Benefits of Deploying Unified Communications on a Cisco Integrated Network

Overview

The mass migration to IP telephony has delivered an initial wave of value to companies large and small. By consolidating voice, video, and data networks onto a single IP network, organizations have reduced the cost of communications, taken advantage of underused network capacity, and laid a foundation for unified communications.

Deploying unified communications across the business also delivers a second wave of value through enhanced communications and collaboration. These capabilities are helping organizations shorten decision cycles, accelerate business, and boost productivity by speeding secure access to information and by making it possible for everyone to collaborate everywhere. Unified communications also provides a communications system that can change and grow at a moment's notice.

More than 70 percent of Fortune 500 companies now use Cisco® Unified Communications to build competitive advantage. In fact, many of Cisco's more than 50,000 unified communications customers are now enjoying a third wave of value created by embedding unified communications capabilities into business processes in order to streamline those processes and, in some cases, to change the way they do business.

Organizations will find that all these benefits can be fully realized only when Cisco Unified Communications is deployed on a Cisco Integrated Network. When unified communications are part of a comprehensive system that includes an integrated end-to-end infrastructure, organizations can successfully deliver a consistent set of unified communications services, not just to campus headquarters but to every place in the network.

The Unified Workspace

Unifying IP Communications and Collaboration Applications

Cisco Unified Communications creates a unified workspace by integrating IP communications and collaboration products and applications into a single, unified system. Without unified communications, disparate voice, video, data, and mobility applications cannot live up to their potential and are far less effective than they could be. The result is communications complexity, inefficiency, information overload, and misdirected communications. All of these challenges delay decisions, slow down processes, and reduce productivity across the enterprise.

Cisco Unified Communications helps companies contend with communications complexity. It also addresses the growing needs of increasingly mobile workers who now conduct business from their desks and in conference rooms, airports, warehouses, and vehicles. Cisco Unified Communications clears communications roadblocks by:

- Unifying voice, video, data, and mobility applications on both fixed and mobile networks: With rich call control, unified messaging, and unified client software, workers can take their workspace (and all its advanced capabilities) with them wherever they go.

- Enabling more effective communications: With presence and instant messaging, people can check the availability of colleagues, know how and where co-workers wish to be reached, and click-to-communicate in real time.
- Delivering media-rich collaboration: When voice, video, and web conferencing solutions use the power of the integrated network, people can collaborate instantly. They can also easily escalate sessions by adding video to an audio conversation or by adding web conferencing or whiteboarding to an existing audio or video conversation.
- Enabling the creation of business applications: With Cisco service creation platforms, customers and partners can develop innovative rich-media and web applications, making it possible to embed unified communications capabilities into existing business process systems.

The Power of an Integrated Network

An End-to-End System

Cisco provides an end-to-end unified communications system that uses the pervasive reach of an integrated network to enable the unified workspace. The secure network foundation includes industry-leading routers and switches that exhibit three types of intelligence:

- Device-aware: Because Cisco integrates intelligence throughout the network — even in the endpoints — a Cisco Integrated Network "knows" which device is being used, where it is being used, and what unified communications applications it is allowed to use.
- Application-aware: A Cisco Integrated Network actively participates with applications, automatically providing the appropriate rights, priorities, and organizational policies of each application.
- Network-aware: Cisco Unified Communications applications seek out the network services they require to help ensure that applications receive the appropriate quality of service (QoS).

When the network and applications interact this way, IT administrators and end users enjoy many benefits. Because the technologies are not bolted together, administrators can use capabilities across platforms, providing the flexibility to quickly and cost-efficiently deploy, operate, and consolidate new communication services. You can add features such as video or wireless voice through software upgrades and incremental hardware that builds upon existing network infrastructure. As a result, you have access to new business applications sooner, increasing their productivity and improving business processes.

Lower Total Cost of Ownership

In addition to these advanced capabilities, by implementing a Cisco Integrated Network (versus a network built with systems from multiple vendors) your organization can also enjoy a lower total cost of ownership (TCO):

- The networking costs per employee are, on average, almost 50 percent lower: According to a report by IDC (Operational Excellence in Networking: Industry Leaders Point the Way, IDC, April 2007), companies that consolidate router, switch, security, wireless, and voice vendors have, on average, a 45.6-percent lower cost per employee than those with six or more vendors.

- Each endpoint has a lower cost of ownership: According to a customer study conducted by Sage Research (Unified Communication Application: Uses and Benefits, Sage Research, 2006; http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns165/net_implementation_white_paper0900aecd8040970b.pdf), organizations that use a single, primary network vendor have on average a 26-percent lower cost of ownership per endpoint than those that use multiple vendors.

- The overall network cost of ownership is substantially lower: Sage Research also found that organizations that use a single vendor for IP telephony have a 43-percent lower network cost of ownership than those that use multiple vendors. These savings are derived from all areas, including network deployment and maintenance, network performance improvements, and benefits for both IT and end users.

Cisco offers validated designs and industry best practices that are required in order for the network to deliver these benefits in deployment, operational manageability, and consolidation. These recommendations are based on the type of business site or its place in the enterprise network.

Recommendations for a Head Office or Campus

Typically, the primary users of business-critical and rich-media applications are the employees in the campus or head office. The campus infrastructure is built around a high-speed LAN switching network. A Cisco Integrated Network delivers the following unified communications benefits in the campus environment.

Faster, More Cost-Effective Deployments

In large companies, approximately 25 percent of personnel move each year. The Yankee Group estimates that it costs companies up to US$150 per move, add, or change. You can significantly minimize this enormous expense with Cisco Unified Communications products and Cisco Catalyst® switching solutions in a Cisco Integrated Network:
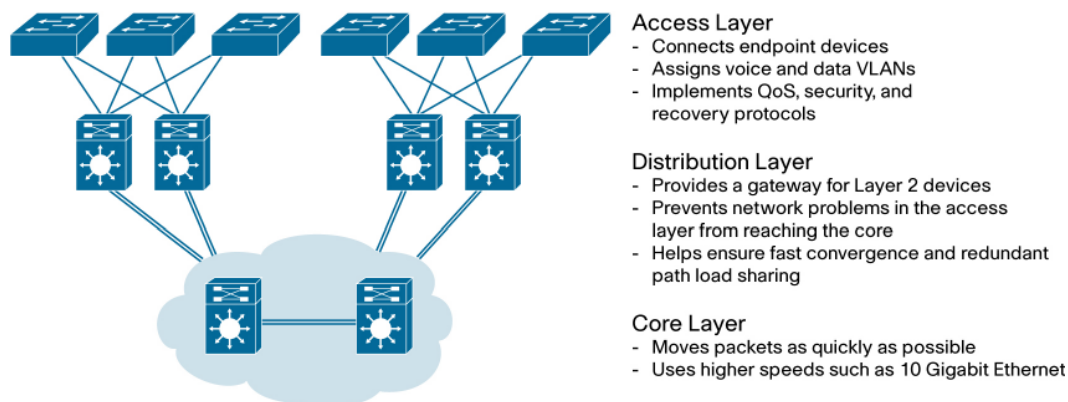
- When a Cisco Unified IP Phone is plugged into a wall jack, the Cisco Catalyst switch automatically detects the phone and extracts the device information through either Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED) or Cisco Discovery Protocol exchange.

- Then, using the Cisco Embedded Event Manager (EEM) feature in the Cisco Catalyst switch, you can automatically configure the switchport for voice. Cisco EEM is a powerful and flexible automation technology. It reduces deployment costs by allowing administrators to set policies that control the actions that a switch should dynamically take when specific events occur.

- For administrators who use Cisco Network Assistant, Cisco offers an alternate method for configuring switches for voice. When a Cisco Unified IP Phone is plugged in, the Smartports Advisor feature on the Cisco Catalyst switch can automatically send a dialogue box prompt to the Cisco Network Assistant management interface. The administrator can then apply the appropriate Smartports Advisor voice macros to that switchport for easy configuration.

- If you need to move to a new location, you simply unplug your phone and plug it into the wall jacks in your new office. Removing the voice configuration on the previous switchport helps to strengthen security. You can remove the configuration dynamically when the phone is unplugged.

Other vendors that partner with infrastructure vendors or offer only voice components lack this type of integration. As a result, each time an IP phone is moved or added to the network, IT personnel must manually reconfigure the switchports, significantly increasing administrative and support costs, especially in large enterprises with tens of thousands of IP phones.

Nonstop Communications over the LAN

IP-based voice networks must deliver the same continuously available service that was provided with traditional time-division multiplexing (TDM) voice networks. High availability starts with a hierarchical network design (Figure 1) that allows for separation of core, distribution, and access layers as well as the fault domains within these layers.

Figure 1. Recommended Network Topology for Highly Available Campus Network

Access Layer
- Connects endpoint devices
- Assigns voice and data VLANs
- Implements QoS, security, and recovery protocols

Distribution Layer
- Provides a gateway for Layer 2 devices
- Prevents network problems in the access layer from reaching the core
- Helps ensure fast convergence and redundant path load sharing

Core Layer
- Moves packets as quickly as possible
- Uses higher speeds such as 10 Gigabit Ethernet

Cisco recommends the following guidelines for building access, distribution, and core layers in the campus.

- Maintain triangle topologies for Layer 3 routing peers, especially between the core and distribution switches: This topology helps ensure that a switch can take two equal paths to get to a destination. These two paths will simultaneously reside in the routing table. If a link failure occurs, the traffic will flow on the other path without requiring a route recalculation.

- Summarize routes from the distribution to the core: This process prevents the core switches from having to respond to routing advertisements coming from the access and distribution layers.

- Deploy switches with high-availability innovations: Cisco Catalyst 6500, Catalyst 4500, and Catalyst 3750-E switches lead the industry in meeting uptime requirements with advanced technology that contains, detects, and resolves faults faster with minimal effect on voice traffic. Features such as Stateful Switchover (SSO) preserve critical state information across dual supervisor engines to help ensure that unified communications traffic is continually switched if a primary supervisor engine fails. Cisco IOS® Software Modularity allows you to upgrade single software modules without having to take the switch out of service, thereby increasing up-time even for planned upgrades. This feature localizes the effect of software process faults with a protected memory architecture. Even if a software process failure occurs, voice and video traffic can continue.

For more best practices for designing a multilayer network, refer to the Campus Network for High-Availability Design Guide at:
http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html.

Quality of Service

Unified communications requires new IP endpoints that deliver rich media to campus constituents. To ensure QoS, all forms of traffic — voice, video, and data — are assigned the appropriate class of service (CoS). CoS and Priority Queuing are controlled by Cisco Catalyst switches.

- Maintaining voice quality through the switch: The CoS value for unified communications voice traffic is controlled by the Cisco Catalyst switch. The switch indicates to the Cisco Unified IP Phone which voice VLAN ID it should use and then automatically applies the appropriate CoS value. The switch can also indicate CoS for traffic coming from devices attached to the phone using the Extended Trust feature. A CoS value of 5 indicates high priority and is usually reserved for voice. Call signaling is given a value of 3, and best-effort traffic is given a value of 0. So even if a rogue PC tries to raise its CoS value to 5, the Cisco Unified IP Phone resets the CoS value on the incoming packets of that PC to the CoS value indicated by the switch.

- Monitoring traffic to ensure QoS: Voice traffic is typically assigned the highest-priority queue. You can set an EEM script on a Cisco Catalyst 6500 Switch to detect excessive packet drops and automatically alert the network administrator. Additional voice traffic monitoring and troubleshooting capabilities are provided through the network analysis module (NAM), a data, voice, and video traffic-analysis blade. For example, if dial tone or call setup latency exceeds specified thresholds, the NAM detects these anomalies, analyzes Cisco Unified Communications Manager response times, and then sends an alert to a network operator. For H.323, Media Gateway Control Protocol (MGCP), Skinny Client Control Protocol (SCCP), and Session Initiation Protocol (SIP) traffic, the NAM monitors active calls between caller and callee pairs and identifies call quality degradation by reporting packet loss and jitter statistics. The NAM also performs Differentiated Services (DiffServ) QoS monitoring and provides traffic usage information for each DiffServ code point, helping validate QoS planning assumptions and detect unauthorized or incorrectly marked traffic that could adversely affect voice QoS.

Operational Manageability

Most networking surveys show that operational costs far outweigh the initial purchase cost of the equipment. Cisco is constantly improving the ways to deploy and manage unified communications on an end-to-end Cisco infrastructure. The following technologies help our customers optimize and efficiently operate this integrated network:

- Smartports macros: Based on Cisco best practices, Smartports macros can be applied to any Cisco Catalyst switch to make port configuration much simpler and more accurate. With a standard or customized Cisco Smartports macro, an administrator no longer has to log into each switchport and configure all the parameters for voice VLANs, port security, Dynamic Host Configuration Protocol (DHCP) snooping, and Spanning Tree PortFast. Instead, the administrator automatically uploads the Smartports macros, which include all the proper settings. Cisco Smartports macros do not function in third-party or multivendor network environments. As you might imagine, the loss of this powerful cost-and-time-saving tool really accumulates when it comes to the moves, adds, and changes that generate significant costs each year. Cisco Smartports make these configuration changes as easy as possible, providing a greater return on investment.

- AutoQoS macros: Cisco developed AutoQoS macros in response to customer demand for a faster way to deploy QoS configurations, which are traditionally deployed manually on

hundreds or thousands of switch and router ports. This powerful feature of Cisco IOS Software automatically handles a range of tasks, including classifying applications, generating policies, configuring QoS, monitoring and reporting to test QoS effectiveness, and enforcing service-level consistency. After Cisco AutoQoS evaluates a network environment and determines policy, it configures the port on an access switch to prioritize voice traffic — with only one command. And it still offers the flexibility to adjust and tailor QoS settings to customer-specific requirements. It also automatically monitors QoS settings and makes this information available in reports, with notification of abnormal events.

- Cisco IOS IP service-level agreements (SLAs): This tool actively monitors the health of the underlying network by generating and then analyzing traffic between multiple network locations or across multiple network paths. It uses the timestamp information to calculate performance metrics such as jitter, latency, network and server response times, packet loss, and mean-opinion-score (MOS) voice-quality scores. Administrators can schedule a Cisco IOS IP SLAs operation at any point in time or continuously over any time interval. Cisco IOS IP SLAs is configured to monitor per-class traffic over the same link by setting the DiffServ code point (DSCP) bits. Administrators can specify measurement characteristics including packet size, packet spacing, protocol type, DSCP marking, and other parameters. They can use measurement statistics provided by Cisco IOS IP SLAs operations for troubleshooting, problem analysis, and designing network topologies (Figure 2).

- Cisco IOS IP SLAs Responder: This component is embedded in the destination Cisco routing device. It processes measurement statistics and sends detailed timestamp information about the processing delay of the destination router back to the source Cisco router. Cisco recommends that round-trip delay be less than 150 ms and jitter be less than 30 ms for successful transmission of voice traffic. Unidirection measurements are also possible.

Figure 2.   How It Works — Cisco IOS IP SLAs Operations
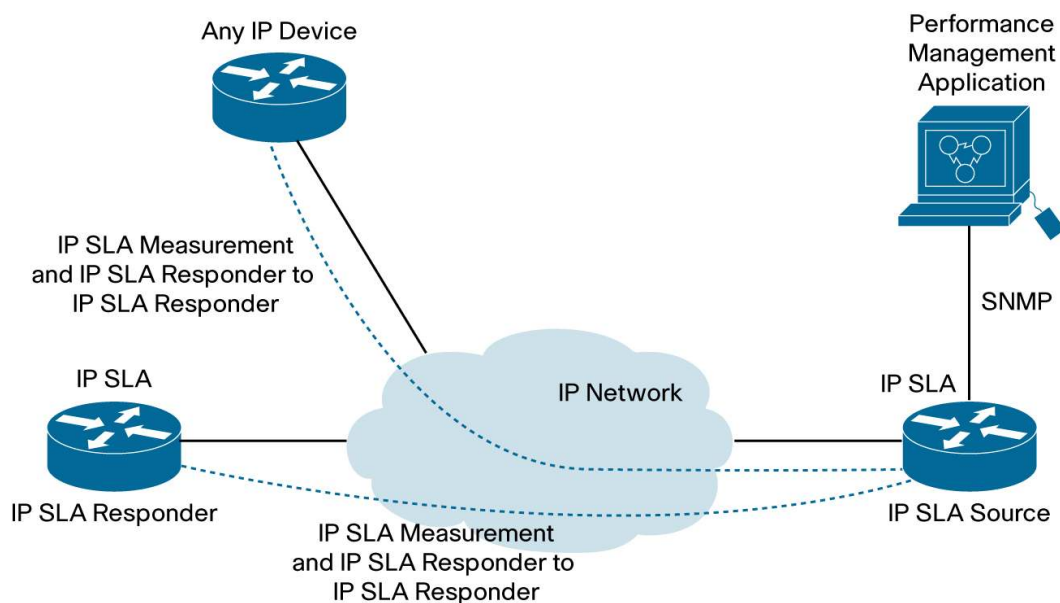
Secure Communications

The increasing number of applications and devices available on the network introduces many new points of vulnerability. As a result, you can no longer deploy security as a mix of "point-product" solutions. Instead, network security must be pervasive, securing everything from endpoints such as IP phones and PCs to the software and devices in the network infrastructure itself. Unlike some vendors, which focus only on securing the voice components or the infrastructure itself, Cisco takes a systems-level approach that integrates security throughout the network. This integration includes features and capabilities in the transport network, the endpoints, the call-processing infrastructure, and the applications.

When you deploy Cisco Unified Communications applications on a Cisco Integrated Network, you do not have to implement separate security devices. Cisco integrates critical security components deep into the network. Cisco is the only vendor that provides this in-depth security control, delivering the following security components:

- Secure connectivity: Cisco offers many options that help ensure secure communications. For example, VLAN segmentation keeps voice traffic on separate virtual network segments. Voice and Video Enabled VPN (V3PN) provides secure remote connectivity. WLANs are protected through Wi-Fi Protected Access (WPA) and WPA2. Call management and endpoints offer strong voice media encryption using the Secure Real-Time Transport Protocol (SRTP), and Transport Layer Security (TLS) provides protection for signaling traffic. At the application layer, Cisco uses HTTPS to permit protected remote management of IP communications applications. And the Cisco Unity® system is the first voice messaging system to offer encrypted messaging.

- Trust and identity: To contextually identify users and establish trust, many standards-based authentication mechanisms must work together. Cisco offers support for traditional authentication, authorization, and accounting (AAA) services in the infrastructure, as well as more advanced capabilities elsewhere with such tools as Extensible Authentication Protocol (EAP) and digital certificates. Wireless LANs (WLANs) can allow IP phones to transparently connect on ports where user authentication with 802.1x is mandated. By deploying Cisco Network Admission Control (NAC) framework, customers can restrict non-security-compliant wired and wireless endpoints that may be vulnerable or infected with worms, viruses, or spyware. All these threats are stopped before they can enter the network and potentially disrupt voice services.

- Threat defense: Cisco uses many techniques to provide protection against aggressive threats. Integrated and standalone firewalls and intrusion detection systems protect the infrastructure, the voice VLANs, and WLANs. A hardened OS and integrated host intrusion prevention solution called Cisco Security Agent protects the call-processing components. To protect endpoints against common Layer 2 exploits such as man-in-the-middle attacks, Cisco employs advanced dynamic Address Resolution Protocol (ARP) inspection protection and other tools on its LAN switches and unified IP phones. In addition, the Cisco Unified Communications applications themselves offer security features. For example, Cisco Unified Communications Manager can support multiple levels of administration access and advanced protection against toll fraud. Finally, the Cisco Integrated Network infrastructure is designed to withstand denial-of-service (DoS) attacks so that data and voice traffic continues to be forwarded even when DoS attacks occur. Cisco Catalyst 6500 and Catalyst 4500 switches provide such protection through CPU rate limiters as well as control plane policing (CoPP), which is embedded in the hardware.

Scalable Wireless Services

Businesses today use wireless networking to give employees access to the business applications and communication tools they need even when they are on the move. By adding voice-over-IP (VoIP) capability to wireless networks, organizations can improve collaboration and responsiveness while realizing cost savings. The combination of Cisco Unified Communications and the Cisco Unified Wireless Network lets organizations provide IP communications for mobile workers while minimizing TCO.

Cisco integrates important technologies into its switching, routing, and wireless offerings to provide optimal support for wireless voice, simplified wireless voice deployment and management, wireless voice call roaming, diverse wireless voice client support, and high-quality wireless voice communications. These technologies include:

- Simplified wireless voice deployment and management: Cisco integrates wireless controller functions into its switches and routers so network managers can scale and manage wireless networks as easily as they scale and manage traditional wired networks. For example, the Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM) supports zero-touch deployments that require no preconfiguration of access points. It also supports QoS policies, mobility groups, and back-end services, as well as other important tools such as template-based configuration management, which allows quick application of systemwide wireless security configurations.

  When deployed with the Cisco Wireless Control System (WCS), the Cisco Catalyst 6500 WiSM supports enhanced monitoring and troubleshooting features such as intuitive heat-map displays, alarm filtering, event correlation, and granular reporting tools. This Cisco Catalyst module also supports the simultaneous tracking of 10,000+ wireless client devices from directly within the WLAN infrastructure when deployed with the Cisco Wireless Location Appliance.

  The Cisco Catalyst 6500 WiSM facilitates maximum access point coverage — 300 lightweight access points per module and clustering of up to 3600 lightweight access points per roaming domain. For remote-site deployments, Cisco also offers the Cisco Catalyst 3750G-24WS Switch, which can manage up to 50 lightweight access points and the Cisco Wireless LAN Controller Module (WLCM) for Cisco integrated services routers, which can manage up to six lightweight access points. Standalone WLAN controllers such as the Cisco 4400 and 2100 Series Wireless LAN Controllers are also available.

- Wireless voice call roaming: Efficient roaming is critical for voice applications, which are unforgiving of any delays in authentication. The Cisco Catalyst 6500 WiSM, the Cisco Catalyst 3750G-24WS, and the WLCM offer fast, secure roaming that facilitates roaming of voice clients between access points in the same subnet (Layer 2 roaming) or between subnets (Layer 3 roaming) without disruption to voice calls.

- Integration with diverse wireless clients: A growing number of client devices support 802.11 wireless voice communications today, including dual-mode cell phones, personal digital assistants (PDAs), laptop softphones, and Wi-Fi handsets such as the Cisco Unified Wireless IP Phone 7920. Cisco Compatible Extensions, a licensing program for wireless clients, facilitates secure interoperation of these devices with the Cisco Unified Wireless Network. It also helps enable interoperability of client-side features such as power-save mode, QoS, and assisted roaming. Wireless clients that support Cisco Compatible Extensions undergo extensive testing at an independent third-party test lab to help ensure

support for innovative Cisco features, as well as interoperability with the Cisco WLAN infrastructure.

High-quality video over wireless: High-speed wireless access points that support the 802.11n standard can deliver 248 Mbps of data. This level represents a significant increase over the 54 Mbps delivered by 802.11g devices, and optimizes the delivery of voice and video. These new access points have higher power requirements, and Cisco Catalyst switches offer 20 watts of enhanced Power over Ethernet (PoE) per port to support 802.11n access points without requiring additional wiring or power outlets. In addition, Cisco wireless access points, client devices, and Cisco Compatible Extensions devices include support for Wi-Fi Multimedia (WMM.) WMM is a component of the IEEE 802.11e WLAN standard that supports priority tagging and queuing to ensure integrated handling of voice communications. Through the use of Layer 2 admission control, QoS can be maintained under heavy user loads to meet demanding wireless networking needs.

Video as a Simple Addition

When Cisco Unified Communications is deployed on a Cisco Integrated Network, adding video to the network is as easy as adding any other application because the applications and the infrastructure are part of an intelligent system. This intelligence extends out to all types of devices (for example, laptops, PDAs, mobile phones, or remote PCs). If a device is video-enabled, the required settings are generated automatically and the appropriate switches are instructed to provide the proper VLAN and QoS to allow the video stream. Without intelligence distributed throughout the network, video cannot be integrated as easily, proper settings require more manual effort, and manageability is compromised.

With an integrated network, organizations can:

- Enable video endpoints: You can introduce traditional video conferencing equipment based on the H.323 video conferencing onto the converged network, and you can enable these systems to automatically register to Cisco Unified Communications Manager. Thereafter you can easily control them with Cisco Unified Communications Manager.
- Optimize video delivery: IP Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to multiple recipients. This technology is ideal for video applications where the same large set of data or video must be transmitted efficiently to multiple clients.
- Dramatically simplify video conferencing management: Call detail records (CDRs) are also integrated into and managed by Cisco Unified Communications Manager. IT managers no longer must download CDRs from two separate systems. Instead, all phone and video records are located in one place.

Energy Savings

Cisco Unified Communications on a Cisco Integrated Network can help reduce your company's carbon footprint and conserve energy with a switching infrastructure that provides additional levels of power control within each Cisco Catalyst switchport. Cisco Integrated Power Management (IPM) provides customers with significant power-consumption savings on devices (for example, IP phones, wireless access points, and IP video surveillance cameras) that use Cisco Discovery Protocol to negotiate power. Whereas the IEEE standard specifies that 802.3af power should be provisioned in large increments of wattage such as 7 or 15 watts of power to each device regardless of power need, the Cisco IPM allows administrators to provision power based on the

power the device actually needs. For example, some Class 3 devices need only 10W instead of the default 15.4W value indicated in the 802.3af standard. This power optimization, combined with the scalable power supplies offered on modular Cisco Catalyst switches, helps customers:

- Maximize PoE port density
- Minimize the number of switches required
- Expand savings through decreased use of electricity, backup UPS, and battery power systems

Voice and Data Teams Share a Common View of the Network

In most enterprises, separate teams manage the voice system and the data infrastructure, reflecting the traditional separation of the voice and data networks. But with unified communications, problems can span both realms, so it is essential that both teams can communicate specific details about problems with one another. Cisco Unified Operations Manager provides a consolidated view of the entire Cisco Unified Communications infrastructure and presents the current operational status of each element. Cisco Unified Operations Manager can:

- Query Cisco Catalyst switches to ascertain the operational status of the switch as well as the system resources and different ports and interfaces
- Alert administrators in case of operational faults
- Track IP phone inventory and IP phone status changes
- Create a variety of reports that document all the moves, adds, and changes of IP phones
- Increase productivity and enable faster trouble isolation by providing contextual diagnostic tools that troubleshoot through diagnostic tests, performance, and connectivity details about different elements of the Cisco Unified Communications infrastructure

Cisco Unified Operations Manager also provides deep visibility into voice packets. This visibility is essential because malfunctions in any voice-processing components — in the LAN or WAN connections or in the infrastructure itself — can affect voice quality. When the Cisco network infrastructure and management tools detect excessive voice packet loss, jitter, or latency, they can alert network administrators and allow them to centrally troubleshoot real-time voice traffic in targeted areas without having to go on site. And because Cisco management software can provide a common view of the network for voice and data teams, these teams can communicate concerns with much greater precision and quickly identify and resolve problems. Here's how Cisco provides this rapid detection and notification of voice anomalies:

- When an administrator is alerted to a voice problem by a switch, the administrator can instruct the switch to mirror the real-time voice traffic so it can be analyzed.
- The Encapsulated Remote Switched Port Analyzer (ERSPAN) on the Cisco Catalyst 6500 Switch mirrors the traffic across the campus and across Layer 3 boundaries to a central site, where it can be analyzed.
- The NAM analyzes the traffic, eliminating the need for the administrator to go on site with a portable troubleshooting tool to solve the problem.

Recommendations for a Branch Office

The Cisco Integrated Network delivers a powerful unified communications experience for campus workers. And now, thanks to the innovative Cisco system approach, companies can consistently and reliably extend this experience to branch-office locations. Branch-office workers are very

---

sensitive to application performance and availability, so the network needs powerful WAN optimization tools and built-in redundancy in case the main connection to the campus is disconnected.

Providing Optimum Voice Quality Across the WAN

According to The Nemertes Research Group, Inc., 90 percent of employees now work in branch offices, and the number of branch offices is growing at the rate of 10 percent a year. As the number of branch offices increases and the new unified communications services at these remote locations continue to evolve, the requirements for the WAN infrastructure are changing.

The Cisco system approach helps ensure optimum voice quality across the WAN in several ways:

- Network-aware Call Admission Control (CAC): Cisco integrated services routers not only support standards-based QoS, they also exchange information with Cisco Unified Communications Manager to enable network-aware CAC with QoS. CAC allows the network to accept or reject a call based on bandwidth and policy considerations. A primary enabler to this solution is the Cisco IOS Software feature called Cisco RSVP Agent. It facilitates dynamic adjustment to changes in the network, supports complex network topologies, and helps enable unified data, voice, and video network designs.

- Resource Reservation Protocol (RSVP): This IETF standards-based signaling protocol secures and reserves bandwidth across the WAN for calls accepted by Cisco RSVP Agent (Figure 3). The resulting user experience is characterized by superior QoS and reliability for calls amid meshed and multitiered networks. Cisco RSVP Agent is supported on the Cisco 2800 and Cisco 3800 Series Integrated Services Routers.

- Low Latency Queuing (LLQ) on the WAN interfaces: This technology gives voice traffic a higher priority over other forms of traffic on the link.

- Traffic shaping: Traffic shaping prevents WAN traffic from reaching the line rate in case of speed mismatches with the central hub. It is also used to stay within the committed information rate delivered by the service provider.

- Link fragmentation and interleaving (LFI): This technology is very helpful when WAN links are less than 768 kbps. LFI takes large packets destined for the WAN and cuts them into manageable pieces for transmission. It allows voice packets to be interleaved within these pieces and transmitted across the WAN. Without LFI, voice packets would have to wait until the entire large packet was transmitted across the WAN before they would be allowed on the link. This delay, of course, could affect the quality of the voice connection.

- WAN optimization: Service modules on Cisco integrated services routers support a variety of technologies that optimize WAN transport. For example, the Cisco Wide Area Application Services (WAAS) Network Module minimizes protocol chatter as it traverses the WAN link, conserving bandwidth for business-critical applications. The Cisco Network Capacity Expansion (NCE) services module can focus on bandwidth optimization through compression, and the Performance Routing services module is a Cisco routing innovation that determines optimized routing paths for different types of applications.

Figure 3.　Cisco Integrated Services Routers and Cisco Unified Communications Manager Help Ensure Optimal Voice Quality Across the WAN
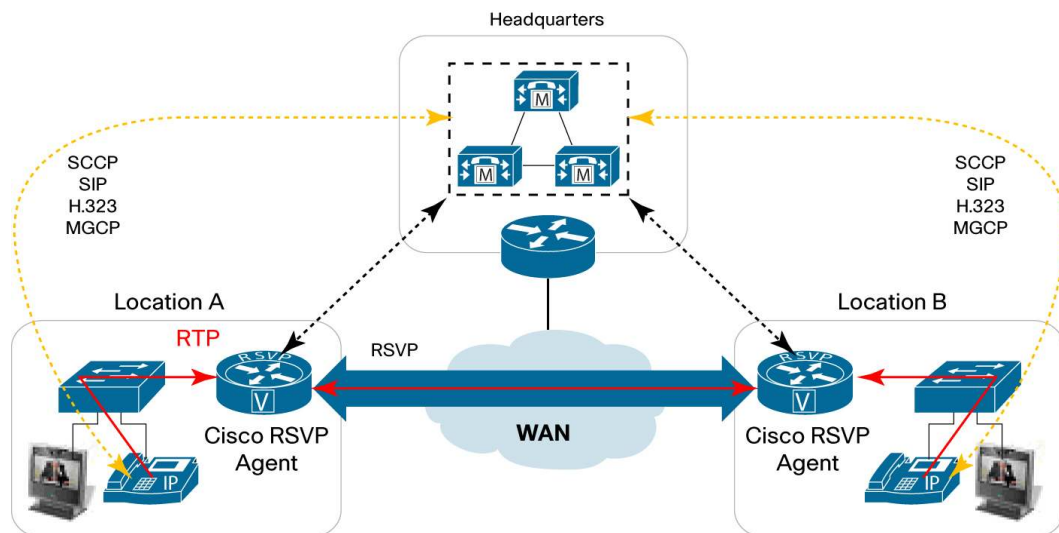
Delivering Resiliency for Intrabranch Communications

Cisco StackWise® Plus technology on the Cisco Catalyst 3750-E and Cisco EtherSwitch Service Modules, such as the 24-Port EtherSwitch Service Module for the Cisco 2600/2800/3700/3800 Series Routers, creates a unified logical switching architecture that delivers a high level of resiliency for voice-enabled wiring closets. The switching stack behaves as a single switching unit that is managed by a master switch. Any member switch can take over for the master switch if a master switch fails. Although the switchover times between the master and member switches may not be at the level of modular switching platforms with SSO, recovery has proven to be acceptable for customers whose data and voice availability requirements are less demanding.

Nonstop Communications over the WAN

Most branch offices, depending on the number of users, operate well with anything from a few Ethernet ports on a Cisco integrated services router to a full Cisco Catalyst 3750-E stackable switching system using Cisco StackWise Plus technology. If WAN resiliency is a concern, network administrators should start with two diverse WAN paths on the same router or different routers for added redundancy. In the latter configuration, features such as Hot-Standby Router Protocol (HSRP) with tracking come into play so that outgoing traffic will always go through the correct router. Performance Routing can help circumvent brownouts and optimize routes based on MOS, latency, jitter etc., because it looks at best-metric routing instead of best-path routing, increasing application resiliency.

Deploying unified communications in the branch office also requires its own redundancy solution. A Cisco Integrated Network provides this redundancy with Cisco Unified Survivable Remote Site Telephony (SRST), an industry-first resiliency capability for remote sites. This innovative capability is embedded in the Cisco IOS Software, which runs on Cisco integrated services and multiservice access routers.

In a centralized call-processing model, the Cisco Unified SRST-enabled router facilitates automatic failover. In this way, local calls and active calls from Cisco Unified IP Phones to the public switched telephone network (PSTN) are maintained even if a WAN failure occurs (Figure 4). Here's how:

- If the WAN link to a remote office fails and the connection to the Cisco Unified Communications Manager for the domain is lost, the phones in that branch office automatically redirect to the Cisco Unified SRST-enabled router.

- The Cisco Unified SRST-enabled router automatically takes over and offers a rich set of telephony functions to help ensure business continuity with minimal effect on the system.
- When the disrupted WAN link is restored, the phones automatically reregister with the original Cisco Unified Communications Manager and, again, no manual intervention is required.

And Cisco Unified SRST accomplishes this reregistration with no additional hardware components, and no manual intervention is required (Figure 4).

Figure 4. Integrated Voice Redundancy if WAN Failure Occurs

- Offers resiliency for remote IP telephony users with central Cisco Unified Communications Manager
- Minimizes business effect of WAN link failure
  - ○ Cisco router autoconfigures and provides local call processing – no manual intervention required
  - ○ Cisco Unified SRST IP phone calls remain secure
  - ○ When WAN is available, autorevert to Cisco Unified Communications Manager
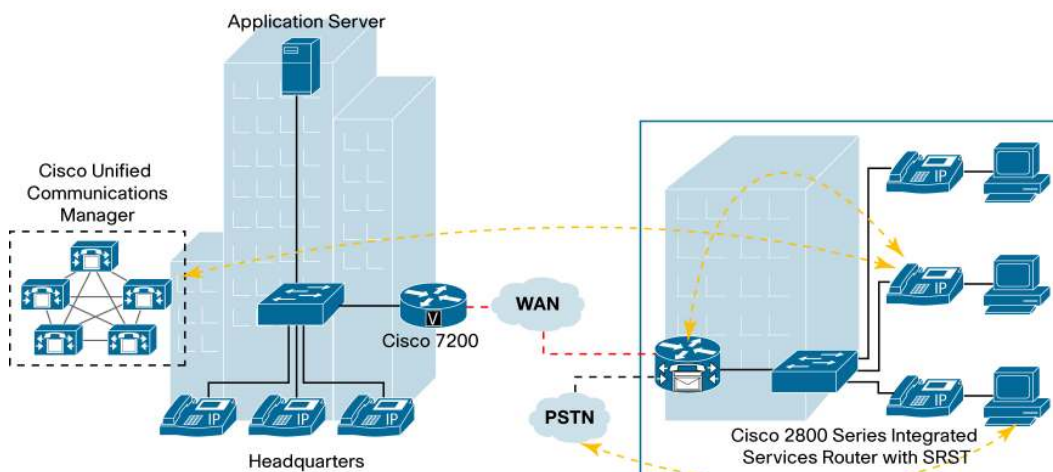
Simplifying Services Integration

For enterprise branch offices and small businesses where onsite telecom and IT expertise is scarce, integrated services are particularly critical. Cisco is the first and only vendor to offer a fully integrated solution that meets the unique needs of small businesses and enterprise branch offices. The telephony system, IP private branch exchange (PBX), voice messaging, data routing, switching, and security requirements are all integrated into a single unified communications platform that operates as a holistic system.

According to industry consultant Current Analysis, this convergence of routing protocols, security services, and voice applications in this platform helps "ensure the integrity and security of both the branch-office network and the central office that the branch is connected to". In essence, the integrated services router becomes a secure, all-in-one converged communications hub.

Cisco integrated services routers are uniquely suited to provide advanced security features with the IP PBX and voice gateway features. As many as 240 users can be supported with Cisco Unified Communications Manager Express, and 720 users with Cisco Unified SRST.

Without this systems approach to small- and branch-office unified communications, customers would instead be forced to deploy multiple devices, integrate their own solutions, and spend more time overall on configuration and troubleshooting. And at the same time they would be more vulnerable to security breaches and QoS problems.

Award-Winning Services and Support

Companies that have deployed Cisco Unified Communications on a Cisco Integrated Network also enjoy significant benefits from using Cisco as their primary vendor for lifecycle services and support. Cisco provides expert services that protect, optimize, and grow network platforms. Cisco and our partners provide a full range of lifecycle services and support that include:

- Comprehensive planning, design, implementation, and optimization services to help ensure a smooth and efficient migration to unified communications
- End-to-end integrated and validated solutions and systems that are easier to order, install, manage, upgrade, and use
- In-depth training, certification, and expertise delivered by Cisco and our worldwide partners
- Twenty-four-hour technical assistance and comprehensive service and support for the complete solution

Cisco and our partners have a proven record of high customer satisfaction and industry recognition of leadership for services and support. With a fully integrated unified communications solution from Cisco, in which the IP phones, access points, switches, routers, and other network components are from Cisco, customers can enjoy the following benefits:

- They can have one point of contact to receive speedy implementation and problem resolution.
- They can be among the first to deploy new features as they are developed. They will do so knowing that the unified communications solution and the integrated network will be completely compatible.

Summary

The benefits of deploying Cisco Unified Communications on a Cisco Integrated Network can positively affect an organization's revenue and profitability, providing competitive advantage for those customers that choose Cisco as their unified communications partner.

- When a high-tech Fortune 500 company replaced its old TDM voice technology with VoIP at 75 percent of its sites, it saved more than US$35 million in voice operating expenses over a span of 30 months. The company estimates its unified communications savings from employee productivity to be $220 to $280 million. This large enterprise was also able to integrate 30 acquisitions in 3 years with no increase in IT voice staff.
- By deploying unified communications across the business, a U.S. government agency exponentially increased its unified communications benefits. The agency expects to reduce annual travel costs by US$10 million and has already reduced voice conferencing costs by 50 percent while increasing monthly usage from 400,000 minutes to 2.5 million minutes in the first year.
- A high-end Japanese retailer used the embedded unified communications capabilities in its inventory application to optimize the customer experience in one of its biggest profit centers. The result? In the 6 months that the company piloted its radio frequency identification (RFID)-enabled in-store inventory application, it increased revenue growth by 113 percent over the previous year. At the same time, the company reduced its sales cycle time by 20 percent while dramatically improving customer satisfaction.

Ultimately, Cisco's extensive experience with unified communications and IP networks means that customers can be confident they have a strong ally in their efforts to implement a successful, secure, and powerful unified communications solution.

For more information, visit http://www.cisco.com/go/unified or contact your local Cisco representative or partner.

Americas Headquarters	**Asia Pacific Headquarters**	**Europe Headquarters**
Cisco Systems, Inc.	Cisco Systems (USA) Pte. Ltd.	Cisco Systems International BV
San Jose, CA	Singapore	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   C22-484573-00 07/08