particular service offering. For example, the Cisco VPN Solutions Center focuses on extending basic element management functionality to reduce operations costs while enabling the network manager to quickly and easily deploy services such as VPNs or IP telephony across multiple devices.

THE CISCO COMMITMENT TO HIGH AVAILABILITY

Cisco is committed to the goal of zero-packet loss networks and continually seeks to improve its products while working with groups such as the IEEE and the IETF to lead the industry. Dynamic Packet Transport (DPT), the basis for the IEEE's Resilient Packet Ring (RPR) standard, tag switching (now the industry standard MPLS), and recent routing protocol convergence improvements are a few examples.

The Cisco Globally Resilient IP (GRIP) initiative is a recent example of this focus, and includes end-to-end high-availability improvements in five areas: routing protocol convergence, the enterprise backbone and edge, and the service provider edge and core network. These new developments are rapidly being introduced across many Cisco product lines, especially the Cisco 12000, 10000, 7600, 7500, 7200, 7100, 6500, and 6400 series.

Some examples of GRIP effectiveness in routing protocols are:

- IP event dampening (which eliminates up to 50 percent of potential packet loss caused by link failures by applying the concept of Border Gateway Protocol [BGP] route-flap dampening to all IP routing protocols)
- BGP convergence optimization (which delivers up to 40 percent improvement in convergence time)
- Incremental Shortest Path First (SPF) Optimization (delivers up to 90 percent improvement in convergence time in OSPF and Intermediate System-to-Intermediate System [IS-IS] networks, depending on network size and fault nearness)

In addition, Cisco routers that use the BGP protocol "pack" updates before sending them to peer routers, reducing both router processing time as well as network convergence time.

Within enterprise networks, the Cisco GRIP initiative has concentrated on allowing edge functions such as Network Address Translation (NAT) and IP Security (IPSec) sessions to be handled in a stateful manner, improving the Gateway Load Balancing Protocol—to increase utilization on links to service providers, and getting multicast convergence—following unicast routing recovery—into the almost-instantaneous, sub-second range. Stateful NAT and stateful IPSec maintain session connectivity during first-hop takeover events, so that all security associations and tunnels are maintained and preserved.

Service providers can gain link and node protection in MPLS core networks (reducing cutover times to backup paths from tens of seconds to less than a tenth of a second), and zero packet loss at edge aggregation points with Cisco Nonstop Forwarding with Stateful Switchover. Cisco Nonstop Forwarding is critical for converged networks carrying IP telephony or video traffic, where loss of only a few packets can have a significant service impact. Stateful Switchover provides zero interruption of Layer 2 connections (for example, PPP, Frame Relay, ATM, High Level Data Link Control [HDLC], Ethernet) from virtually any hardware or software fault. It also prevents route flaps between participating neighbor routers, further increasing network stability.

Service provider networks built with MPLS technology are enhanced as well. A series of improvements make reroutes occur much more rapidly, at the link and node level, and protect the MPLS label-switched paths (LSPs), enabling all traffic carried by an LSP to be rerouted around a failure within milliseconds.

Cisco also offers professional services to help enterprises and service providers to improve network availability. For example, the Cisco Network Availability Improvement Support (NAIS) service works with customers to identify and resolve gaps in the areas of network design, network management, and operations process and procedures.

THE SIGNIFICANCE OF THE CISCO POWERED MARK

Cisco has made the process of selecting a network service provider easier with the establishment of the Cisco Powered Network designation. Less than five percent of the service providers in the world have qualified for the Cisco Powered Network designation. When using network services with this designation, recognizable by the display of the mark (see Figure 10), an enterprise can feel confident that the service is based on Cisco equipment end-to-end and that the service provider follows industry best practices in design, operations, and maintenance. These best practices include:

- Configuration management (configuration consistency, software version control, test plans, back-out plans, password management, naming conventions, and documentation)
- Performance and capacity management (base-lining, capacity planning, and QoS management)
- Fault management (fault detection, resolution, escalation, analysis, out-of-band management, and help desk metrics)
- Security management (policies, access control, partner management, intrusion reactions, and CERT network security advisories)
- NOC management (organization and staffing, operations procedures, record keeping, trouble tickets, escalation procedures, and exception reporting)

Figure 10
The Cisco Powered Mark

To keep network service levels at their highest, service providers who qualify for a Cisco Powered Network designation are invited to take advantage of network audits performed by Cisco professionals. This audit takes a “snapshot” of the service provider’s network, examines configuration and other software issues, and provides a summary and report with specific recommendations to the network service provider. Service providers can also take advantage of various no-cost or discounted training opportunities on Cisco products and technologies to help address staff training needs and thus bolster the competence of operations staff.

By becoming a part of the Cisco Powered Network family, Cisco expertise and resources become a part of the service provider’s overall solution in every aspect of the business. Authorized providers offer predictable performance and top quality service; benefits that are less likely to occur with networks built out of various point products from different vendors.

To achieve Cisco Powered Network status, service providers must establish clear standards for network performance and customer service, report or publish these results against these standards, and offer SLAs to their customers. Cisco believes the greatest value of an SLA is in making sure that all parties agree on network performance standards, responsibilities, and what happens when something goes wrong. Through a well-designed SLA, the network service provider becomes a partner to the enterprise in meeting its business networking goals. SLAs provide an incentive for network service providers to quickly correct problems and to keep networked applications up and running. Much like a life insurance policy, however, an SLA is something that should never be collected on, since payments under typical SLAs don’t come anywhere near the levels of potential lost business.

Another aspect of SLAs that bears on network availability is how the enterprise user can determine whether the network service provider is meeting the terms of the SLA. In a complete network failure, there usually is no question, but for less obvious network degradations, there might well be. A service provider that makes network performance results readily available tells their customers that they have good results, and takes pride in them. Cisco encourages service providers to make such information available on the Web, in monthly and on-demand reports, and also encourages enterprise customers to take the time to understand their particular negotiated SLA.

Security-minded network service providers will have installed intrusion detection systems (IDS) in their network. These products monitor all traffic in the network, looking for suspicious activity or traffic, and automatically alerting network operations personnel. Even the simplest IDS capability from Cisco uses signature analysis to identify 59 of the most common network attacks and information-gathering scans. Suspicious traffic can be logged, creating an audit trail for later review, and if desired, causing the routers to automatically drop the doubtful packets. The most recent Cisco products provide preventive protection against entire classes of attacks by also analyzing and reacting to the behavior of the system under attack.

Many tools are now available to help enterprise users determine whether a network service provider is meeting the terms of a negotiated SLA. The Cisco Service Assurance Agent (SAA), built into the Cisco IOS Software, can measure SLA performance end-to-end, or across any segment of a network or VPN service. Cisco SAA software acts as both source and responder, and measurements can be made to and from any Cisco IOS Software-based equipment, and to some equipment at the end of the network that is not manufactured by Cisco, such as printers and file servers. Measurements available through the Cisco SAA include not only traditional data-oriented parameters such as availability, connect times, round-trip delay times, and packet loss, but also more advanced metrics such as end-to-end and hop-by-hop response times and jitter (interpacket delay variance, especially important for voice/IP applications). The Cisco SAA measurements are based on synthetic operations (time-stamped test messages, for example) and don’t disrupt normal traffic flows. These capabilities far exceed solutions based on add-on boxes.

To help promote network security and reliability, service providers with a Cisco Powered Network designation can avail themselves of a no-cost security assessment, which provides “friendly” hackers from Cisco who try to penetrate the service provider network at an agreed-upon time. The goal is to find and fix vulnerabilities before network intruders discover them.

Network service providers that display the Cisco Powered Network designation for their Managed Security Services show that they have special expertise with respect to firewalls, access control lists, IP address filtering, and other tools of the security trade.

CONCLUSION

There are many factors involved in achieving the high levels of network availability that today’s business-critical applications demand. This white paper emphasizes two points: the unique value that Cisco brings and the important role network service providers play in realizing these goals. Businesses achieve network reliability and availability by paying attention to numerous points, large and small, and isn’t something that can be added on without forethought and planning.

Overall network availability also relates to exactly what is expected of the network service provider. When the service is basic Web hosting, a network service provider must focus more on its physical environment and network connectivity, while a network service provider offering managed services requires a much broader range of in-house skills and processes. Cisco highly recommends SLAs, but only as a means of aligning expectations, not as something an enterprise should hope to collect on.

To be confident that your entire network, including portions outsourced to a service provider, will contribute to the resiliency and success of your business, consider an end-to-end solution, buy reliable, well-tested network elements, reduce complexity, ensure your staff is knowledgeable and trained, and use service providers that have achieved Cisco Powered Network designations.

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.
168 Robinson Road
#28-01 Capital Tower
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 Website at** www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • 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

SB/LW6661 07/04

Printed in the USA