Maximizing Availability in the Branch with Integrated Services Routers

Executive Summary

In today's highly networked environments, nothing is more critical than availability—access to data, applications and content from anywhere, anytime. As enterprises and government agencies of every size become more geographically distributed, it is the branch offices that depend on the network the most. Whenever networks fail, multisite organizations lose, both in productivity and in profitability.

This paper discusses how to meet the critical need for high availability networking in branch offices by taking advantage of the Integrated Services Router's unique combination of high-availability features and capabilities for up to thousands of branch sites. This technology allows the router to enable more interfaces and options while dramatically increasing performance of multiple, simultaneous services and maximizing availability. Many companies are already installing Integrated Services Routers in their multisite locations.

The paper also examines current techniques for ensuring high availability and explains the importance of an end-to-end services approach, where resiliency and security are built into the fabric of the network and extend out to the edge of the organization. It highlights the evolution of Cisco's high availability capabilities, and the importance for network designers, operators, and administrators to build a culture that stresses zero downtime to ensure reliability in the face of change and future growth.

The Critical Need for High Availability in the Branch

Due to mergers, reorganization, and entrance into global markets, a significant percentage of today's enterprises and agencies are expanding into as many as thousands of locations. IT administrators are increasingly being asked to oversee these geographically distributed communications networks that store, protect, and deliver critical business information between branch sites.

Such organizations cannot tolerate downtime, or its impact on productivity, profitability, and competitiveness. Even a brief network interruption impedes operations and can have long-lasting effects. Overall, network downtime and service degradation cost companies with at least 1000 employees US$32.7 million each year in lost revenue and productivity, according to Infonetics Research.

Maximizing service availability at the branch requires networks designed for 24x7x365 uptime. Highly available branch networks need to:

- Ensure fast recovery from typical faults while minimizing or eliminating the impact on service
- Simplify network configuration and management
- Provide secure connectivity and automatically defend against attacks
- Optimize delay-sensitive applications such as unified communications and video
- Ensure continuous voice-over-IP (VoIP) services

Multisite organizations rely on networking for optimal connectivity at every point, from users' desks, PDAs, or phones, at the access point and the router, through the WAN to the hub, and in the headquarters system in the main office. Approximately 40 percent of employees now work in branch offices. High availability is especially critical in sites where productivity depends almost entirely on constant and secure connectivity with headquarters. Branch networks need to be particularly stable and robust, as most small offices do not have an IT specialist on site.

Network downtime may be planned or unplanned. Planned downtime usually involves network maintenance and upgrades. While planned downtime is scheduled to minimize impact on business, it may still cause inconvenience and loss of profits, especially for multinational companies operating in multiple time zones, Internet service providers (ISPs), or critical government agencies. Any network providing features to minimize the effects of network maintenance offers a significant advantage to IT strategies and the enterprise.

Unplanned downtime can be caused by problems outside of the network, such as power outages, link failures, or denial-of-service (DoS) attacks. Even more arise from problems within the network, such as configuration errors, poor network design, software or hardware malfunctions, lack of change management, a network management system for proper monitoring, or troubleshooting resources. Studies have shown that one of the greatest causes of failure in branch networks lies in errors made in network configuration. Another significant contributor is the loss of connectivity due to link and circuit failures.

Such unplanned downtime is the cause of significant business losses. According to Infonetics Research, an enterprise of 1000 employees or more experiences an average of 3.7 hours of WAN outages and 3.4 hours of services degradation per month. Over time, multisite organizations suffering even from infrequent downtime may experience significant loss of revenue and reputation, as well as lower financial performance and additional expense.

The Cisco High Availability Solution for the Branch

Cisco Systems® has been a leader in high availability networking for 25 years, providing end-to-end communications from the service provider core to the campus edge and branch. Unlike network component vendors who focus on point product redundancy features, Cisco® provides a complete strategy for high availability delivered across a multisite network. This approach minimizes deployment and maintenance downtime, mitigates attack, and gets the network back up quickly. It targets every potential cause of downtime, both planned and unplanned, by integrating resiliency features across the product line and evolving network design and operational best practices. This helps organizations transform distributed IP networks into self-defending, autonomic intelligent information networks. A critical step in this strategy is the introduction of the Integrated Services Router, now in its second generation.

> “The [new] Cisco router will become the communications hub of our new stores and regional offices. We’ll be able to deploy a single converged solution that is easier to manage, lowers our operating costs, and uses the infrastructure already in place.”
>
> **—A Leading U.S. Retailer**

These new generations of routers build services into the router hardware, enabling the simultaneous use of more interfaces and features while increasing performance of multiple, concurrent services. Built on this innovative new technology, Cisco is able to provide a networking foundation for branch environments that includes increased security via self-defending networks; self-healing, system-level analysis and management; enhanced video and communications services; third-party applications and server virtualization, and the integration of wired and wireless networks. Allowing network administrators to invest in just one box instead of four or five, the Integrated Services Router’s integrated, embedded system is designed to effectively manage networking well into the company’s future.

The Integrated Services Router accomplishes all of the above networking requirements by working with other devices as part of a collective system—a Cisco network that is designed for high availability from end to end. Cisco integrated services routers have been engineered to interoperate with the Cisco Advanced Services Routers (ASR) headend routers. The Cisco ASR series aggregation routers specifically are designed to deliver enhanced levels of

performance and availability, utilizing the modular software approach of Cisco's IOS XE operating system, enabling customers to build a truly integrated, efficient, and highly available end-to-end intelligent information network.

Cisco IOS Software, as run on the Cisco Integrated services Routers, supports an exhaustive set of standards and protocols. Based on these, each device in the network can use the network intelligence inherent in Cisco IOS Software to fully cooperate in providing resilient services. The importance of an end-to-end application services perspective cannot be overemphasized. All the benefits of deploying strategic applications evaporate if the underlying network is unreliable.

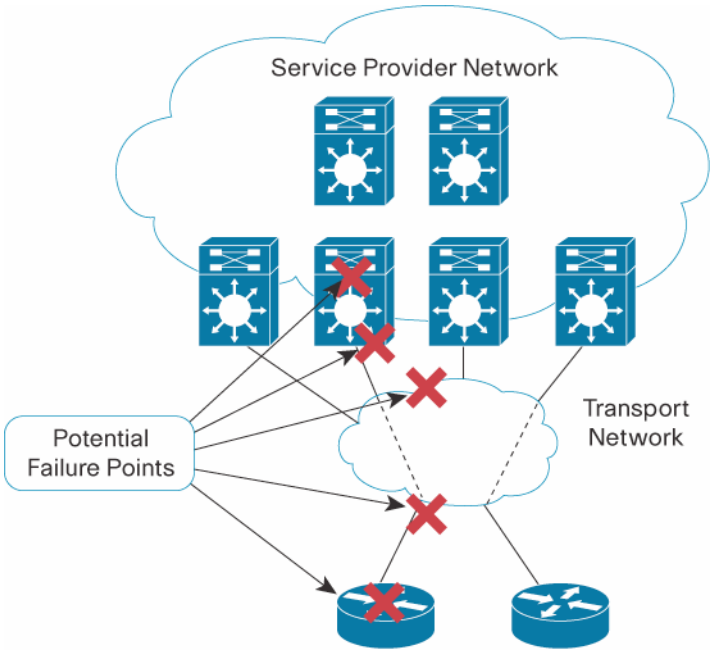
Fast Recovery from Typical Faults While Minimizing or Eliminating Service Impact

Faults can and will occur. However, a resilient network allows the network to operate even when problems arise, rapidly detecting faults and handling traffic in a predictable fashion according to the designed-in redundancy.

Availability breakdowns can be caused by different issues (Figure 1). Typical faults include:

- Hardware failures and loss of power
- Circuit or link failures outside of the branch office
- Software failures
- Poor performance due to lack of bandwidth management or unexpected traffic bursts

Figure 1. Points of Network Failure



Cisco's end-to-end networking offers a powerful series of high availability features to rapidly detect interface and link failures and route traffic over backup links. Cisco IOS Software also brings many capabilities to the Integrated Services Router to combat these points of failure, including robust routing protocols and first-hop redundancy protocols such as Hot Standby Router Protocol (HSRP), Gateway Load Balancing Protocol (GLBP), and Virtual Router Redundancy Protocol (VRRP) to route around failures. Effective quality of service (QoS) mechanisms prioritize traffic and make efficient use of all available bandwidth.

Managing Hardware Failures and Loss of Power

Hardware failures and power outages are rarely within the control of the network administrator, but Cisco can help to lessen the impact of such problems. Some Integrated Services Router models are designed to minimize downtime with features such as redundant hot-swappable power supplies, including a hot-swappable fan tray with redundant fans, and hot-swappable line cards. The Integrated Services Router includes ports for Power over Ethernet (PoE) based on the IEEE 802.3.af industry standard, which supports a remote power reset that eliminates late-night, onsite visits to reset network devices.

For hardware failures, online insertion and removal (OIR) of Network Module-Enhanced (NME) or Service Module (SM) allows administrators to utilize hot-swappable network modules in case one should fail. The Integrated Services Router also provides support for Error-Correcting Code (ECC) memory, which includes special circuitry for testing the accuracy of data as it passes in and out of memory. ECC supports network and application information to make failure impacts as transparent as possible to the user.

The ISR G2s build on the he resiliency features of the first generation while adding more hardware-based redundancy. All Cisco 3900 series ISRs now support both hot swappable power supplies and fan trays. The Cisco 2911 through 2951 models can support redundant power through an external RPS. Another hot swappable item on the Cisco 2921 and above are the SFP modules, allowing for rapid replacement of a failed interface, while the auto-failover feature allows that failed interface to dynamically map to another with a shared MAC address.

Another innovation on the ISR G2 family lies in the Service Ready Engine and the SRE-900. This module is designed to provide high-performance application support from within the router. The SRE concept allows for applications to be downloaded to the module remotely. From a hardware perspective, this module supports 2 500GB SATA hard drives. These drives are externally accessible and hot swappable as well. The drives can be configured to function using Redundant Array of Independent Disks (RAID) technology, achieving RAID1 or mirrored redundancy.

Responding to Link Failures from Outside the Branch

All Cisco networks are grounded on proven auto backup/auto failover technologies that transparently transfer the data stream to an alternate DSL or dialup connection in case of an upstream link or circuit failure, while autonomously backing up the server to save as much data as possible.

Important protocols such as GLBP and Multilink Point-to-Point Protocol (MLPPP) are built directly into the Integrated Services Router to assist in more effective management of data and to provide better use of resources while offering resiliency. Load sharing is particularly critical in remote environments. Most of the time, redundant routers and links placed for resiliency in event of failure are usually online. Innovations such as GLBP and Cisco Express Forwarding allow all available traffic paths to be used, increasing performance. Resiliency protection is available and critical traffic gets the best possible performance at all times.

The Enhanced Object Tracking (EOT) feature increases the availability and speed of recovery of a router system, decreases outages and their duration, and provides a scalable solution that allows other internal software processes such as HSRP, GLBP, and even static routes to track individual objects or a list of objects. Each tracked object is identified by a unique number that is specified using the tracking command-line interface. Client processes use this number to track a specific object. The tracking process notes any change of object state and then notifies interested client processes.

As more WANs move to ethernet-based access circuits, the ability to see these circuits end-to-end is critical. Ethernet Operations, Administration and Management (OAM) technologies provide this capability. OAM provides the service assurance over a converged network that service providers are looking for in an Ethernet network. Service assurance provides the detection, resiliency, and monitoring capabilities that are needed for service availability, increased service velocity, allowing auto-provisioning of equipment, and making end-to-end deployment easy

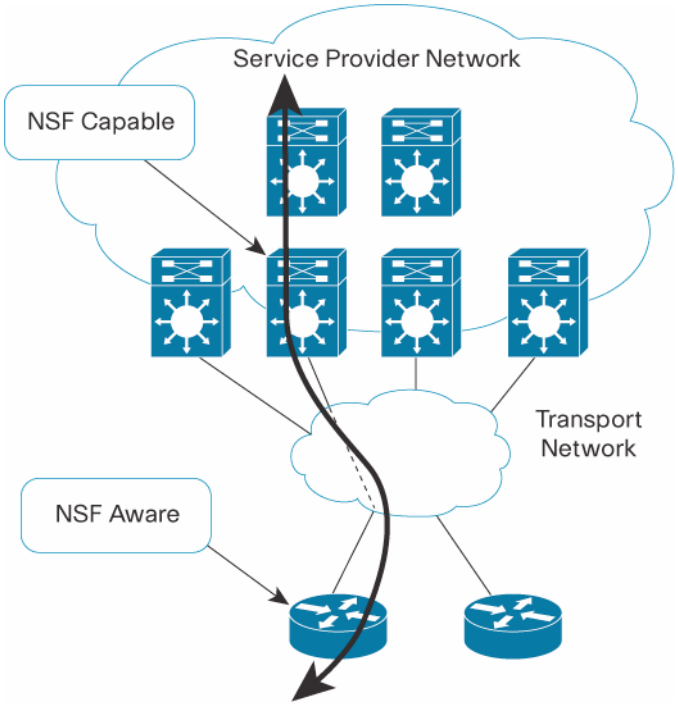
through connectivity fault management and link-level protection. Ethernet OAM helps the service provider to provide end-to-end service assurance across the IP/MPLS core, the Ethernet metro, and to the customer's premises.

Managing Hardware or Software Failure

The most common method of protection from hardware and software failures is the use of redundant equipment. The level of redundancy employed is usually determined by careful analysis of the risk, impact, and cost of downtime versus the added cost of redundant equipment. Such an analysis must be done on the network as a whole. The goal is to eliminate as many single points of failure as possible within a given budget.

Edge and aggregation routers are often determined to be critical failure points. For large networks with many branch locations, either the service provider edge routers or the enterprise edge routers (or both) are strengthened with additional redundant components. Cisco IOS Nonstop Forwarding (NSF) with Stateful Switchover (SSO) provides extremely high availability when redundant route processors are used (Figure 2).

Figure 2. High Availability with Cisco IOS Nonstop Forwarding (NSF)



For the greatest benefit, branch devices should also support NSF Awareness, which enables the branch router to continually forward traffic through a peer router that might undergo a switchover to redundant hardware. This allows the Integrated Services Router to help NSF-capable routers perform nonstop forwarding of packets. All Integrated Services Routers support NSF Awareness.

The Embedded Event Manager (EEM) also provides new components and methods to invoke customized local actions triggered by defined events such as a failure. EEM policies are created using a programmable scripting language founded in Tool Command Language (Tcl). This allows network operators to harness the vast network operational data and hardware and software diagnostics embedded within Cisco IOS Software, permitting them to monitor and proactively detect dangerous conditions that might affect network service. The EEM also includes methods to automate actions in response to those conditions. Tightly integrated with Cisco IOS Software, the EEM has intrinsic knowledge of the state of the network from the viewpoint of the device it is operating on. The ability to create programmable actions reduces reliance on a remote management system at headquarters and offers network

managers far more detailed fault control. In the future, the EEM will be tightly integrated with the Enhanced Object Tracking feature, extending the range of monitoring and recovery capabilities.

To shorten the impact of planned downtime, Cisco IOS Software has been enhanced to more quickly perform reloads and upgrades. With the Warm Upgrade feature, the new Cisco IOS Software image is preloaded on the router while it is still providing service. Existing operation is only briefly halted, and control is then transferred to the new, in-memory Cisco IOS Software version. The result is a faster software upgrade for the branch routers and a reduction in planned downtime. In case of a software failure, the Warm Reload feature quickly reinitializes the software, bypassing the load and decompression steps and minimizing interruption in service.

Stateful Network Address Translation (SNAT) is a Cisco IOS Software feature that allows two network address translators to function as a translation group. One member of the group handles traffic requiring translation of IP address information informs the backup translator of active flows as they occur. The backup translator can use information from the active translator to prepare duplicate table entries; then, if the active translator is hindered by a critical failure, the traffic can rapidly be switched to the backup. As the traffic flow continues, the same network address translations are used and the state of those translations has been previously defined. The result is a more resilient IP network with no session loss, even when dynamic NAT is being used.

Managing the Network for Maximum Connectivity

Performance Routing (PfR) is an enhanced, end-to-end routing solution in Cisco IOS Software that provides automatic outbound route optimization, load distribution, and bandwidth cost minimization for multihomed locations by selecting paths based on cost, load, and performance. While other routing mechanisms provide both load-sharing and failure mitigation, Cisco PfR is unique in that it can make routing changes based on criteria other than routing metrics, going beyond Cisco's Border Gateway Protocol (BGP) to select an exit link based on service-level agreements (SLAs) with ISPs. Cisco PfR periodically selects the optimal exit link from the available ISP connections based on performance (delay, packet loss, and reachability) and cost information, improving connectivity performance, increasing reliability, and lowering ISP link costs.

IP SLAs (IP Service Level Agreements) are a network performance measurement feature in Cisco IOS Software that provides a scalable, cost-effective solution for service-level monitoring and edge-to-edge network availability measurements. They allow administrators to understand levels for IP services and reduce the frequency of network outages. They can also perform network assessments, verify QoS, and ease the deployment of new services, as well as assist administrators with network troubleshooting. IP SLAs use unique service-level assurance metrics and methodologies to provide highly accurate measurements, including response time, one-way latency, jitter, packet loss, and Website download time. IP SLAs are frequently used to verify availability, test connectivity between network edges, and verify the availability of business applications.

With these complete capabilities, the Integrated Services Router is easier to deploy, offers more stable performance, and performs more flexibly in unanticipated circumstances.

Easing Network Configuration and Management

A recent study by the University of Michigan and Sprint showed that 59 percent of the problems causing downtime in IP networks pertain to router management issues. The Integrated Services Router helps network administrators avoid these problems by allowing them to:

- Reliably configure powerful branch network routing for simultaneous delivery of multiple services
- More quickly deploy basic and advanced services
- Manage these services using common tools and interfaces for simplicity in operations
- Increase network security while minimizing the number of separate boxes

- Use existing and future interfaces and network modules that speed data delivery and free up hardware for new applications
- Troubleshoot faster, “spare” more easily, and train staff more quickly

Designing high availability solutions for branch offices provides specific challenges to network administrators. Branch personnel are often unfamiliar with network technology, requiring devices to be managed remotely from headquarters. This includes configuring, managing, maintaining, and troubleshooting routers.

Studies have shown that the greatest cause of failure in branch networks lies in configuration management errors. This is particularly important in managing a network where administrators do not have the ability or time to touch every router. Multisite organizations need a system of capabilities that can scale to provide updates to hundreds (or thousands) of devices, roll back to an earlier configuration if a problem is found with even one of these devices, and track and log changes and manage any code problems introduced by updates.

Cisco offers a complete feature set to help administrators avoid the all-too-common mistakes that can appear in such highly networked environments. This includes a special focus on two critical areas within the branch: fault management and change management. Offering greater ease of use and complete access to system information, the Integrated Services Router makes accurate network configuration faster and more functional—a robust foundation for the branch network.

Knowing that a major cause of network downtime is human error, Cisco has introduced a configuration rollback feature that allows administrators to checkpoint a specific configuration, make changes to it, and then, if necessary, roll back to that previous point (not to the default configuration). This is an especially critical feature in the branch, where a networking specialist might otherwise have to travel out to a remote site to fix a new problem introduced by faulty programming. Config Rollback allows the network to be immediately and easily rolled back to a previous, working configuration, while the administrator continues to develop an error-free environment.

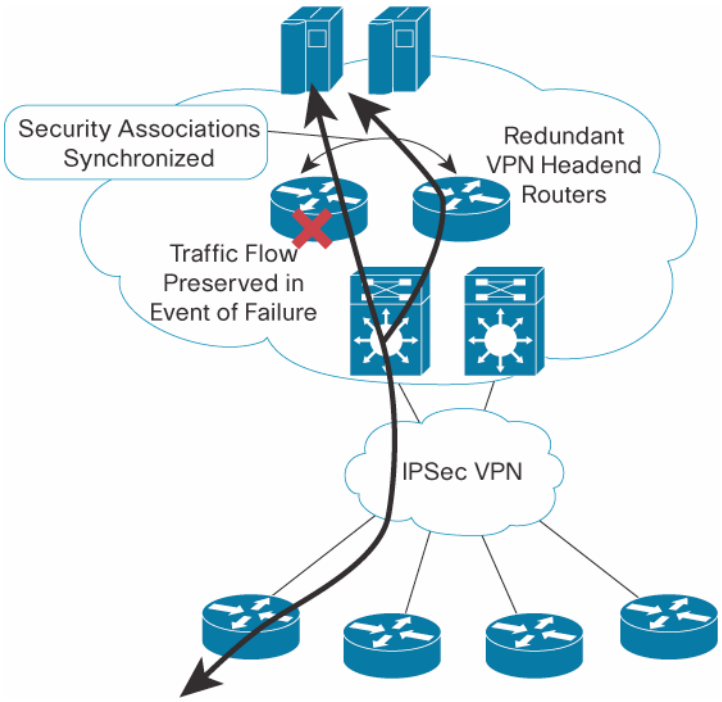
The Role-Based CLI Access security feature also allows the network administrator to define “views,” a set of operational commands and configuration functions that provide selective or partial access to the Cisco IOS executive and configuration mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible.

For those customers unfamiliar or uncomfortable with CLI, Cisco Configuration Professional (CCP) provides a free, graphical user interface (GUI) tool for configuration and monitoring of devices. With many built in wizards and troubleshooting capabilities, this device manager can help to significantly reduce configuration errors, even by relatively novice users.

Provide Secure Connectivity and Automatically Defend Against Attack

Cisco offers powerful encryption and protocols to support continuous connectivity. Cisco IOS Software and the Integrated Services Router support an accelerated IP Security (IPSec) encryption for headend, remote-access, and site-to-site VPN deployments. High availability is further enabled by stateful failover for IPSec (Figure 3). This enables the router to continue processing and forwarding IPSec packets if a planned or unplanned outage at the headend occurs. Network administrators employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This process is transparent to the user and does not require adjustment or reconfiguration of any remote peers.

Figure 3. IPSec Stateful Failover



Stateful failover for IPSec uses SSO and HSRP. The box-to-box stateful IPSec solution employs HSRP for failure detection and Cisco IOS Software high availability infrastructure services to synchronize Internet Key Exchange (IKE) and IPSec security associations between a primary and standby router. SSO allows the active and standby routers to share IKE and IPSec state information so that the standby router has enough information to become the active router at any time. In the event of a failure to the primary VPN headend router, remote VPN routers continue to forward IP packets to a consistent IP and MAC address, and the changeover of devices doing the routing is transparent to users.

Cisco IOS support for Dead Peer Detection (DPD) allows branch devices to determine loss of connectivity or failure at headend sites, and to automatically connect to a backup or disaster recovery site. DPD is the “keepalive” protocol for IKE. A periodic message option feature allows users to configure the router to query the liveliness of its IKE peer at regular intervals. The benefit of this approach is earlier detection of dead peers. In addition, keepalive packets are not sent if traffic is being received, which lowers overhead. DPD sends keepalive packets only if there is user traffic to send and no user traffic is received.

Cisco provides administrators with every feature they need to properly configure, optimize, balance, and manage their systems. The goal of Cisco’s intelligent networks is the delivery of comprehensive high availability services that are readily managed and transparent to the user.

Enabling the Self-Defending Network Against Attack

The most dramatic and often most expensive form of downtime results from a malicious attack from outside or inside the company. Branches need networks that can defend themselves against such attacks and can maintain essential services while doing so. Assaults are less likely in branches where VPNs are based on service provider MPLS networks, but many remote sites choose the less-expensive option of running their VPNs over the Internet. In these circumstances, there is a greater risk of attack, including:

- DoS attacks or oversubscription, where hackers deliberately overload connectivity pipes to bring the network router to a standstill using a “Trojan horse” command.

- Viruses, which are pieces of malicious code that attach themselves to a host file or message and are physically propagated by users sending or sharing them through e-mail or by loading disks.
- Worms, a subclass of viruses that do not need a host. They are freestanding applications that duplicate themselves and use system resources (most notoriously by tapping into Microsoft Outlook address lists) and the modem drivers to send those duplicates out.

The Integrated Services Router and the Cisco network address these points of failure with a design that defends against attack, assisted by a suite of security features to maximize high availability. Built on multisite voice and video-enabled VPN (V3PN) solutions, Cisco networks secure connectivity in geographically dispersed locations using a VPN tunnel built over a generic routing encapsulation (GRE) interface. Users can further take advantage of Dynamic Multipoint VPN (DMVPN) to enable the secure exchange of data not only between the branch and the head office, but also between branch offices without traversing the head office. This improves network performance, reducing latency and jitter while optimizing head office bandwidth utilization. Cisco network security solutions additionally provide encryption of multiservice traffic across the VPN, and help ensure interoperation with Cisco PIX® firewalls for perimeter security and an intrusion prevention system (IPS) to protect the WAN backbone from attack. Group Encrypted Transport VPN (GETVPN) provides for secure transport in a native MPLS network, maintaining QOS and other packet header information.

Several of the security services in Cisco IOS can be configured for Stateful failover, where they maintain connections through the failure and recovery process. Stateful Network Address Translation (SNAT) maintains translation tables between routers in an HSRP group for failover. Stateful IPSEC failover maintains Security Association (SA) tables between routers so that VPN tunnels stay up during the event. Finally, IOS Stateful Firewall failover eliminates the requirement for TCP connections to be reset during a failure.

Cisco delivers Cisco IOS Software tools to simplify security and availability with features such as AutoSecure, AutoQoS, EasyVPN, and the Cisco Configuration Professional (CCP). These are built on the Cisco IOS code base across all routers, unlike vendor products that require multiple operating systems for routing, security, switching, voice, and acceleration. Cisco's end-to-end solution includes market-leading firewall and IPS technologies, secure WAN and voice, endpoint security, Layer 2 security, complete intrusion and detection and prevention (IDP), forensics capabilities, flexible deployment, and far easier migrations—with no "forklifting" from version to version, but rather memory and card-level upgrades, free new feature support, and more. Powerful tools enable automatic fault management and detection of event warning signs, proactively preventing problems from developing, and raising awareness of future needs.

Integrating Cisco IOS security features directly into the router offers many benefits. First, it leverages the existing network infrastructure, enabling new security features on the router through Cisco IOS Software without deploying additional hardware. This reduces the number of devices in the network, lowering training and manageability costs for an overall lower total cost of ownership. Router network modules are also covered by existing Cisco SMARTnet® maintenance contracts to further reduce cost and ease manageability. Secondly, integrating security directly into the router protects a network's gateways, because routers are the first points of entry into the network. This allows best-of-breed security to be deployed at all potential points of entry. This allows best-of-breed security to be deployed at all entry points into the network.

Security on the router not only protects the first point of entry into the network, but also uses the intelligence of the router as a "trusted handler" of the traffic, integrating more advanced security, QoS, and routing features. This enables security features to share information and coordinate a fast, accurate response to a threat. Integrated security protects the router itself, while creating a preventive line of defense against attacks targeting the network infrastructure.

Configuring and Monitoring the Network Against Attack

The Integrated Services Router's prevention capabilities start with strong configurations using the Cisco CCP, a Web-based, easy-to-use device management tool for network and security administrators. It offers smart wizards and advanced configuration support for LAN and WAN interfaces, NAT, stateful firewall policy, intrusion prevention, VPNs, and QoS policy features. Cisco CCP also offers a one-click router lockdown and a security auditing capability to check and recommend changes to router configuration.

Cisco IOS NetFlow collects and measures data as it enters specific routers or switch interfaces. By analyzing this data, network administrators can identify causes of congestion; determine the class of service (CoS) utilization for each user and application; and identify and classify security violations and unwanted WAN traffic. NetFlow's macroanalytical and anomaly detection capabilities are used to characterize DoS attacks, worms, and viruses, alerting administrators to security violations or unwanted changes in network behavior. NetFlow allows detailed, accurate real-time traffic measurements and high-level aggregated traffic collection.

Network-Based Application Recognition (NBAR) provides additional device-level security and performance via an intelligent network classification engine that recognizes Web-based applications and peer-to-peer client/server applications which dynamically assign TCP or User Datagram Protocol (UDP) port numbers. Once the application is recognized, the network can invoke specific services for that particular application. NBAR also works with QoS features to help ensure that network bandwidth is being used most effectively. This includes the ability to help ensure sufficient bandwidth to critical applications, limit bandwidth to other applications, drop selective packets to avoid congestion, and mark packets appropriately.

Cisco IOS Software authentication, authorization, and accounting (AAA) network security services allow the primary framework to set up access control on a router or access server. AAA is an architectural framework and modular means of configuring three independent, but closely related, security functions in a consistent manner. It is flexible, scalable, and supports multiple authentication methods.

Dealing with a Network Attack

Once an attack has been launched, Cisco IOS Control Plane Policing provides significant protection against DoS attacks aimed at the network infrastructure by monitoring packets destined for the control planes of routers and switches. Administrators can identify, mark, and prioritize control plane traffic to help block unauthorized "junk" packets. Control Plane Policing increases infrastructure reliability, security, and availability, and it can defend against worms and other fast-replicating applications that may overload a route processor.

The Cisco Intrusion Prevention System (IPS) provides the ability to inspect all traffic traversing router interfaces, to identify unauthorized or malicious activity like hacker attacks, worms, or DoS attacks, and to terminate illegitimate traffic to suppress or contain threats. IP-SLAs, as part of the network configuration capabilities, play a role in attack situations by collecting signatures of attackers.

Cisco is the only networking leader that is a member of the Forum of Incident Response and Security Teams (FIRST), an international confederation of computer incident response teams that cooperatively resolve computer security incidents and promote incident prevention programs. Cisco is also the only networking company that follows the full disclosure policies recommended by the U.S. Cybersecurity Council, posting detailed information for the public about the company's security practices.

Ensuring Continuous VoIP Services

As companies continue to move to VoIP systems for telephony and video, high availability capabilities are becoming an especially important part of network administrators' strategies. Such high-bandwidth applications can become vulnerable in a network that is not fully equipped to handle the demands of today's communications technologies. Potential issues in voice deployments in the branch can include:

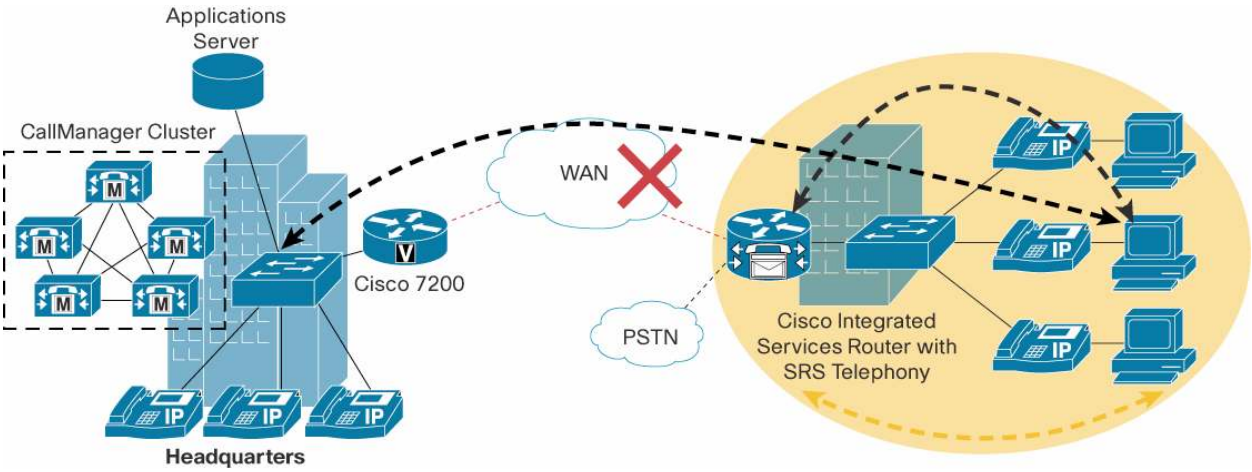
- Failure of any sort of link to the PSTN
- Failure of the WAN link, especially as it may be sharing PBX info
- Failure of the Ethernet connection from an IP phone to the switch, or from the router to the telephone

The only network vendor currently in the market providing a full IP telephony/video solution, Cisco offers Dynamic Multipoint V3PN solutions designed in the router to deliver toll-quality voice and video. The Cisco Integrated Services Router addresses possible points of failure by providing a powerfully protected link over which data, voice, and video are maximized via QoS policies for latency-sensitive traffic. Based on these technologies, network administrators are able to manage multisite environments with wire-speed encryption, bandwidth conservation, and comprehensive LAN and WAN security.

Managing Unexpected Outages in Voice Networks

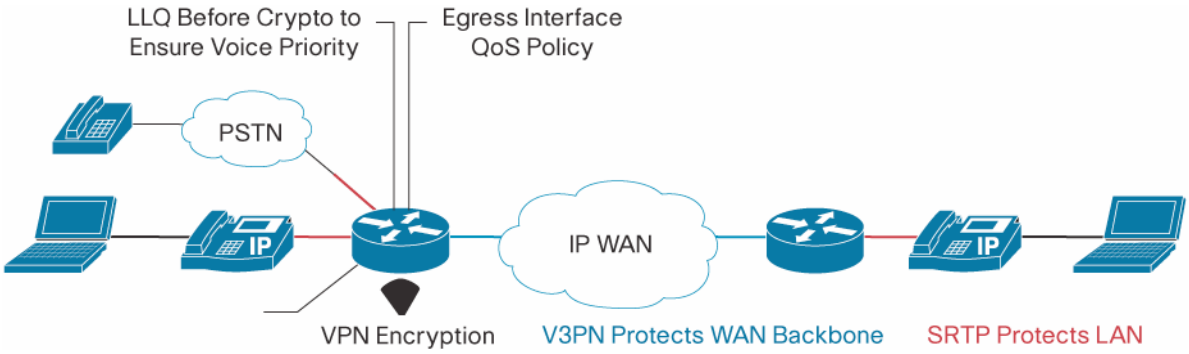
As well as providing a protective foundation for wide-bandwidth communications, Cisco offers Survivable Remote Site Telephony (SRST) features for remote offices, providing additional telephony-specific resiliency. An industry-first capability embedded in Cisco IOS Software on the Integrated Services Router, SRST (Figure 4) provides call-processing redundancy for centralized Cisco CallManager deployments, using the existing network infrastructure at the remote office. If the WAN link to the remote office fails and the connection to the CallManager is lost, branch phones are redirected to the local PSTN routes. Once the disrupted WAN link is restored, the phones automatically re-register with the original Cisco CallManager.

Figure 4. SRST—Voice Redundancy in the Event of WAN Failure



To protect callers on the LAN and help ensure messaging security, the Integrated Services Router also supports the 128-bit Advanced Encryption Standard (AES) media encryption, implemented via Secure Real-Time Protocol (SRTP), a standards-based extension to the protocol for voice in IP telephony environments (Figure 5). An X.509 Version 3 digital certificate, which embeds the encryption key in the phone itself to automate call encryption, is also supported, as well as third-party certificate authorities. Encryption and secure key exchange enable the software images in the IP phones to be signed and verified using the Message Digest 5 (MD5) Secure Hashing Algorithm (SHA), certifying the legitimacy of the image. When in secure mode, the signaling used in the IP telephony system can be encrypted through the use of Transport Layer Security (TLS) or Secure Sockets Layer (SSL) Version 3.0, preventing man-in-the-middle attacks from compromising system integrity.

Figure 5. Secure, Toll Quality IP Telephony with SRTP



Optimizing QoS

Low-latency queuing (LLQ) supports prioritizing multiservice encrypted voice and video traffic traversing the VPN. QoS features, such as “traffic shaping” to ensure quality on asymmetric link speeds, and “link fragmentation and interleaving” to control jitter in the presence of large packet transmissions, are critical to ensuring voice and video quality.

LLQ also gives delay-sensitive data, such as voice, preferential treatment over other traffic. Egress Interface Queue Management enables better administration of data to prevent network congestion.

Accelerated IPSec encryption is especially critical for voice and video traffic in its support for VPN deployments. Stateful failover for IPSec enables a router to continue processing and forwarding IPSec packets after a planned or unplanned outage occurs, helping to maintain high sound and visual quality.

The Cisco V3PN solution also provides comprehensive resiliency, addressing both VPN network transport and the IP telephony network. The full Layer 3 routing and stateful VPN failover capabilities of Cisco VPN routers provide network resiliency beyond the VPN device all the way to the network host, eliminating network black holes.

Comprehensive Support and Professional Services

Cisco backs these high availability technologies with award-winning design, support, and laboratory functions to help ensure that branch customers are receiving the best possible solutions for their sites. With more than 630 depots, 10,000 field engineers, and 2900 certified channel partners working in 120 countries, Cisco offers a comprehensive technical support program to assist branch offices 24x7x365 with their networking needs.

A recent study of 2310 enterprises and 1825 small to midsize businesses revealed that current customers believe Cisco provides world-class service and support, the most knowledgeable technicians, and the best consulting. Cisco is the only IT company to offer an end-to-end networking architecture that truly integrates voice, data, and video. As a result, Cisco was selected as the networking leader that best understands industry and individual business needs.

Cisco Technical Support Services are the gateway to the Cisco Technical Assistance Center (TAC), providing 24-hour troubleshooting and technical support services for Cisco customers globally, both online and over the phone. This organization enhances administrator productivity and self-sufficiency by providing access to Cisco technical engineering staff and comprehensive documentation, tools, and labs. For example, the Cisco Software Advisor is a valuable online tool designed to help network administrators find the software that provides the features they need and is compatible with their installed hardware; as well as allowing them to compare features in different software releases or research a software release.

> "By converging applications into a single system engineered for speed and security, Cisco Integrated Services Routers enable us to easily deploy voice, data, and security services to travel centers anywhere around the country. That's the level of capability and flexibility we need to provide the very best service to our travel center patrons, professional drivers, and employees."
>
> **—Jon Duren, Chief Technology Officer, Idle Aire**

Cisco's focus on advanced technology solutions has led to the creation of Cisco Advanced Services, which have been developed from technology best practices that focus on helping administrators plan, design, implement, operate, and optimize technology investments with the help of Cisco's extensive engineering expertise. This helps to build a knowledge-transfer management process shared with customers and partners.

Cisco's Advisory Services deliver business transformation consultating services, helping companies implement Internet business solutions. These engagements are focused to extend Cisco's own best practices, methodologies, and architectures for aligning IT to business processes. Cisco's transformation consultants deliver complex solutions, allowing enterprises, agencies, and service providers to use the Internet to their competitive advantage.

Finally, Cisco's Customer Proof of Concept (CPOC) Labs are large-scale labs where network administrators can stage and validate customized network solutions prior to implementation through hands-on testing utilizing Cisco's deployment expertise.

Conclusion: Cisco's End-to-End Approach Improves Availability

Cisco leads the industry with complete dedication to high availability networking across the branch network. Throughout its 20-year history, Cisco has consistently developed new technologies and protocols in network accessibility. No other vendor today can approach Cisco's list of achievements in the field of high availability, and these accomplishments extend to the new Integrated Services Router.

In this paper, we have shown that Cisco offers a truly formidable suite of capabilities for maintaining high availability in the branch. Designed from the ground up for always-accessible networking, Cisco's end-to-end perspective provides IT organizations with a more easily deployed, maintainable, self-defending network architecture. The Integrated Services Router further strengthens this approach by providing simultaneous use of more interfaces and features while increasing performance of multiple, concurrent security, management, and integration services.

With the Integrated Services Router, Cisco offers a comprehensive, future-proofed solution for high availability in the branch that minimizes network outages and ensures nonstop access to the most business-critical applications. Cisco's focus on integrating new infrastructure services with performance enables companies to create networks that are more intelligent, resilient, and reliable.

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.

Printed in USA C11-604722-00 05/10