How Cisco IT Uses Its Own IT Technologies to Achieve Business Resilience

High availability and redundant network architecture protect infrastructure from disruptions.

Cisco IT Case Study / Business Management / Business Resilience: This case study describes Cisco IT's internal deployment of Cisco® products for the company's internal network, from planning to implementation. Cisco deploys its own products to assure the continual operation of its internal network and IT infrastructure, as well as the continued productivity of its employees. Cisco's leading-edge enterprise environment is one of the largest and most complex in the world; Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

"Designing the network and IT infrastructure for the stability of Cisco's business is our number-one goal."

– Craig Huegen, chief network architect, Cisco IT

CHALLENGE

Planning and preparing for disaster recovery and business continuity are important tasks for any enterprise. Many businesses focus their efforts on disruptions to the network and IT environment because these disruptions can have significant impact on business productivity, profitability, customer relations, and shareholder confidence.

A disaster recovery strategy is critical, but is only one element of a larger business resilience strategy. Business resilience helps an organization not only to recover from and adjust easily to unplanned events, but also to take advantage of new opportunities. A business resilience strategy covers more than just the network and IT infrastructure—it gives workers secure and reliable tools for communication, collaboration, and access to enterprise applications and data anytime, anywhere.

Like other companies, Cisco Systems relies on its network and IT infrastructure to keep its business running—but Cisco also uses its network to increase worker, application, and collaboration resilience. Cisco addresses its challenges for business resilience through a combination of proactive planning, well-designed procedures, and extensive use of its own products and technologies.

SOLUTIONS

Network Resilience

Cisco's enterprise network serves approximately 36,000 employees in more than 70 countries worldwide, carrying enormous volumes of data, voice, and video traffic. To assure business resilience, Cisco IT has developed extensive disaster recovery plans that prepare for a wide range of potential disruptions across the company, from the failure of a single network device in a local office to a major earthquake at the company headquarters in San Jose, California. "Designing the network and IT infrastructure for the stability of Cisco's business is our number-one goal," says Craig Huegen, chief network architect for Cisco IT.

Also important are measures to deter and mitigate security attacks on the network, desktop computers, phones, and data center systems. These attacks include viruses and worms distributed through e-mail or Internet downloads, as well as hacker intrusions and denial of service (DoS) attacks launched over Internet connections to the Cisco

network. Finally, Cisco IT must assure continued resilience of the network as it carries new types of traffic, such as IP voice and storage area networking.

Solution

At Cisco, network resilience is based on a high-availability network design, with a redundant architecture that automatically recovers or reroutes communications around failures. This design protects individual devices and the entire network infrastructure from disruptions caused by power outages, equipment and connectivity failures, viruses, security attacks, and similar events. Elements of the Cisco network design that support its resilience include:

- Backup WAN links and redundant hardware at important access points and network junctions.
- Reliable Cisco IOS® Software features that support resilience in Cisco routers and switches, such as nonstop forwarding (NSF), Hot Standby Router Protocol (HSRP), and stateful switchover (SSO).
- Backup support for environmental conditions (cooling, for example) and electrical power through Cisco redundant power systems and the Power over Ethernet (PoE) features in Cisco Catalyst® LAN switches.
- Standardized network equipment configurations that are maintained centrally and audited daily. When needed, configuration updates go through a rigorous control change process, then are downloaded from the Cisco Network Operations Center (NOC) at the company's headquarters. These controls reduce the need for manual configuration of routers, switches, and other network elements, and lower the associated risk of error.
- Monitoring of the entire Cisco network, 24 hours a day, from the central NOC, which allows the rapid problem detection and resolution that minimizes impact on users and business activity.

Campus redundancy. At Cisco headquarters, the local- and metropolitan-area networks (LANs/MANs) that serve more than 50 buildings are built with a redundant design. All routers are set up in pairs, all connections are duplexed with full bandwidth, and each intercampus link has an alternate path. Dual routers at the desktop network hubs use HSRP to provide high-speed, stateful failover between them. Within the Layer 2 switched networks in each building, spanning tree is enabled between the Cisco Catalyst 6500 Series switches, and the PortFast feature is enabled to minimize downtime in case of a switch failure.

The internal desktop network in San Jose operates on a Gigabit Ethernet core, which provides sufficient capacity for most campus traffic—some links between data centers are now running at 10 Gigabit Ethernet speeds. Each building has at least two fiber paths back to every other building to maintain reliability. This campus redundancy design is presented in greater detail in the Cisco IT Catalyst 6500 case study.

In other major Cisco campuses around the United States, high availability and redundancy in network links and equipment are configured throughout the core, distribution, and access layers.

Redundant WAN connections. All remote offices have primary and secondary links, configured with the same bandwidth, to the Cisco WAN. For many locations, Cisco IT uses leased-line SONET circuits to provide this redundancy. In addition, most remote parts of the Cisco network have a redundant equipment infrastructure in at least the core and distribution layers.

In locations where SONET circuits are expensive or unavailable, virtual private network (VPN) services provide the backup connection to the Cisco WAN. Cisco IT also uses VPN services for disaster recovery along the most critical WAN routes, such as when both the primary and secondary paths failed on a transatlantic cable. Read more about this design in the Cisco IT WAN VPN case study.

Quality of service. Quality of Service (QoS) mechanisms operate across the Cisco network, helping to ensure that the most critical voice and data traffic receives bandwidth priority, regardless of network status. With the QoS features in Cisco routers and switches, the network can adapt as needed to changing conditions. Read the Cisco IT QoS case study to learn more about this principle for business resilience.

Backup power supplies. All Cisco offices are supported by uninterruptible power supply (UPS) units that provide electrical power to switches, routers, and Cisco IP Phones for more than two hours. If power fails, users have sufficient time to back up their work and complete final business calls and transactions, minimizing disruption and data loss. Backup power for Cisco data centers is supplied by multiple UPS systems and two diesel generators, which also operate in a redundant design. PoE features in Cisco Catalyst switches deliver electrical power over the LAN connection to devices such as Cisco IP Phones and Cisco Aironet® wireless access points, keeping these devices operational in the event of a building power failure.

Application Resilience Application resilience helps ensure that employees have continuous access to data and applications, that applications perform as expected, and that data is securely replicated and stored to protect its integrity. Resilience planning in this area requires consideration of two issues. The first issue is the differing tolerances of applications for availability and data loss. The second issue is how to support application resilience within the data center, through optimized WAN links, properly configured QoS, and via content caching and delivery in remote offices.

To ensure application resilience, Cisco IT staff address numerous challenges, including maintaining application availability if the main data center is inaccessible, handling planned downtime of application and data servers, as well as distributing applications and data storage globally for better performance. Security planning for application resilience primarily considers attacks on servers and storage devices. But this planning must also consider protection of confidential company information, from a database breach to the risk incurred when an employee loses a personal digital assistant (PDA).

Solution

Mirrored data centers. Cisco's major application servers and storage systems are housed in a data center on the San Jose campus. A backup data center nearby provides full mirroring and failover if a problem occurs in the primary center. These data centers are connected by both optical links (using the Cisco ONS 15454 SONET Multiservice Provisioning Platform) and IP/SONET network links. Servers and storage are distributed between the two data centers, and operate in clusters for flexible system usage, failover, and data replication. Another data center in North Carolina serves as a disaster recovery site in case of a major event in San Jose.

Distributed applications. Cisco content services switches, Wide Area File Services technology, and Cisco Application and Content Networking System (ACNS) Software support resilience by distributing application traffic within the data centers and on local servers around the world. These solutions also support partial application use if the data centers are inaccessible. More information about Cisco strategies for application and content distribution is presented in the ACNS case study.

Security. Cisco security technologies and procedures are deployed throughout the company's IT infrastructure—controlling network access, detecting and mitigating attacks on application servers and data storage systems, as well as preventing disruption of desktop computers and Cisco IP Phones. The data centers are protected by integrated Cisco IDS 4250 intrusion detection systems to defend against direct attacks on servers. Cisco security teams are located in numerous countries for fast response to incidents, and can monitor security status through a virtual operations center.

An example of the value of these protections is how Cisco was able to address the Slammer virus in 2003. "Once we became aware of the Slammer worm, we used Cisco access control technologies to close off our internal network," explains Brian Christensen, director of infrastructure hosting in Cisco IT. "In particular, Cisco NetFlow technology helped us to determine if any occurrences of the worm had entered our environment. Within six minutes of learning of the virus, we had scanned and protected our internal network to ensure that Slammer made no impact." To learn more about how Cisco's security deployment has mitigated the impact of other attacks at the host level, see the Cisco IDS 4250 case study.

To protect corporate resources from new and unknown malicious attacks that are not stopped by traditional antivirus software, Cisco IT has installed Cisco Security Agent endpoint security software on more than 38,000 desktop and notebook computers used by employees. In addition, Cisco uses commercial virus scanning tools and an e-mail antispam service. For details on the benefits Cisco has realized from its internal deployment of this solution, read the Cisco Security Agent case study.

VSAN separation. Cisco IT maintains data in storage area networks (SANs) in the data centers, and makes extensive use of the virtual SAN (VSAN) feature on Cisco MDS 9000 Family multilayer SAN storage networking switches. The result is a more resilient data center—any issues related to storage system stability, security, or performance are isolated within the VSANs. Read more details about this configuration in the Storage Networking case study.

QoS. Cisco routers and switches support application resilience with features for defining distinct QoS parameters for different applications. These features help to ensure that critical locations continue to receive bandwidth priority as the resilient network design adapts to outages or other negative conditions.

Workforce Resilience Enabling Cisco employees to work easily anytime, anywhere is critical to business resilience. Workforce resilience focuses on giving employees the right tools and flexible network access to work productively inside and outside of the office in any situation. These resources must be portable, convenient, and easy to use.

Solution

VPN services and teleworker solutions. Broadly available throughout the world, VPN services are an essential element of the Cisco workforce resilience strategy. Once connected to the Cisco VPN, employees use tools on their home or notebook computers, such as Cisco VPN Client software for data, the Cisco IP SoftPhone or the wireless Cisco IP Communicator for voice, and Cisco VT Advantage for video communications.

In addition, the Cisco Business Ready Teleworker Solution securely extends campus services to the home, providing access to data and applications as well as automatic transfer of voice calls, voicemail, and features from the worker's office phone to a Cisco IP Phone at home. This solution enables Cisco employees to work productively when bad weather or other circumstances preclude travel to the office.

The outbreak of Severe Acute Respiratory Syndrome (SARS) throughout parts of Asia in 2003 provides one example of using VPN services and Cisco products for business resilience. "At the height of the SARS period, most of Cisco's 800 staff in China were working from home," explains Greg Dixon, Cisco IT manager in Beijing. "The Cisco IP SoftPhone played a major role in mitigating possible productivity loss. When we were preparing contingency plans at the beginning of the SARS epidemic in anticipation of office closures, we were surprised how little we had to do because we were already positioned well in terms of broadband VPN access from employee homes." Learn more about the implementation of VPN services for Cisco employees in the Cisco VPN Client case study.

PC security. With the explosion of electronic worms and viruses, strong security for desktop and notebook computers is critical for worker resilience. Products such as Cisco Security Agent protect employee computers from the impact of Internet worms and viruses, and prevent the computer from spreading the infection to other systems, even if the computer's antivirus software is out of date.

Wireless network access. All Cisco campuses have deployed Cisco Aironet wireless LAN access points, enabling employees to easily connect to the Cisco network in conference rooms, cafeterias, and other areas. This allows workers to remain connected to the network and work productively anywhere on a Cisco campus. Wireless-enabled laptop computers and Cisco VPN services also allow employees to securely connect to the Cisco network using wireless services in Internet cafes, hotel rooms, or home. More information about the use of wireless technology in the Cisco network is presented in the Wireless LAN case study.

Collaboration Resilience Collaboration resilience ensures the ability of employees to effectively communicate and work with others, in a variety of forms and over varied media, for faster response to evolving situations.

Solution

Cisco uses voice, e-mail, paging, and instant messaging systems to help employees communicate and collaborate with each other as well as with customers, suppliers, and partners. Employees need easy, reliable access to these systems around the clock, whether working in a Cisco office, in a hotel room, from home, or when traveling.

Converged IP network. Simply being able to re-route voice calls over a different path on the IP network can provide for continuous communications. When the public network voice service to Cisco's Glasgow office failed, Cisco network managers were able to work with the carrier to forward all incoming calls to a Cisco office in London, where they were routed back to Glasgow over the Cisco WAN. All outgoing calls from Glasgow were also routed over the WAN to the London office, where they were sent out of that office's public network connection.

Advanced Cisco IP Communications features also support workplace flexibility for Cisco employees. Cisco Unity® unified messaging provides a single mailbox that makes it easy for employees to retrieve all voice, fax, and e-mail messages from a computer or telephone. The extension mobility feature in Cisco CallManager allows employees to apply their own extension numbers to any Cisco IP Phone in the company's global network. Cisco CallManager automatically redirects telephone calls and voicemail to that phone, enabling the employee to immediately begin work in a different office.

Survivable Remote Site Telephony. Business resilience plans must assure continued communications if a centralized Cisco CallManager or Cisco Unity cluster is not operational or accessible. In its usual role, Cisco Survivable Remote Site Telephony (SRST) is used in branch offices to maintain telephone service in case of interruption in the WAN link to a centralized Cisco CallManager. Cisco also uses SRST in the same location as all centralized CallManager clusters to provide the connected Cisco IP Phones with continuing service. This gateway connection to the PSTN assures that voice calls can always be made from a Cisco IP Phone. Read about this communications design in the Survivable Remote Site Telephony case study.

Additionally, all Cisco employees can use the Cisco IP SoftPhone on notebook computers, enabling them to place and receive calls from any location with a network connection—even a wireless hotspot in a coffee shop or airport.

Success Factors The size and scope of Cisco's business and IT infrastructure makes business resilience planning and execution a complex effort. The most critical factors include consistent implementation of security, availability, management, and application optimization capabilities in the routers, switches, servers, and other infrastructure elements.

Because of Cisco's breadth and depth of products and technologies, Cisco IT can take advantage of the Cisco IOS Software features that are common to foundation networking technologies such as switches and routers, as well as advanced technologies such as Cisco wireless and IP Communications products. These features allow Cisco to build an integrated enterprise architecture that reduces cost and complexity, makes resources and applications more available and secure, and enables faster, stronger implementation of new capabilities for resilience across the enterprise. For example, Cisco HSRP, supported on multiple Cisco routing platforms, helps ensure that user traffic immediately and transparently recovers from first-hop failures in network edge devices or access circuits.

Cisco IOS technologies also support collaboration resilience. When one building on the Cisco San Jose campus experienced a power outage, employees were able to take their Cisco IP Phones and notebook computers, find vacant desks in other Cisco buildings, connect to the Cisco network, and resume work immediately. The Cisco Discovery Protocol feature on Cisco IP Phones, along with the AutoQoS and auxiliary VLAN features on the Cisco Catalyst switches, handled these moves automatically by assigning the correct QoS, VLAN, security, and other

features to the phones. Without these capabilities, transferring the phones to new locations would have required manual reconfiguration, and may have reduced security controls or voice quality.

RESULTS

Cisco has gained significant benefits from its efforts to assure business resilience, including:

- Highly available networks, applications, and data systems through principles such as redundancy and creative use of new services such as VPNs.
- Enhanced application survivability through mirrored data centers and distributed content.
- Survivable voice communications through local call processing and PSTN gateways.
- Protection of network and business assets with comprehensive security mechanisms and practices that address a wide range of threats.
- Employees who can work anytime, anywhere for both daily mobility and fast relocation to alternative sites under variable and unpredictable circumstances.

NEXT STEPS

“At the highest levels, Cisco supports business resilience by promoting network availability, mitigating the impact of security threats and information loss, and protecting the company’s corporate reputation,” says John Stewart, information security director for Cisco Systems. At Cisco, technology deployments, plans, and processes for resilience are continually evolving to serve a growing company, advancing technology, new types of security threats, and new business needs.

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.**