



WHITE PAPER

BENEFITS OF DEPLOYING CISCO UNIFIED COMMUNICATIONS WITHIN A CISCO INTELLIGENT NETWORK

Adoption of IP Communications accelerated in 2005 as many businesses and organizations embraced this powerful technology. According to Synergy Research, the sales of IP telephony systems—to date the most popular of all IP Communications* applications—are projected to top US\$10 billion in 2009. Cisco Systems® alone is displacing almost 12,000 traditional phones every business day, and more than 37,000 Cisco® customers use an all-IP solution—the largest number of IP Communications installations in the industry.

THE ADVANTAGE OF DEPLOYING CISCO UNIFIED COMMUNICATIONS WITHIN A CISCO INTELLIGENT NETWORK

Cisco began developing IP Communications solutions in 1997 and has provided IP Communications services and applications longer than any other vendor. The Cisco Unified Communications system of voice and IP Communications products and applications helps organizations communicate more effectively—by helping them streamline business processes, reach the right resource the first time, and increase profitability. Cisco has led the industry in employing a *systems approach* that integrates Cisco Unified Communications within a Cisco Intelligent Network, helping enable capabilities and information sharing throughout the network. Cisco intelligent networks are *application-aware* and actively participate with the applications, automatically providing end devices with rights and priorities based on the needs of the device and the application in accordance with organizational policy. Embedded in the Cisco Intelligent Network, the Cisco Unified Communications applications are also *network-aware*; they seek out the network services they require—for example, an IP phone retrieving the proper settings for power or quality of service (QoS).

When the network and applications communicate in this way, IT and telephony administrators and end users achieve many benefits. Because the respective technologies are not locked in silos or just bolted together, administrators can use capabilities across platforms, providing the flexibility to quickly and cost-efficiently deploy, operate, and consolidate new communications services. New features and functions, such as video or wireless voice, can be added easily to this unified and integrated fabric through software upgrades and incremental hardware that build upon existing investments in the Cisco Unified Communications and network infrastructure. As a result, end users get access to new, high-quality IP Communications applications sooner, increasing their productivity and improving business processes.

From a financial standpoint, implementing a network with a single, primary vendor gives organizations a substantial opportunity to achieve a lower total cost of ownership (TCO) than does a network built with systems from multiple vendors, according to a study conducted by Sage Research (commissioned by Cisco) that included in-depth interviews with customers. A primary vendor supplies the network equipment, telephony systems, IP phones, and associated applications. The financial benefit found by this study is compelling: the network cost of ownership per endpoint in a primary-vendor network is 26 percent lower than that of a multivendor network. Savings are spread equally across all areas, including network deployment and maintenance, network performance improvements, and benefits for IT and end users. Sage Research also found that organizations that use a single, primary vendor for IP telephony have a 43-percent lower network cost of ownership than those that use multiple vendors. Further, Gartner's analysis of Cisco services in February 2005 reported that "Cisco's service and support continues to be an asset and a major source of differentiation between the company and the rest of the enterprise market."

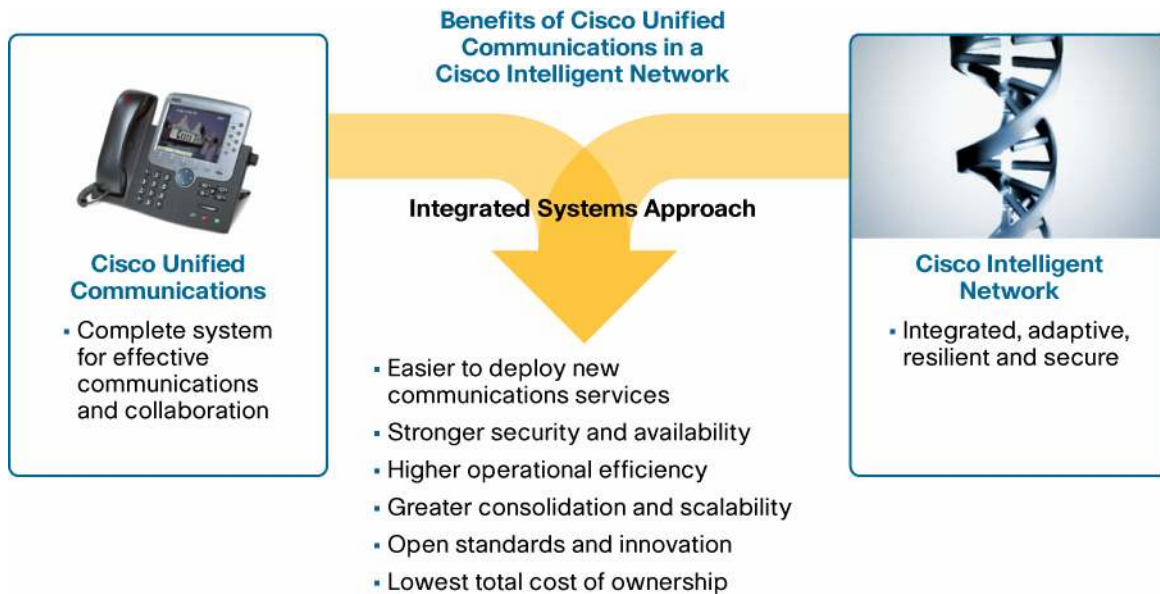
* IP Communications includes IP telephony; unified messaging and voicemail; contact center and self-service solutions; and audio, Web, and videoconferencing.

HOW CISCO DOES IT

A Closer Look at the Benefits of the Cisco Solution

Customers enjoy significant business and technical benefits by combining Cisco Unified Communications with a Cisco Intelligent Network, as summarized in Figure 1.

Figure 1. The Benefits of Deploying Cisco Unified Communications within a Cisco Intelligent Network



The following outlines how Cisco switching, routing, and wireless solutions uniquely deliver these benefits with Cisco Unified Communications.

DEPLOYMENT BENEFITS

- Faster, more cost-efficient IP phone moves, adds, and changes
 - Automatically configure Cisco Catalyst[®] switches for voice
 - Efficiently power Cisco Unified IP phones
 - Automatically configure Cisco Unified IP phones
- Ensure optimum voice quality across the WAN
- Secure IP Communications everywhere—from the endpoints to the network infrastructure
- Always-available voice

OPERATIONAL BENEFITS

- Faster resolution of voice issues
 - Rapid detection and notification of voice anomalies
 - Centralized troubleshooting—avoid onsite visits
 - Common view of the network for voice and data teams
- Reduced 911 costs and dispatching errors
- Greater accuracy of voice configuration changes

CONSOLIDATION BENEFITS

- Consolidated Cisco Unified Contact Center voice recording
- Scalable wireless voice services
- Services integration, which simplifies the network
- Video as a simple addition
- Integrated services and support

DEPLOYMENT BENEFITS

Faster, More Cost-Efficient IP Phone Moves, Adds, and Changes

The simplicity with which Cisco customers can make phone moves, adds, and changes and the resulting administrative cost savings is one example of the power of Cisco Unified Communications integration. In large companies, about 25 percent of their personnel move each year (a common industry standard for moves, adds, and changes) and the Yankee Group estimates that it costs companies up to US\$150 per move, add, or change. This operational expense can be minimized with Cisco Unified Communications products and Cisco Catalyst switching solutions.

After a Cisco Unified IP Phone is plugged into a wall jack, the connected Cisco Catalyst switch port can be automatically configured for voice and then it automatically provides the proper configurations and optimal power to the Cisco Unified IP Phone. Other vendors that offer only the voice components, or partner with infrastructure vendors, lack this type of integration. As a result, each time a phone is moved or added to the network, IT personnel must be notified so they can manually reconfigure the switch ports—significantly increasing administrative and support costs as IP telephony deployments continue to grow.

How It Works

Automatically Configure Cisco Catalyst Switches for Voice

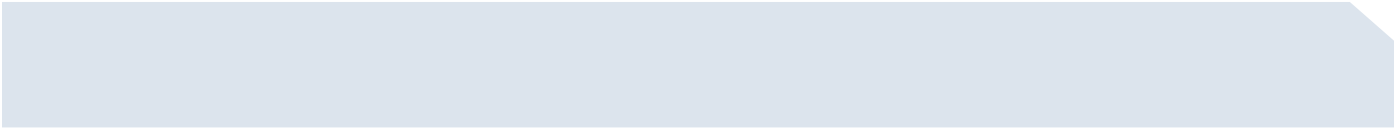
When a Cisco Unified IP Phone is plugged into a wall jack, the connected Cisco Catalyst switch (for example, the Cisco Catalyst 6500, Catalyst 4500, Catalyst 3750, Catalyst 3560, and Catalyst Express 500) detects that the link is now “up” and issues a Cisco Discovery Protocol exchange with the phone to get device information. If this information indicates that the endpoint is a Cisco Unified IP Phone, then the switch port can be automatically configured for voice using the Cisco IOS® Software Embedded Event Manager (EEM) feature in the Cisco Catalyst 6500.

Cisco EEM is a powerful and flexible automation technology that helps administrators to set custom policies that control what actions a switch should dynamically take when particular events occur.

At a later time, if users decide to unplug their phone and move it to a new location, then removing the voice configuration on the previous switch port helps to strengthen security. This removal can be done dynamically when the phone is unplugged, helping reduce administrative costs. This dynamic switch configuration change is once again enabled by the Cisco EEM feature.

In addition to the EEM-based method of automatically configuring switch ports for voice, Cisco also offers administrators who use Cisco Network Assistant, the GUI-based network management application for small and medium-sized business (SMB) networks, another method to quickly configure 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 then has the option to apply the appropriate Smartports voice macro (described later in the paper) to that switch port, simplifying the Cisco Catalyst switch configuration for voice.

Additional Cisco technologies, such as Smartports macros or AutoQoS macros, can be used to simplify and increase the accuracy of voice configurations on Cisco Catalyst switches. Cisco Smartports macros include a suite of voice-critical macros and templates that can be applied to any Cisco Catalyst switch port (for example, the Cisco Catalyst 6500, Catalyst 4500, Catalyst 3750, Catalyst 3560, and Catalyst Express 500) to make configuration much simpler. These macros are based on Cisco best practices and experience with running IP Communications in the network. With a standard or customized Cisco Smartports macro, an administrator no longer has to log into each network switch port and



configure all the parameters for ports that support IP Communications, including such parameters as voice VLANs, port security, Dynamic Host Configuration Protocol (DHCP) snooping, and Spanning Tree PortFast. Instead, the company can automatically upload a single template to a switch that includes all the proper settings. Cisco Smartports macros do not function in third-party or multivendor network environments, translating into loss of a powerful cost- and time-saving tool. Administrators can also develop custom Smartports macros that take advantage of other time-savings Cisco technologies, such as AutoQoS.

Cisco developed AutoQoS macros in response to customer demand for a faster way to deploy QoS configurations, which may have to be set on hundreds or thousands of switch and router ports to assure optimal voice and video quality, regardless of network congestion. This powerful feature of Cisco IOS Software automatically handles a range of tasks traditionally done manually, including classifying applications, generating policies, configuring the proper QoS configurations, monitoring and reporting to test QoS effectiveness, and enforcing service-level consistency. After Cisco AutoQoS evaluates a network environment and determines policy, *with only one command* it configures the port on an access switch to prioritize voice traffic—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. In network environments that lack Cisco AutoQoS, applying QoS involves many repetitive steps that must be applied individually to each switch in the network. Although Cisco AutoQoS enhances the operation of voice traffic from any source, it has been specifically optimized and tested only on a Cisco end-to-end infrastructure. Cisco has completed extensive benchmarking encompassing thousands of hours to deliver the highest compatibility of Cisco AutoQoS across Cisco switches, routers, and IP phones.

Efficiently Power IP Phones

IP Communications devices such as IP phones require power to operate, but getting power from a wall socket is not always a viable option—especially when phones scale into the thousands. In 2000, Cisco was the first company to introduce inline power (evolving to Power over Ethernet [PoE], the IEEE 802.3af standard) that enabled the LAN switching infrastructure to provide power over an Ethernet cable to a powered device. Cisco offers Cisco Unified IP phones and Cisco Catalyst switches (for example, the Cisco Catalyst 6500, Catalyst 4500, Catalyst 3750, Catalyst 3560, and Catalyst Express 500) that support both the 802.3af standard and Cisco prestandard PoE (inline power) for additional flexibility.

Beyond the basic PoE standard, Cisco provides additional levels of power control with Cisco Intelligent Power Management (IPM) and massive PoE scalability that enables high-density PoE deployments. Like other unique features available with Cisco Unified Communications in a Cisco infrastructure, Cisco PoE provides customers with significant power-consumption savings to powered 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 (for example, a single Cisco Catalyst 6500 can support more than 288 Class 3 PoE devices), thereby minimizing the number of required Cisco Catalyst switches and the cost of electricity, backup UPS, and battery power systems.

To further optimize power consumption and to protect the switch against misbehaving endpoints, administrators can set hard limits on the amount of power that is delivered to each switch port, using the latest Cisco Catalyst 6500 PoE daughter card. By limiting the power on a per-port basis, this card can safely override IEEE standards-based power classification, and the switch shuts off the port when it exceeds the configured power limit, protecting the switch from over-current and over-subscribing the power supply.

Automatically Configure Cisco Unified IP Phones

When the Cisco Catalyst switch has the proper voice configuration and is delivering the appropriate amount of power to the Cisco Unified IP Phone, it can use the Cisco Discovery Protocol to automatically set certain configurations on the Cisco Unified IP Phone and other devices attached to the phone (for example, a PC). The Cisco Catalyst switch indicates to the Cisco Unified IP Phone the voice VLAN ID** it should use and the class-of-service (CoS) value it should apply to the voice traffic. The Cisco Catalyst switch, using the Extended Trust feature, can also indicate what CoS value the Cisco Unified IP Phone should apply to traffic coming from devices attached to the phone. 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 marked with a 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 Extended Trust CoS value communicated by the Cisco Catalyst switch. As a result, voice quality through the switch is not adversely affected by that rogue PC.

** Voice VLANs can be thought of as individual channels within a physical network. They are used to isolate traffic that is highly sensitive to network conditions such as voice so that this traffic can be assigned preferential treatment through QoS settings.

Ensure Optimum Voice Quality Across the WAN

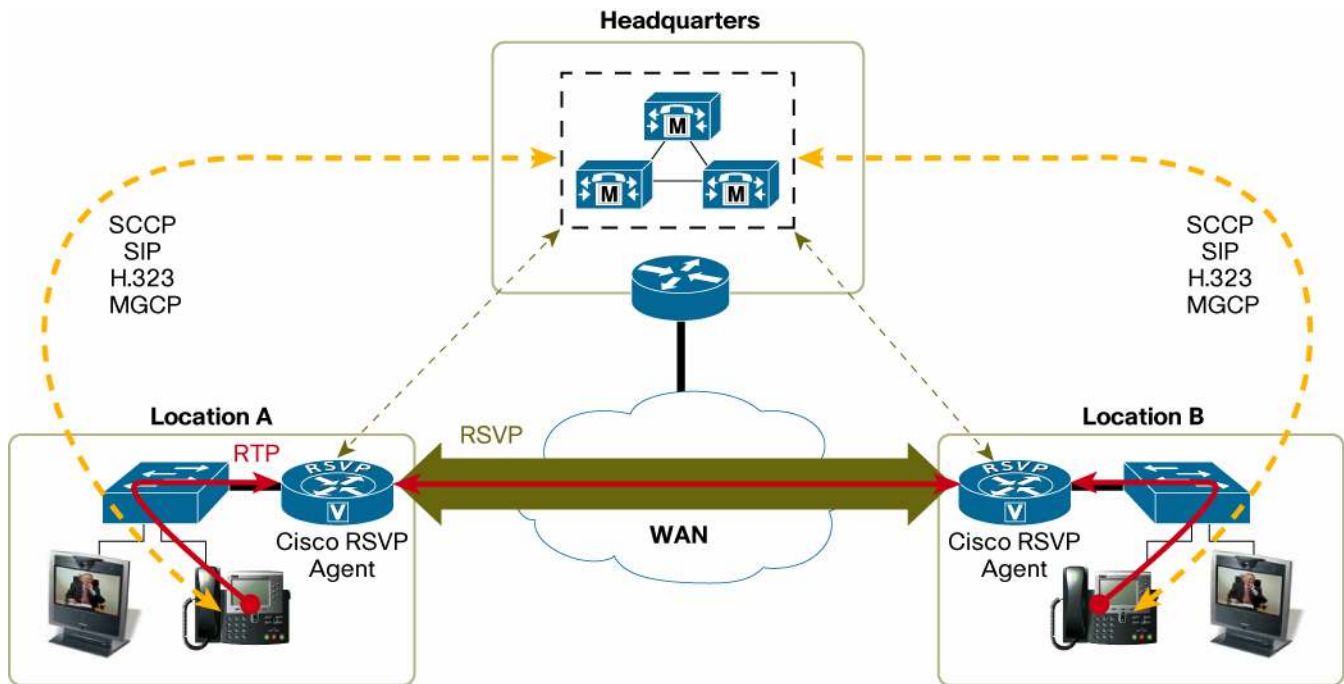
Cisco has also taken a *systems approach* of integrating Cisco Unified Communications within a Cisco Intelligent Network to help ensure optimum voice quality across the WAN. Not only do Cisco integrated services routers support standards-based QoS, but they also exchange information with Cisco Unified CallManager to enable network-aware Call Admission Control (CAC) with QoS. With CAC, the network can 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, which helps enable 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), an IETF standards-based signaling protocol for reserving resources in the IP network, secures and reserves bandwidth across the WAN for calls accepted by Cisco RSVP Agent. 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 2600XM, 2691, 2800, 3700, and 3800 series integrated services routers.

How It Works

IP voice call setup is initiated between the IP phone, IP videophone or gateway, and Cisco Unified CallManager. Cisco Unified CallManager classifies a call based on parameters such as application (voice or video) and Multilevel Precedence and Preemption (MLPP), and signals to the Cisco RSVP Agent in the access router. Bandwidth pools are preconfigured in the router on a per-application and per-interface basis. Using the classification provided by Cisco Unified CallManager, the Cisco RSVP Agent attempts to set up a call within the appropriate bandwidth pool and across the WAN to a far-end Cisco RSVP Agent for the receiving party. If RSVP bandwidth is secured, the Cisco RSVP Agent signals back to Cisco Unified CallManager. Cisco Unified CallManager in turn signals to the IP phone, IP videophone, or gateway and the call proceeds. The Cisco RSVP Agent can apply differentiated services code point (DSCP) marking to media packets based on instruction from the Cisco Unified CallManager. DSCP packet marking may be applied to place the RSVP secured media stream into the router priority queue. If RSVP bandwidth cannot be secured, the Cisco RSVP Agent signals back to Cisco Unified CallManager, which administers policies. The call is either disallowed or allowed to proceed with a lower-priority DSCP packet marking applied by the Cisco RSVP Agent as instructed by the Cisco Unified CallManager.

Mid-call policies may also be applied for handling of changes to the media stream such as transfers during a call. Network design using the Cisco RSVP Agent allows voice and video calls to proceed as part of a single unified network together with data. This setup allows for support of meshed designs, multitiered designs, adjustment to dynamic link changes, and redundant links. This single design helps reduce the costs for both infrastructure and management. Because CAC is managed and secured and QoS is applied as a network component, there is no reliance on end-user devices. Cisco RSVP Agent functions independently of the call-signaling protocol, and hence, Session Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP), H.323, and Media Gateway Control Protocol (MGCP) are all supported. Figure 2 shows how the Cisco Unified CallManager and Cisco RSVP Agent in the router work together to optimize the voice quality across the IP network.

Figure 2. Cisco Integrated Services Routers and Cisco Unified CallManager Help Ensure Optimal Voice Quality Across the WAN



Secure IP Communications Everywhere—From the Endpoints to the Network Infrastructure

Security can no longer be viewed as a mix of point-product solutions. The increasing number of applications and devices available on the network introduces many new points of vulnerability—from IP phones to wireless devices to remote users. Network security must be pervasive, from endpoints such as IP phones and PCs to the software and devices in the network infrastructure itself. In essence, the network becomes the main point of control for preventing and responding to security threats from internal and external sources.

When customers deploy Cisco Unified Communications applications in a Cisco infrastructure, they do not have to implement a separate security apparatus. Cisco provides all three critical security components: secure connectivity, trust and identity, and threat defense; Cisco also is the only vendor that integrates these technologies deep into the fabric of the network. Whereas some competitors focus either on securing only the voice components or on securing the infrastructure itself, Cisco takes a systems-level approach that offers security features and capabilities in the transport network, the endpoints, the call-processing infrastructure, and the applications. Taking advantage of the intelligence of the network to manage security just makes sense.

How Cisco Does It

Within the Cisco Self-Defending Network architecture, Cisco offers the following security for Cisco Unified Communications:

- **Secure connectivity**—To help ensure that communications over the WAN, LAN, and wireless LAN (WLAN) are secure and private, Cisco offers many options. VLAN segmentation keeps voice traffic on separate virtual network segments, and Voice and Video Enabled VPN (V3PN) affords secure remote connectivity. WLANs are protected through Wi-Fi Protected Access (WPA) and WPA2. Additional capabilities, such as traffic and processor thresholds and route authentication, protect the stability and availability of the network infrastructure. Call management and endpoints offer strong voice media encryption using the Secure Real-Time Transport Protocol (SRTP), and the protection of signaling traffic with Transport Layer Security (TLS). And, at the application layer, Cisco uses HTTPS to permit protected remote management of IP Communications applications. Also, the Cisco Unity® system is the first voice messaging system to offer secure private (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 through the use of such tools as Extensible Authentication Protocol (EAP) and digital certificates. Customers can smoothly enable voice on their secure data networks with important capabilities such as 802.1x with voice VLANs and secure WLANs that allow IP phones to transparently connect on ports where user authentication with 802.1x is mandated. And 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 before they have a chance to enter the network and potentially disrupt voice services.
- **Threat defense**—Many techniques protect against aggressive threats. Firewalls, both integrated and standalone, 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. Cisco is the only vendor to offer advanced dynamic Address Resolution Protocol (ARP) inspection protection and other tools on the LAN switches and Cisco Unified IP phones to protect the endpoints against common Layer 2 exploits such as man-in-the-middle attacks. And the Cisco Unified Communications applications themselves offer security features: for example, Cisco Unified CallManager offers the ability to support multiple levels of administration access and advanced protection against toll fraud. As part of providing robust network infrastructure, it is also important that the network infrastructure be able to withstand denial-of-service (DoS) attacks so that data and voice traffic continues to be forwarded even when such attacks occur. For example, the Cisco Catalyst 6500 and Catalyst 4500 provide such protection through CPU rate limiters as well as control plane policing (CoPP) in hardware.

This integrated security helps Cisco offer an IP telephony network that is the strongest, most secure system available, according to a 2004 Network World report that was based on a study by Miercom, a leading New Jersey-based network consultancy and product test center. The report also noted that “a sophisticated hacker assault team could not break or even noticeably disturb [it] even over three days of concerted effort.” Cisco security is based not on point products, but rather on multilayer, system-level security that pervades the entire infrastructure, from endpoints such as the IP phones or PCs to the call-processing components to the software and silicon on the router.

For more information about Cisco Unified Communications and security, visit <http://www.cisco.com/go/ipcsecurity>.

Always-Available Voice

As customers transition from traditional time-division multiplexing (TDM) voice networks to IP-based voice networks, voice services need to be continuously available.

In addition to proper network design, operations, management, and support, Cisco high-availability innovations lead the industry in meeting these uptime requirements. These innovations contain, detect, and resolve faults faster so that the impact to voice traffic is minimized. For example:

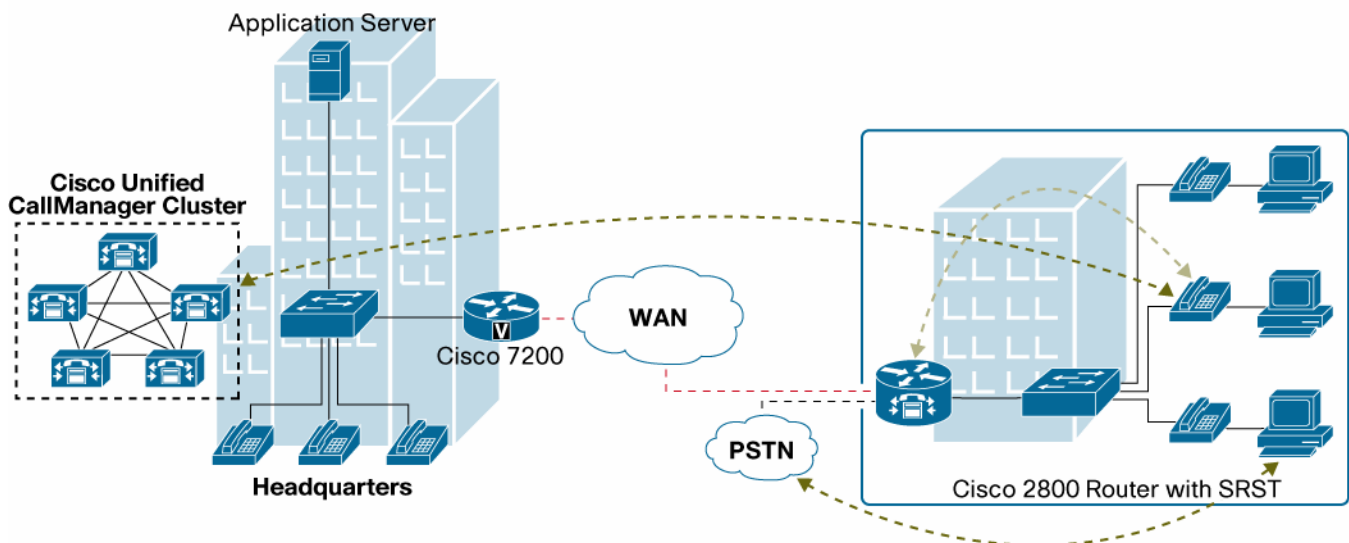
- When using the Cisco Catalyst 6500 with IOS Software Modularity, if a software process failure occurs, voice calls continue, even in single supervisor engine systems. This innovation localizes the effect of software process faults with a protected memory architecture so that the switch continues normal operation if they occur. By using the process restartability capability with state checkpointing and Non-Stop Forwarding (NSF), Cisco IOS Software Modularity also minimizes service disruption by avoiding routing reconvergence if there is a fault in a routing process. Cisco Catalyst 6500 switches with IOS Software Modularity also help enable software updates (for example, security patches, software fixes, etc.) to be incorporated into the switch without disrupting voice calls. This process is achieved through the subsystem In-Service Software Upgrade (ISSU) capability.
- Layer 3 NSF and Layer 2 stateful switchover (SSO) on the Cisco Catalyst 6500 and Catalyst 4500 preserve critical state information across dual supervisor engines to help ensure that voice and data traffic is continually switched if a primary supervisor engine fails.
- Real-time diagnostics in the Cisco Catalyst switches help protect the network against latent module failures, which can potentially cause erratic behaviors (such as routing flaps or link flaps) that add latency to voice calls or decrease call quality. Real-time diagnostics minimize these situations through proactive hardware and software fault-detection mechanisms. Combined with NSF, SSO, and custom EEM policies, these detection mechanisms can be used to automatically trigger subsecond supervisor engine failover (for complete or partial supervisor failures), helping enable the switch to dynamically heal itself.
- Cisco StackWise™ technology on the Cisco Catalyst 3750 creates a unified logical switching architecture that delivers a high level of resiliency for voice-enabled wiring closets.

Cisco designed its unified communications system from the beginning for packet networks. Cisco Unified CallManager, Cisco Unified IP phones, Cisco Unity voicemail and unified messaging servers, and Cisco Unified Contact Center and self-service solutions are all liberated from specific physical locations. Customers can design their networks by placing Cisco Unified CallManager and other Cisco call-control servers in clusters and deploying them in multiple locations anywhere in the network. When Cisco Unified CallManager and these other servers are distributed across an IP network in a cluster design, resiliency is built into the infrastructure and can take full advantage of the routeability and inherent resiliency of IP packet networks.

Although this type of architected resiliency can be common to all IP-based communications environments, Cisco adds an industry-first resiliency capability at remote sites with Cisco Unified Survivable Remote Site Telephony, a unique capability embedded in the Cisco IOS Software running on Cisco integrated services and multiservice access routers. In a centralized call-processing model, the Cisco Unified Survivable Remote Site Telephony router facilitates automatic failover so that 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. If the WAN link to a remote office fails and connection to the Cisco Unified CallManager for the domain is lost, the phones in that branch office automatically redirect to the Cisco Unified Survivable Remote Site Telephony router. The Cisco Unified Survivable Remote Site Telephony router automatically takes over and offers a rich set of telephony functions to help ensure business continuity with minimal impact. When the disrupted WAN link is restored, the phones automatically reregister with the original Cisco Unified CallManager—and again, no manual intervention is required. Cisco Unified Survivable Remote Site Telephony is accomplished through this integrated system with no additional hardware components (Figure 3).

Figure 3. Cisco Unified Survivable Remote Site Telephony—Voice Redundancy if WAN Failure Occurs

- Offers resiliency for remote IP telephony users with central Cisco Unified CallManager
- Minimizes business effect of WAN link failure
 - Cisco router auto-configures, provides local call processing—no manual intervention required
 - Cisco Unified Survivable Remote Site Telephony IP phones calls remain secure
 - When WAN is available, IP phones auto-revert to Cisco Unified CallManager



OPERATIONAL BENEFITS

Faster Resolution of Voice Issues

Malfunctions in any components of the voice-processing infrastructure, in the LAN or WAN connections, or in the infrastructure itself can affect voice quality. Given the business criticality of voice applications, it is important that the network infrastructure provide deep visibility

into voice traffic so that any issues can be quickly identified and resolved. When the Cisco network infrastructure and management tools detect excessive voice packet loss, jitter, or latency, they can alert network administrators of these issues and then enable 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, they can communicate about concerns with much greater precision and understanding—leading to faster problem resolution.

How It Works

Provide for Rapid Detection and Notification of Voice Anomalies

Voice traffic is typically assigned to the strict-priority queue (the highest-priority queue) on a given switch interface. An EEM script on a Cisco Catalyst 6500 can be set up so that if excessive packet drops in the strict-priority queue are detected, an alert can be immediately sent to the network administrator. In addition, the network analysis module (NAM), a data, voice, and video traffic analysis blade for the Cisco Catalyst 6500, provides multifaceted voice traffic monitoring and troubleshooting capabilities. If the dial tone or call setup latency exceeds specified thresholds, the NAM detects these anomalies by analyzing Cisco Unified CallManager response times and then sends alerts to a network operator. For H.323, MGCP, and SCCP (SIP in mid-2006) traffic, the NAM monitors active calls between caller and callee pairs and identifies call quality degradation by reporting packet loss and jitter statistics. Also, the NAM performs Differentiated Services (DiffServ) QoS monitoring and provides traffic usage information for each DiffServ code point, helping to validate QoS planning assumptions and detect incorrectly marked or unauthorized traffic that could adversely affect voice traffic.

Centralized Troubleshooting—Avoid Onsite Visits

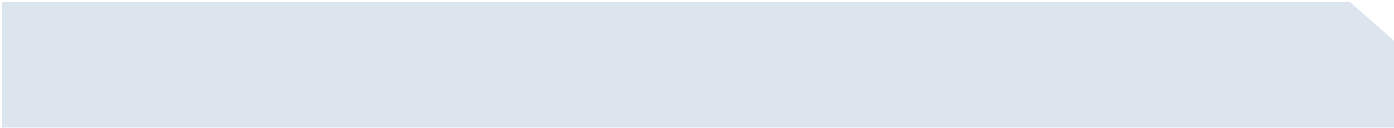
When an administrator is alerted to a voice problem by a given switch, then that administrator can instruct the switch to mirror the real-time voice traffic so it can be analyzed. The challenge is that typical traffic mirroring technologies require the administrators to go on site so they can directly connect to the switch or to the same subnet as the switch. However, using the Encapsulated Remote Switched Port Analyzer (ERSPAN) feature on the Cisco Catalyst 6500, administrators can mirror real-time voice traffic across the campus and across Layer 3 boundaries to a central site, where it can be analyzed by the NAM. This saves administrators time and effort because they do not need to go on site with a portable troubleshooting tool to solve the problem.

Voice and Data Teams Share 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 network. But because problems can span both realms with IP Communications, it is essential that both teams have the facility to 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. It can query Cisco Catalyst switches to ascertain the operational status of the switch as well as the system resources and different ports and interfaces and then alert administrators in case of operational faults. It enables tracking of IP phone inventory, and also tracks IP phone status changes, and creates a variety of reports that document move, add, and change operations on IP phones in the network. It increases productivity and enables faster trouble isolation by providing contextual diagnostic tools to enable troubleshooting:

- Through diagnostic tests, performance, and connectivity details about different elements of the Cisco Unified Communications infrastructure
- Using synthetic tests that replicate end-user activity and verify gateway availability and other configuration and operational aspects of the Cisco Unified Communications infrastructure
- Through IP service-level agreement (SLA)-based diagnostic tests that can measure the performance of WAN links and measure node-to-node network quality
- By providing actionable information in notification messages (Simple Network Management Protocol [SNMP] traps, syslogs, and e-mail) through context-sensitive links to more detailed information about service outages



Today, the network operations team monitors the network infrastructure with the CiscoWorks LAN Management Solution (LMS). And the voice operations team can view the IP communications infrastructure with the Cisco Unified Operations Manager 1.0. Because both management tools are part of the CiscoWorks suite of tools, however, they share a common framework and terminology. Therefore, the voice team can troubleshoot voice quality issues, even if that takes them into the network elements of the data infrastructure. Because a set of tools and a common view of the network is shared between the voice and data teams, they can communicate about the problem with much greater precision and understanding—leading to faster problem resolution.

Reduced 911 Costs and Dispatching Errors

Operational costs are also lowered (and worker safety enhanced) with another unique feature of Cisco Unified Communications in a Cisco infrastructure solution—E911, an application that is available with Cisco Emergency Responder.

The challenge with any E911 system is how to maintain an up-to-date list of phones and their locations so that emergency personnel can be dispatched quickly to the correct location. This maintenance can be a challenge because large companies on average move almost 25 percent of their employees each year. Cisco provided an industry-unique solution to this problem for IP Communications that eliminates manual updates required in other 911 systems—both IP and TDM—and reduces dispatching errors.

How It Works

Emergency services can be a challenge with IP telephony because in conventional private-branch-exchange (PBX) implementations—both IP and TDM—every direct-inward-dial (DID) number is an Emergency Location Information Number, or ELIN (a dialable telephone number), which must correspond with an Emergency Response Location (ERL). The ERL contains information such as street address and floor number. In the enterprise environment, ERLs and their associations with ELINs are created by the customer and sent to the public safety database. In conventional TDM and IP 911 systems, each time a device corresponding to a DID changes location, the associated ERL must be changed administratively, and an update must be sent to the public safety database. This manual updating process is time-consuming.

When Cisco Unified IP Telephony solutions run on a Cisco infrastructure, Cisco Emergency Responder dedicates a relatively small number of DIDs to be ELINs. Cisco Emergency Responder works with Cisco Discovery Protocol to track devices automatically as they change location and maintains a database that associates the new device location, or ERL, with an appropriate ELIN. When an emergency call is placed, Cisco Emergency Responder associates the correct ELIN with a device based on its current location. This approach does not require that locations be associated with common DIDs or be administratively changed and updated with the public safety database. Only the dedicated ELINs and their associated ERLs need to be maintained, and these should be very stable, changing only when a customer adds or decommissions a building.

Greater Accuracy of Voice Configuration Changes

Misconfigurations by administrators not only can adversely affect network uptime, but also can increase operational costs by requiring additional effort to fix the misconfigurations. If administrators choose to make further voice configuration changes on their switches, they can accurately do so by taking advantage of the Cisco best practices incorporated in the Smartports and AutoQoS features described in the previous “Deployment Benefits” section. In addition, the Cisco Catalyst 6500 offers further capabilities to enable efficient and accurate voice configuration changes. If configuration changes are applied but do not achieve their desired effect, then administrators can use the Configuration Rollback feature to return to a previous configuration state. If administrators want to check to see if there might be a voice configuration error on their switch, then they can run a configuration checking command (**show diagnostic sanity**) to see if any warnings appear (for example, port duplex mismatch or PortFast on phone port not enabled).

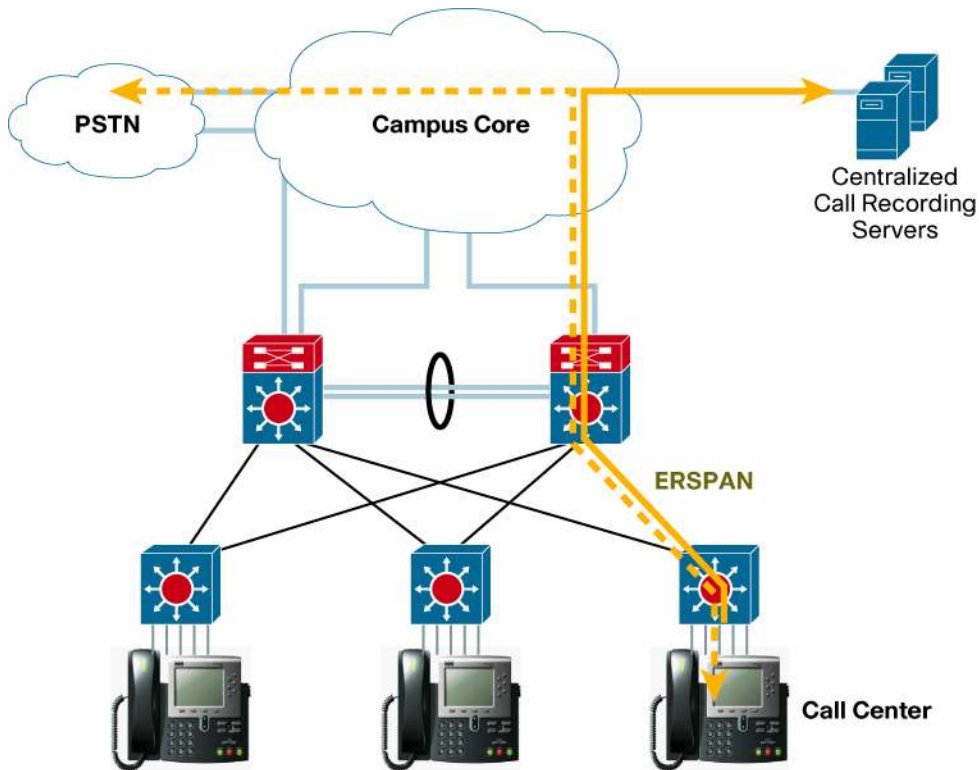
In addition, Secure Copy Protocol (SCP) for the Cisco Catalyst 3750 provides a secure and authenticated method for copying switch configuration or software images to other members of a Cisco Catalyst 3750 switching stack. This ability to safely copy switch configuration and software images greatly reduces errors that could be introduced by manually configuring multiple switches in the same switching stack.

CONSOLIDATION BENEFITS

Consolidated Cisco Unified Contact Center Voice Recording

For compliance and quality purposes, many organizations require voice recording of their IP contact center calls and trading floor conversations. These replicated calls have typically been sent to multiple voice recording servers located on each floor, using SPAN or RSPAN mirroring technologies. However, using the ERSPAN feature on the Cisco Catalyst 6500, the replicated voice calls can be sent to centralized call recording servers located several hops away across the campus LAN (Figure 4). This centralization enables the voice recording servers and associated storage to be consolidated, reducing operational and capital expenditures.

Figure 4. ERSPAN Feature Helps Enable Centralization of Cisco Unified Contact Center Voice Recording



Scalable Wireless Voice Services

Today's businesses are turning to wireless networking to give employees immediate access to the business applications and communication tools they need. By adding voice-over-IP (VoIP) capability to their wireless networks, businesses can further improve collaboration and responsiveness, and realize new cost savings. The combination of Cisco Unified Communications and the Cisco Unified Wireless Network*** lets businesses and other organizations take immediate advantage of IP Communications for a mobile workforce while minimizing TCO. Cisco has integrated important technologies into its switching, routing, and wireless offerings to provide optimal support for wireless voice that enables simplified wireless voice deployment and management, wireless voice call roaming, diverse wireless voice client support, and high-quality wireless voice communications.

*** The Cisco Unified Wireless Network is an integrated end-to-end solution that addresses all layers of the WLAN, from client devices and access points to switching and routing, to network management, to the delivery of advanced wireless services integration and award-winning, worldwide 24-hour product support.

Simplified Wireless Voice Deployment and Management

As wireless access points are deployed to provide pervasive wireless coverage for IP Communications, it becomes important to ease the deployment and management of these devices while keeping the network secure. Integrating wireless controller functions into Cisco switches and routers gives network managers the control to scale and manage their wireless networks as easily as they scale and manage their traditional wired networks. For example, the Cisco Catalyst 6500 Series Wireless Services Module (WiSM) supports zero-touch deployments that do not require manual or preconfiguration of the access points. It also supports template-based configuration management that enables the quick application of system wide wireless security configurations, QoS policies, mobility groups, back-end services, and other important configurations. The Cisco Catalyst 6500 WiSM supports several embedded troubleshooting tools and when deployed with the Cisco Wireless Control System (WCS), it supports enhanced monitoring and troubleshooting features, including intuitive heat map displays, alarm filtering, event correlation, and granular reporting tools. This Cisco Catalyst module also supports the simultaneous tracking of thousands of devices from directly within the WLAN infrastructure when deployed with the Cisco Wireless Location Appliance. The Cisco Catalyst 6500 WiSM helps enable maximum access point coverage scalability—300 lightweight access points per module (10,000+ wireless client devices) and clustering of up to 3,600 lightweight access points per roaming domain. For remote-site deployments, Cisco also offers the Cisco Wireless LAN Controller Module (WLCM) for Cisco integrated services routers that can manage up to six lightweight access points. Standalone WLAN controllers (for example, the Cisco 4400 and 2000) 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 and the WLCM offer fast, secure roaming that helps enable voice clients to roam 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 Voice Clients

A growing number of client devices support 802.11 wireless voice communications today, including dual-mode cell phones (for example, Nokia E60, E61, E70), personal digital assistants (PDAs), laptop soft phones, and Wi-Fi handsets (for example, Cisco Unified Wireless IP Phone 7920). Cisco offers a licensing program called Cisco Compatible Extensions for wireless clients to help them interoperate securely with the Cisco Unified Wireless Network and help enable interoperability of client-side features such as power save mode, QoS, and assisted roaming that voice communications require. 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 Wireless Voice Communications

QoS is vital to enabling reliable, toll-quality voice communication. Cisco wireless access points, client devices, and Cisco Compatible Extensions devices include support for Wi-Fi Multimedia (WMM), a component of the IEEE 802.11e WLAN standard that supports priority tagging and queuing to ensure intelligent handling of voice communications. Implementing QoS in a WLAN makes network performance more predictable and bandwidth usage more effective. Through the use of Layer 2 admission control, QoS can be maintained under heavy user loads to meet demanding wireless networking needs.

Services Integration Simplifies the Network

For small businesses and enterprise branches where onsite telecom and IT expertise is scarce, the benefits of data and voice integration are particularly critical. Cisco is the first and only vendor to offer customers a fully integrated solution that meets their telephone system and small PBX, voice messaging, data routing, switching, and security requirements in a single platform.

By operating as a holistic system, Cisco integrated services routers are uniquely suited to provide advanced security features with the IP PBX and voice gateway features needed to support up to 240 users with Cisco Unified CallManager Express and 720 users with Cisco Unified Survivable Remote Site Telephony.

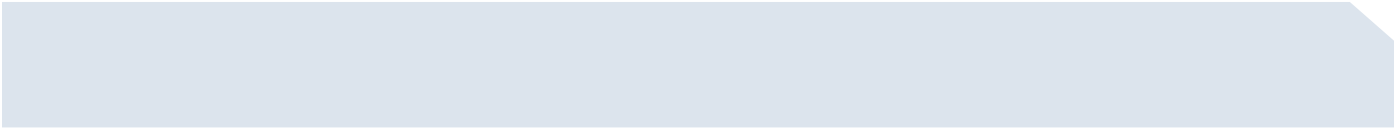
According to industry consultancy Current Analysis, this convergence of routing protocols, security services, and voice applications helps “ensure the integrity and security of both the branch-office network and the central office that the branch is connected to.” In essence, this allows the integrated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

Without this systems approach to small-office and branch-office IP Communications, customers would instead be forced to deploy multiple devices, systems-integrate their own solutions, and spend more time overall on configuration and troubleshooting—all while being more vulnerable to security breaches and QoS problems.

Features of Cisco Integrated Services Routers

- Embedded full-featured call processing in Cisco IOS Software with Cisco Unified CallManager Express or failover capability with Cisco Unified Survivable Remote Site Telephony
- An integrated Cisco Unity Express Advanced Integration Module (AIM) or network module for local Auto Attendant and voicemail
- Embedded security for V3PN and encryption
- Embedded digital-signal-processor (DSP) slots for VoIP processing and both transcoding and multiparty conferencing
- Integrated voice WAN interface cards (VWICs) for both voice and data connectivity needs
- Integrated WLCM, which can simplify the management of up to six lightweight access points
- Integrated call-quality monitoring and troubleshooting with the NAM for integrated services routers
- Integrated network modules that scale to 24 analog ports, plus 12 foreign-exchange-office (FXO) ports or 8 digital Basic Rate Interface (BRI) ports
- Integrated low-density switching modules for PoE to phones and wireless access points
- Intelligent Cisco IOS Software routing protocols such as the wide range of QoS protocols

In addition, numerous voice functions, such as transcoding****, voice gateway (PSTN and PBX), and connectivity to older analog devices, have been integrated into the Cisco Catalyst 6500 Series switch through the Cisco Communications Media Module. These switch-integrated functions help to smooth the transition from older endpoints to IP-based endpoints.



**** Transcoding enables communication between different types of codecs, which are used to convert voice from analog to digital signals—such as when data packets must be sent from the IP infrastructure across the PSTN.

Video as a Simple Addition

The unique advantage of deploying video on a Cisco infrastructure is the resulting unity of applications and infrastructure. After customers deploy a Cisco Unified Communications system, enabling video is as easy as adding any other application to the network. Cisco Unified Video Advantage is a video telephony solution comprising the Cisco Unified Video Advantage software application and Cisco VT Camera, a video telephony USB camera. With the Cisco VT Camera attached to a PC co-located with a Cisco Unified IP Phone, users can place and receive video calls on their enterprise IP telephony network. Users make calls from their Cisco Unified IP phones using familiar phone interfaces, but now calls are enhanced with video on a PC, without requiring any extra button-pushing or mouse-clicking. With Cisco Unified Video Advantage, video is integrated into the Cisco infrastructure much like voice and uses the same network intelligence already operating for voice. This integration helps enable tight weaving of video into the existing voice and Web meeting workflows. With any phone call, the network automatically determines if a user's PC is equipped with a Cisco Unified Video Advantage client. If users have Cisco Unified Video Advantage, a video session automatically starts on the PC simultaneous with the initiation of the phone connection. Call features such as call forward, transfer, conference, and hold are now available with video and are all initiated through the Cisco Unified IP Phone. In addition, the application itself has intelligence and seeks out network services automatically. Cisco Unified Video Advantage negotiates with the intelligent network to help ensure it has priority settings for efficient video delivery.

The intelligence of the infrastructure extends out to all types of devices—a laptop, a PDA, a mobile phone, or a remote PC—and automatically determines if the device is video-enabled. If so, the required settings are generated automatically, and the appropriate switches are instructed to provide the proper VLAN and QoS settings to allow the video stream.

Without the network intelligence, video cannot be integrated as easily, proper settings require more manual effort, and manageability is compromised.

Not only can new endpoints be easily video-enabled, traditional videoconferencing equipment based on the H.323 videoconferencing standard can be brought onto the converged network. IT managers can point Cisco Unified CallManager to these systems, and they can be enabled to automatically register to Cisco Unified CallManager. Thereafter they can be controlled by Cisco Unified CallManager.

Dial plans for both video and voice are also integrated in a Cisco Unified Communications on a Cisco network solution. Just as a user would dial a five-digit number to join an audio conference, the user would dial the same five-digit number to join the videoconference. The user simply dials the number and a screen pop alerts the user as to whether the videoconference has video availability.

From an IT perspective, videoconferencing management is dramatically simplified because call detail records (CDRs) are also integrated into and managed by Cisco Unified CallManager. IT managers no longer must download CDRs from two separate systems—the phone and the video. Instead, all records are located in one place.

Integrated Services and Support

As customers migrate to unified communications, they have found significant benefits in services and support from a primary vendor. The end-to-end Cisco Intelligent Network and Cisco Unified Communications services and support provide customers with critical benefits that deliver strategic, business, technical, and cost-savings advantages.

Cisco Systems offers the products, services, technology expertise, and market leadership that make it a strong choice as a primary vendor and business partner. Cisco customers gain unmatched, comprehensive solutions backed by expert services throughout the network lifecycle while preserving their technology investments for the future. A few examples of services and support that differentiate the Cisco Unified Communications solution within a Cisco Intelligent Network include:

- Comprehensive planning, design, implementation, and optimization services that provide smooth and efficient migration
- End-to-end, integrated solutions and systems that are easier to order, install, manage, upgrade, and use
- Cisco in-depth training, certification, and expertise delivered by Cisco and worldwide partners
- End-to-end, 24-hour technical assistance and comprehensive service and support for the complete solution.

Companies must protect, optimize, and grow their network platforms using a lifecycle support model that creates business value and operational excellence. Cisco and its partners provide a full range of lifecycle services and support that are critical for today's foundation and advanced networking technologies, including routing, switching, unified communications, wireless, security, storage, and optical solutions. Cisco and its partners have a proven record of high customer satisfaction and industry recognition of leadership for services and support.

In addition, with a fully integrated communications system from Cisco (where the IP phones, access switches, access points, routers, Cisco IOS Software, and other components are from Cisco), customers have one point of contact to receive speedy implementation and problem resolution. Problems are quickly resolved by Cisco; customers do not have to first determine whether the problem is with the data vendor or with the telephony vendor. Further, as new features are developed—especially those that are based on primary functions of the Cisco infrastructure such as Cisco Discovery Protocol—Cisco customers can be confident that they will be among the first to deploy them—and they will do so with confidence of complete compatibility between the telephony and the infrastructure elements.

Ultimately, the many years of experience Cisco has with unified communications and IP networks means that customers can be confident that they have the strongest ally in their efforts to implement a successful, secure, and powerful unified communications solution.

For more information, visit <http://www.cisco.com/go/voice>, <http://www.cisco.com/go/unified>, <http://www.cisco.com/go/switching>, <http://www.cisco.com/go/routing>, <http://www.cisco.com/go/wireless> or contact your local Cisco representative or partner.



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland •
Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

