WHITE PAPER

BENEFITS OF CISCO IP COMMUNICATIONS IN A CISCO INTELLIGENT NETWORK

Adoption of IP Communications accelerated in 2004 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*, grew to US$3.5 billion in 2004—an 85-percent increase over the 2003 figure. Sales are projected to top US$10 billion in 2008. Cisco Systems® alone is displacing 10,800 traditional phones every business day, and more than 28,000 Cisco® customers use an all-IP solution—the largest number of IP Communications installations in the industry.

The significant design advantages, flexibility, and real-world successes of all-IP deployments have given this option an edge over the hybrid approach in the market. In a hybrid design, IP telephony is essentially bolted onto a core time-division multiplexing (TDM) architecture; therefore, only the IP-enabled endpoints have access to the rich capabilities of IP Communications. Also, because the TDM endpoints still exist on a separate network, companies do not realize the benefits of single management, and they may also lose the benefits of convergence that allows video and other IP-based applications to be easily added to the network and enables easy conferencing with voice, video, Web, and presence services.

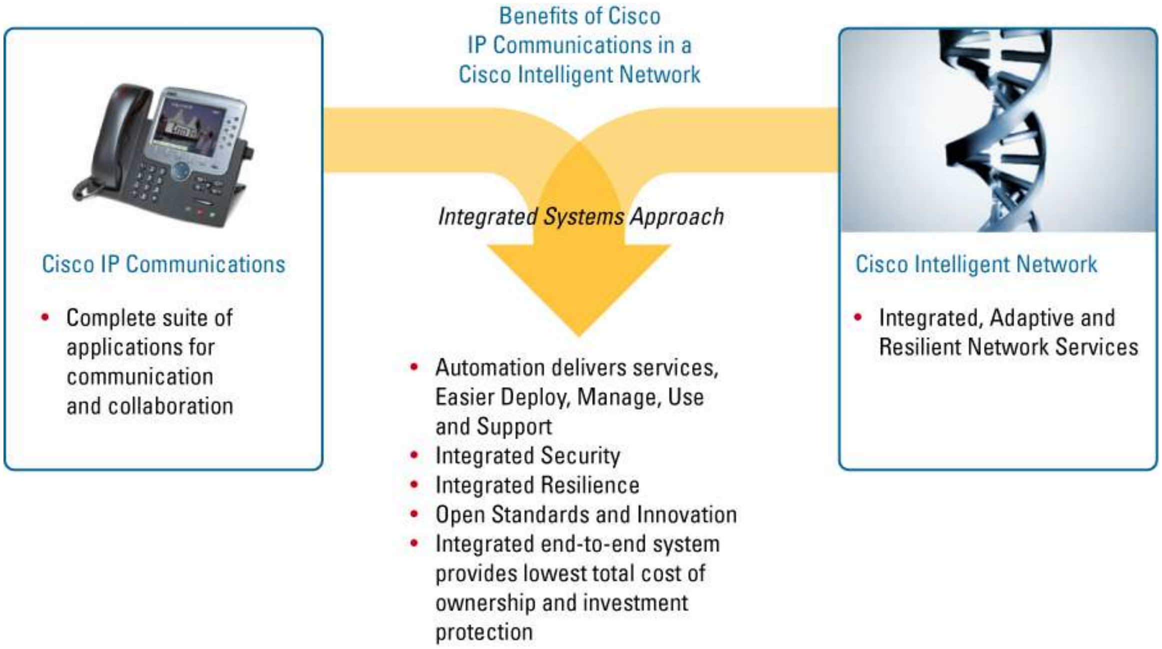
A CONVERGED, INTELLIGENT NETWORK

Organizations that choose the all-IP option face another choice: whether to run IP Communications applications from one vendor on a different vendor's infrastructure, or choose IP Communications applications from the same vendor that built the infrastructure.

Cisco began developing IP telephony applications in 1997 and has provided IP Communications applications longer than any other vendor. From the start, Cisco's focus has been on the most efficient ways to create a modular, resilient, adaptive, and secure converged infrastructure as well as integrated applications for data, voice, and video. Cisco employs a *systems approach* that uses intelligence in the network to deliver cost advantages, productivity gains, industry-leading security, and a higher return on investment. A higher level of integration advantage is realized when Cisco IP Communications runs in a Cisco network.

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

Figure 1. The Benefits of Cisco IP Communications in a Cisco Intelligent Network


Benefits of Cisco IP Communications in a Cisco Intelligent Network
Cisco IP Communications
• Complete suite of applications for communication and collaboration
Integrated Systems Approach
• Automation delivers services, Easier Deploy, Manage, Use and Support
• Integrated Security
• Integrated Resilience
• Open Standards and Innovation
• Integrated end-to-end system provides lowest total cost of ownership and investment protection
Cisco Intelligent Network
• Integrated, Adaptive and Resilient Network Services

This paper highlights the features that customers gain when deploying Cisco IP Communications in an intelligent Cisco IP network. It also demonstrates the unique value that this systems approach delivers.

THE ADVANTAGE OF CISCO IP COMMUNICATIONS IN A CISCO INTELLIGENT NETWORK

When customers run Cisco IP Communications applications in a Cisco infrastructure, they gain the powerful advantage of an intelligent network that is *application-aware*. This means that the network actively participates 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 purpose-built Cisco IP 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), or a video-enabled PC automatically retrieving the newest software versions and upgrading itself.

When the network and applications communicate in this way, customers can more quickly deploy communications. Fewer business disruptions occur on the Cisco Intelligent Network because the network automatically recognizes malfunctions and takes steps to heal itself. This also simplifies management and reduces management costs.

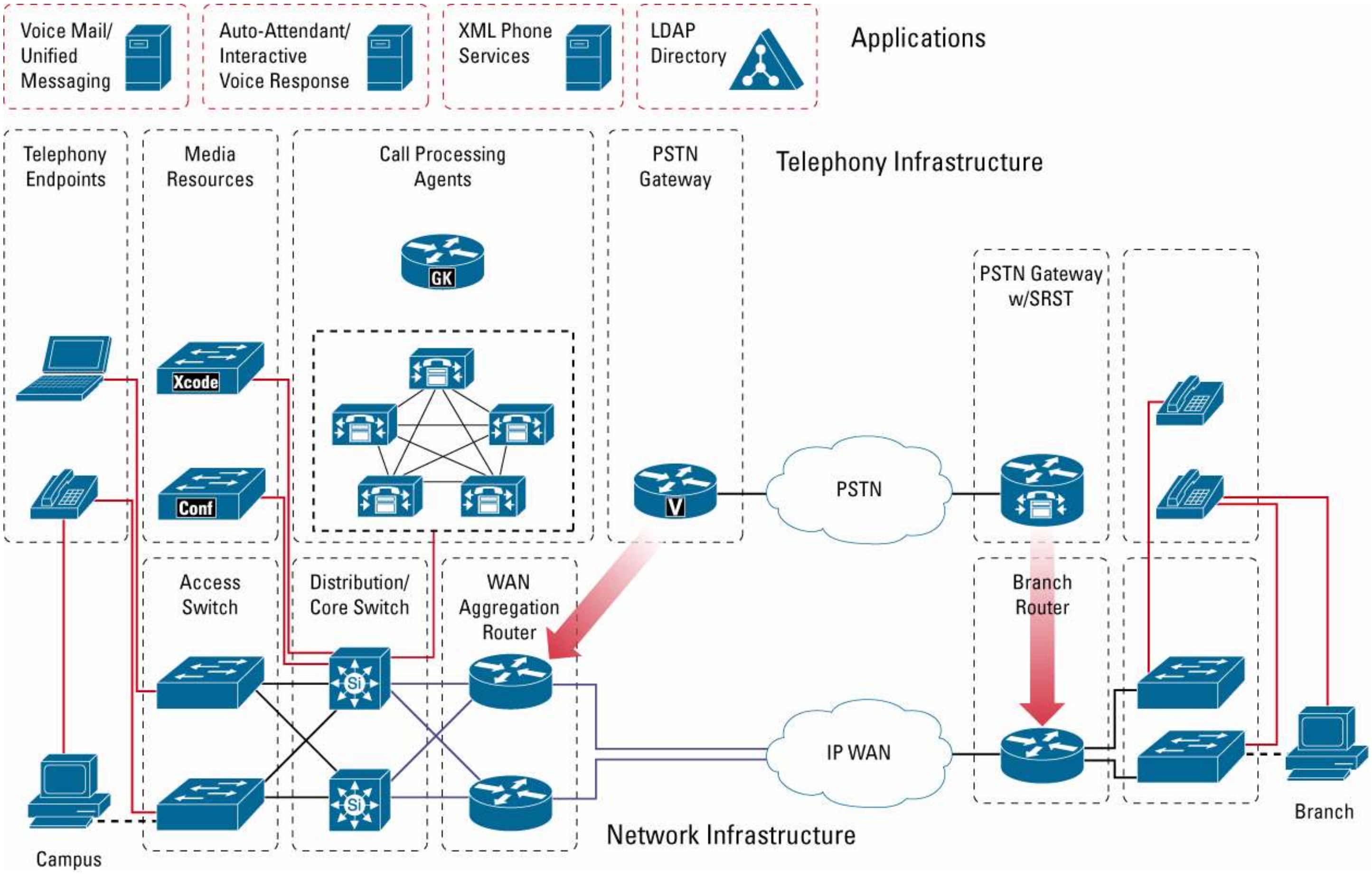
For example, Cisco network and application intelligence helps enable the simplicity and speed with which Cisco customers can make IP phone moves, adds, and changes. To move phones, users simply unplug their IP phones from one area of a building, move to another building, and plug them into a new Ethernet port. The phone automatically registers to the nearest Cisco CallManager or Cisco CallManager Express instance, the software-based, call-processing component at the heart of Cisco IP Communications. Operational attributes such as QoS are then automatically configured for the phone. Because the network is active and operates based on policies, fewer errors occur—helping ensure greater business continuity.

Network intelligence also allows addition of video to IP phones and other IP-enabled endpoints through a software upgrade, and for integration of video into existing voice and Web meeting workflows. Management is simplified because it is handled automatically in the network.

Network intelligence also encompasses integrated security. 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.

Unlike competing networks, a Cisco Intelligent Network is fully converged so that functions previously located in separate devices now move into the network fabric itself. For example, when a vendor other than Cisco deploys its IP telephony applications to hundreds of branch offices running a Cisco networking infrastructure, separate boxes must be placed in each office beside the Cisco router or switch to provide transcoding and voice gateway functions. 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 public switched telephone network (PSTN). In a Cisco converged network, this function is contained in modules that are inserted into the routers themselves (Figure 3).

Figure 2. Integrated IP Communications Infrastructure



In a converged Cisco intelligent network, PSTN gateway functions are merged into existing Cisco routers as network modules, eliminating the need for separate platforms. New features and functions can be added through software and module upgrades distributed across the network.

New features and functions can be added easily to this unified and integrated fabric through software upgrades, protecting each customer's investment in the Cisco IP Communications infrastructure. For example, customers who deployed Cisco IP phones initially only to run voice were later able to easily add video to their communication through software upgrades distributed across the network. Customers also can distribute new digital certificates throughout the Cisco IP Communications infrastructure to provide superior authentication and encryption functions.

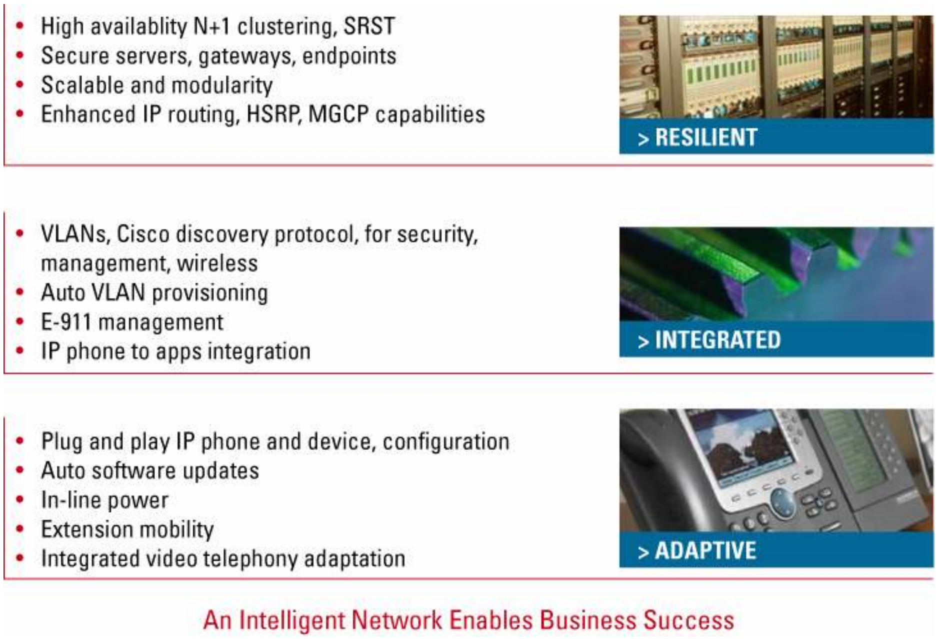
New features added to Cisco IP Communications applications, whether to Cisco Unity® Unified Messaging, to Cisco CallManager, or to Cisco Contact Center solutions, have undergone exhaustive preintegration testing on the Cisco infrastructure before release. If problems arise, Cisco takes full responsibility to resolve the issue and has specific escalation models in place to help ensure that customer problems achieve resolution quickly.

In a study done by Sage Research that examined the cost of ownership of 226 organizations whose networks used multiple vendors versus those that have standardized on a primary vendor, problem resolution was significantly faster on a primary-vendor network. The study found that "almost three-quarters of primary-vendor organizations report that their typical time to resolution of trouble tickets is less than 4 hours, compared with just over half of the multivendor organizations that report this level of rapid response."

The Sage study also found that, when companies choose a primary network vendor strategy for adding IP Communications using a systems approach, they achieve a 47-percent savings in both network and telephony costs.

Cisco IP Communications in a Cisco Intelligent Network delivers significantly higher levels of automation to streamline the automation deployment, management, and ease of using communications services. These benefits extend to all applications working together as a system to provide improved resilience, security, and higher quality of service.

Figure 3. IP Communications Intelligent Infrastructure



- High availablity N+1 clustering, SRST
- Secure servers, gateways, endpoints
- Scalable and modularity
- Enhanced IP routing, HSRP, MGCP capabilities

- VLANs, Cisco discovery protocol, for security, management, wireless
- Auto VLAN provisioning
- E-911 management
- IP phone to apps integration

- Plug and play IP phone and device, configuration
- Auto software updates
- In-line power
- Extension mobility
- Integrated video telephony adaptation

An Intelligent Network Enables Business Success

UNRIVALED SCALABILITY

The single-vendor approach also offers customers the ability to inexpensively scale their IP Communications solutions to almost any size—without a complete equipment upgrade. With the hybrid approach customers may be required to replace old private-branch-exchange (PBX) platforms with newer platforms. The only significant cost with the Cisco solution running in a converged Cisco network infrastructure is to add an instance of Cisco CallManager to the central site. Any other vendor would need to provide a comparable central solution, but none offers the option for a zero-cost migration for redundant call processing in the branch offices.

HOW CISCO DOES IT

A Closer Look at the Benefits of the Cisco Solution

This section examines the significant business and technical benefits customers enjoy from a Cisco Intelligent Network and how those capabilities are uniquely delivered across Cisco IP Communications applications on a Cisco infrastructure. These benefits include:

- Faster moves, adds, and changes
- Faster deployment of QoS settings
- Cisco Smartport Macros: The fastest way to configure all phone settings
- Reduced costs and dispatching errors with automatic Enhanced 911 (E911)
- Video as a simple addition
- Secure IP Communications everywhere—from the endpoints to the network infrastructure
- Built-in resiliency
- Power over Ethernet (PoE) and intelligent power management to reduce power costs
- Single-platform, router-integrated call processing for small businesses and enterprise branches
- Faster time-to-voice problem resolution with CiscoWorks IP Telephony Environment Monitor (ITEM)
- Complementary and value-add IP Communications applications from more than 300 Cisco partners
- Integrated services and support

Faster 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 IP integration. This ease of moves, adds, and changes is the direct result of two important capabilities that are built into the Cisco data infrastructure: Cisco Discovery Protocol and Cisco AutoQoS.

A network management staple of Cisco data infrastructures for many years, Cisco Discovery Protocol operates in the background and facilitates communication between a Cisco IP phone plugged into a network and the network switch. Because it operates automatically, IT managers do not have to physically visit switches to set the proper voice parameters. This is available only when a Cisco IP phone operates on a Cisco infrastructure.

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 port switches. As IP telephony networks scale, administrative costs increase exponentially.

Cisco Discovery Protocol automation translates into significant IT cost savings at large companies where 25 percent of their personnel move each year (a common industry standard for moves, adds, and changes). The Yankee Group estimates that it costs companies up to US$150 per move, add, or change—an expense that can be eliminated with a Cisco IP Communications solution.

The IEEE has developed a new standard called Link Layer Discovery Protocol (LLDP), derived directly from the Cisco Discovery Protocol. Not yet widely deployed, LLDP provides some of the capabilities offered by Cisco Discovery Protocol. Cisco switches can implement LLDP in a fully compliant manner. In addition, through the LLDP encoding mechanism called Type Length Value (TLV), all the features of both Cisco Discovery Protocol and standard LLDP are available to Cisco customers. This allows customers to support the new standard on their existing Cisco Discovery Protocol-based network without requiring modifications to the infrastructure.

How It Works

Cisco has enhanced Cisco Discovery Protocol for IP telephony by adding new fields that help an IP phone automatically retrieve the information it needs to operate from the local switch. These fields include the voice VLAN ID, which is an identification number that tells phones when they are plugged into switch ports the correct voice VLAN they should join.** Based on the PoE standard, Cisco Discovery Protocol also automatically assigns the proper power requirements depending on the needs of the Cisco IP phone (refer to the section “Power over Ethernet and Intelligent Power Management Reduce Power Costs” for more information).

After a user connects an IP phone to the network, the phone initiates a Cisco Discovery Protocol exchange with the access switch. When the phone is recognized, the access switch indicates to the phone the voice VLAN it should use and also indicates the class-of-service (CoS) value it should apply to the traffic. 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. If a phone is disconnected, the infrastructure removes access into the voice VLAN for that port, thus preventing unauthorized access from other devices that could connect to the vacated port.

What is unique in this interaction is that Cisco Discovery Protocol operates automatically in response to a device being plugged into or removed from a jack—because this protocol is an integral part of the Cisco infrastructure.

On other vendors’ telephony systems that lack the integration with Cisco Discovery Protocol, each time users move their phones, Ethernet jacks become potential points of increased security vulnerability. IT personnel must manually reconfigure those jacks or they remain security holes because a hacker could plug a PC into a voice port and use its existing QoS allocated to that port. The PC could then generate large amounts of traffic, quickly congesting the LAN and disrupting voice and video services to the other IP phones. The urgency to track these security holes and the time required to be vigilant in closing them add to the administrative costs of competing IP telephony systems on Cisco infrastructures.

When Cisco Discovery Protocol is used in concert with other security tools such as *dynamic Address Resolution Protocol* (ARP) inspection and *gratuitous ARP denial*, Cisco Discovery Protocol also can help protect against *voice over misconfigured IP telephony*, an eavesdropping technique where a hacker uses packet sniffing to capture and reassemble voice streams.

Faster Deployment of QoS Settings

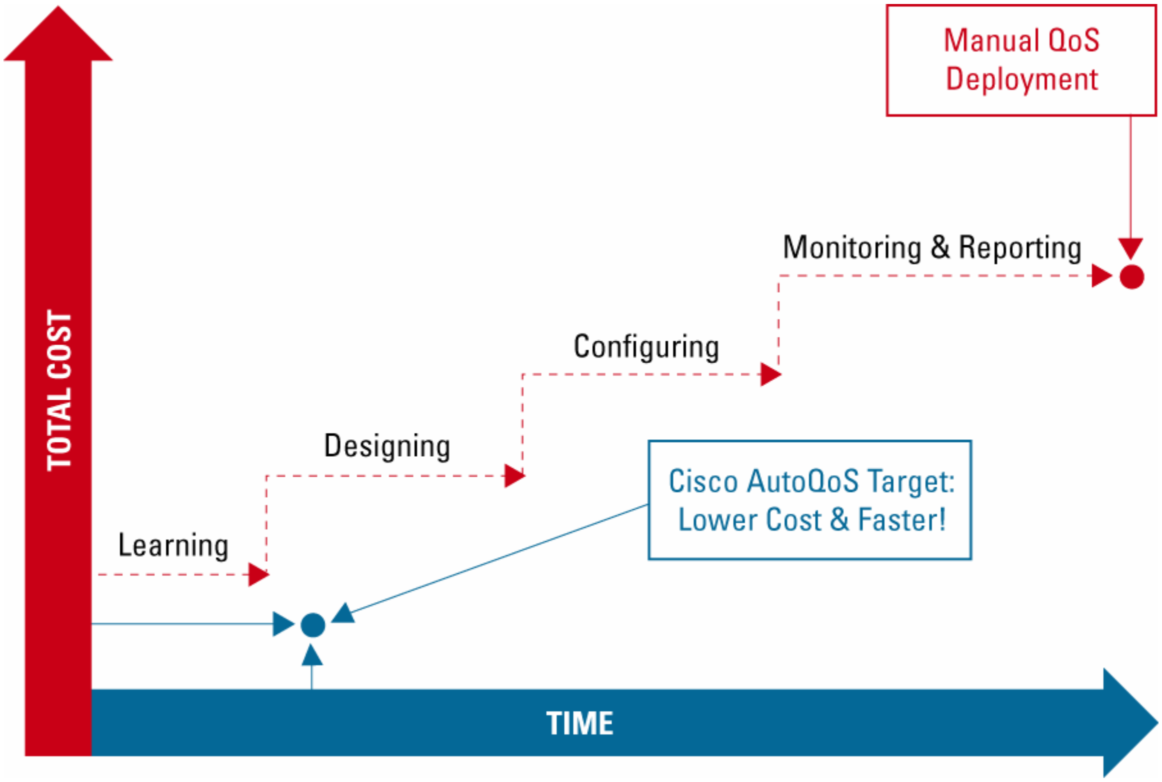
Among the most important capabilities a network infrastructure must provide to its voice-enabled endpoints are the correct QoS settings. This challenge becomes magnified when QoS must be delivered to hundreds or thousands of IP phones. QoS is the essential ability of the network, through the switches and routers and in concert with phones and video endpoints, to protect delay-sensitive traffic so voice and video quality is assured regardless of network congestion.

Cisco developed AutoQoS in response to Cisco customer demand for a faster way to deploy QoS settings. This powerful feature of Cisco IOS® Software helps companies quickly and automatically configure hundreds of switches and routers with the proper QoS settings with just a few commands. Cisco AutoQoS 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 (Figure 5).

In network environments that lack Cisco AutoQoS, applying QoS involves many repetitive steps that must be applied individually to each switch in the network.

** 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.

Figure 4. AutoQoS Reduces Time and Costs over Manual QoS Deployment



Automating QoS distribution is critical to reducing the cost and time to deploy QoS as large numbers of IP phones are added to the network.

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 without affecting other network 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.

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.

Cisco Smartports Macros: The Fastest Way to Configure All Phone Settings

The results from the development of Cisco AutoQoS were so successful that Cisco further extended this technology to deliver Cisco Smartport Macros. Whereas AutoQoS is designed only to rapidly deploy QoS settings, Cisco Smartport Marcros includes a suite of voice-critical macros and templates that can be applied to ports to make configuration much simpler. These macros are based on Cisco best practices and experience with running IP Communications in the network.

Cisco Smartport Macros do not function in third-party or multivendor network environments, translating into loss of a powerful cost- and time-saving tool.

How It Works

With a standard or customized Cisco Smartport Macro, an organization 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, DHCP Snooping, and Spanning Tree PortFast. Instead, the company can automatically upload a single template to a switch that includes all the proper settings.

For organizations that run Cisco IP Communications in a Cisco infrastructure, this capability can be further automated with Cisco Discovery Protocol. Because this protocol operates in the background, talking to each switch, noting devices attached to each switch port, and building a topology map, it can be instructed to detect which devices are connected to a switch such as IP phones, PCs, a Cisco Aironet® access point, a PC made video-ready with Cisco VT Advantage, or another switch or router. Cisco Discovery Protocol also can apply the appropriate Cisco Smartport Macro. For example, if it detects a 30-port switch with IP phones attached to all the ports, it automatically configures those switch ports with the customized Cisco Smartport Macro that optimizes voice and video traffic.

Automatic E911 Cuts Costs and Reduces Dispatching Errors

Administrative costs are also lowered (and worker safety enhanced) with another unique feature of the Cisco IP 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 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 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 IP Telephony runs 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.

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 converged IP Communications solution, enabling video is as easy as adding any other application to the network. Cisco VT Advantage is a video telephony solution comprising the Cisco VT 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 IP phone, users can place and receive video calls on their enterprise IP telephony network. Users make calls from their Cisco 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 VT Advantage, video is integrated into the Cisco infrastructure much like voice and uses the same network intelligence already operating for voice.

The advantage of deploying video in a Cisco converged network is that not only is the network *application-aware*, but the applications are also *network-aware*. This helps enable video to be tightly woven 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 VT Advantage client. If users have Cisco VT 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 IP phone. In addition, the application itself has intelligence and seeks out network services automatically. Cisco VT 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 personal digital assistant (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 CallManager to these systems, and they can be enabled to automatically register to Cisco CallManager. Thereafter they can be controlled by Cisco CallManager.

Dial plans for both video and voice are also integrated in a Cisco IP 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 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.

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 opens up 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 IP 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 IP Communications:

- Secure connectivity—To help ensure that communications over both the WAN and LAN 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. 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.
- Threat defense—Many techniques protect against aggressive threats. Firewalls, either integrated or standalone, and intrusion detection systems protect the infrastructure and the voice VLANs. 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 ARP inspection protection and other tools on the LAN switches and Cisco IP phones to protect the endpoints against common Layer 2 exploits such as man-in-the-middle attacks. And the Cisco IP Communications applications themselves offer security features. For example, Cisco CallManager offers the ability to support multiple levels of administration access and advanced protection against toll fraud.

For more information about IP Communications and security, visit http://www.cisco.com/go/ipcsecurity.

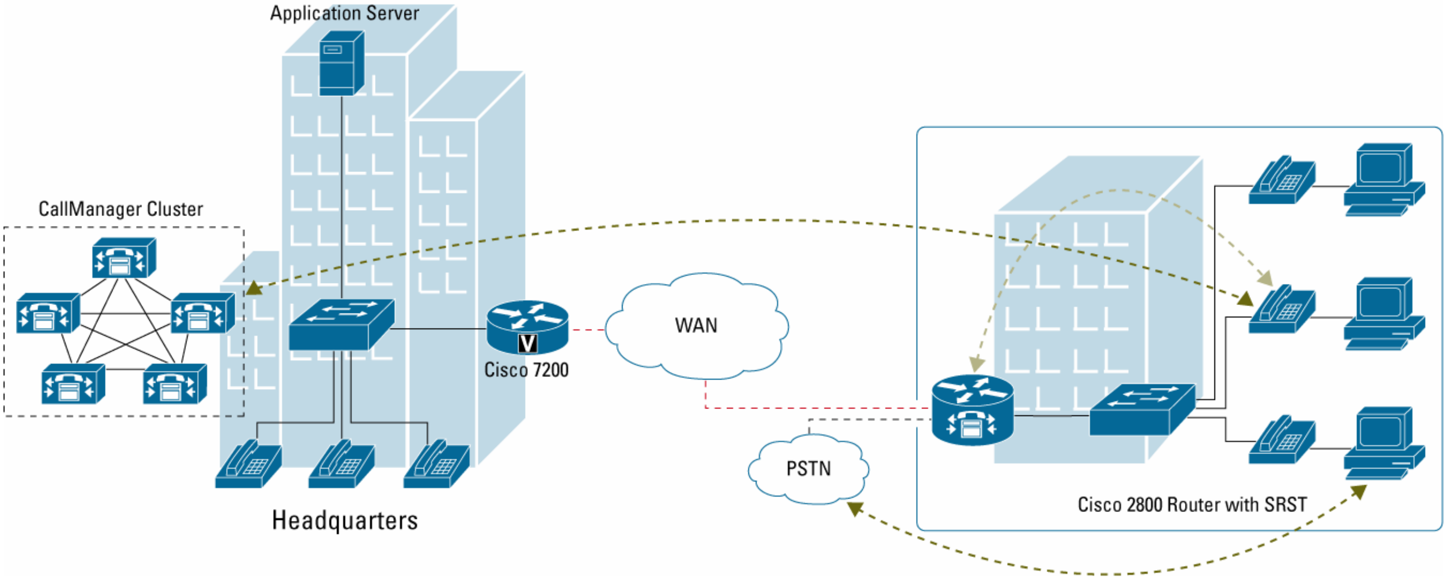
Built-In Resiliency Extends to Remote Sites

Cisco designed its IP Communications system from the beginning for packet networks. Cisco CallManager, Cisco IP phones, Cisco Unity voicemail and unified messaging servers, and Cisco Customer Contact and self-service solutions are all liberated from specific physical locations. Customers can design their networks by placing Cisco CallManager and other Cisco call-control servers in clusters and deploying them in multiple locations anywhere in the network. When Cisco 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 resilience 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 Survivable Remote Site Telephony (SRST), 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 SRST router facilitates automatic failover so that local calls and active calls from Cisco IP phones to the PSTN are maintained even if a WAN failure occurs. If the WAN link to a remote office fails and connection to the Cisco CallManager for the domain is lost, the phones in that branch office automatically redirect to the Cisco SRST router. The Cisco SRST 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 CallManager—again, no manual intervention is required. Cisco SRST is accomplished through this integrated system with no additional hardware components (Figure 6).

Figure 5. Cisco SRST—Voice Redundancy if WAN Failure Occurs

- Resiliency for remote IP Telephony users with central CallManager
- Minimizes business impact of WAN link failure:
  - Cisco router auto-configures, provides local call processing—no manual intervention required
  - SRST IP phone calls remain secure
  - When WAN is available, IP Phones auto-revert back to CallManager



Power over Ethernet and Intelligent Power Management Reduce Power Costs

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 PoE, and now an 802.3af standard) that enabled the LAN switching infrastructure to provide power over an Ethernet cable to a powered device.

Cisco now offers Cisco IP phones and LAN switches that support both the 802.3af standard and Cisco prestandard PoE (inline power) for additional flexibility. Cisco provides additional levels of power control with intelligent power management. Like other unique features available with Cisco IP Communications in a Cisco infrastructure, Cisco PoE provides customers with significant power-consumption savings to powered devices 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 power detection and management technology allows users to provision power based on the power the device actually needs. The Cisco Intelligent Power Management feature can provide customers substantial savings in electrical costs and backup UPS and battery power systems. By providing a more precise allocation of power to devices, a total Cisco IP Communications solution also optimizes port density, reducing the need for additional deployment of switches and power supplies.

Single-Platform, Router-Integrated Call Processing for Small Businesses and Enterprise Branches

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 CallManager Express and 720 users with Cisco SRST.

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 issues.

Features of Cisco Integrated Services Routers

- Embedded full-featured call processing in Cisco IOS Software with Cisco CallManager Express or failover capability with Cisco SRST
- 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 voice-over-IP (VoIP) processing and both transcoding and multiparty conferencing
- Integrated voice WAN interface cards (VWICs) for both voice and data connectivity needs
- 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

Faster Time to Voice Problem Resolution with CiscoWorks IP Telephony Environment Monitor

Malfunctions in any components of the voice-processing infrastructure, in the LAN or WAN connections, or in the infrastructure itself can impact voice or video quality. Tracking problems and achieving resolution is greatly expedited on a Cisco IP Communications in a Cisco infrastructure 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.

CiscoWorks ITEM is a suite of applications that operates in real time to continuously evaluate and report the operational health of a Cisco IP Communications implementation. This information is displayed in a Web-based screen that provides real-time status and alerting of actual and suspected problems in the voice-processing infrastructure.

But what if changes are made somewhere else in the network infrastructure and this impacts voice quality? What if a new application is added to the data center and, because of business reasons, is given a high-priority QoS, eroding the bandwidth allocated to voice traffic and disrupting voice quality?

CiscoWorks ITEM has automated testing that can detect higher latency and jitter that may result from QoS configuration changes and alert operators to this situation. If the problem is being caused elsewhere on the data network, however, the voice team must coordinate with the data side to find the problem.

Today, the network operations team monitors the network infrastructure with the CiscoWorks LAN Management Solution (LMS). 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.

More Than 300 Cisco Partners Delivering Innovative, Advanced IP Communications Applications

Organizations worldwide are developing innovative, profit-generating IP Communications applications—and many of these applications are being developed for Cisco CallManager and Cisco CallManager Express to be displayed on Cisco IP phones.

Cisco IP Communications has a distinct advantage in the IP telephony applications space over competing systems because of the robustness of the Cisco Technology Developer ecosystem. Because Cisco has the largest installed base of IP phones of any competitor and holds the largest share of the market, more than 300 Cisco Technology Developer partners are actively developing applications. This is due also, in part, to the long-term Cisco commitment to maintaining Extensible Markup Language (XML) as an open standard and the company's development of an open interface. Besides XML, Cisco IP Communications applications are also based on other industry standards such as the Telephony Application Programming Interface (TAPI) and Java TAPI (JTAPI). Cisco also has created a wealth of resources such as programming guides, FAQ libraries, discussion forums, software development kits, and a robust developer support program. All these resources have made it easier for IP Communications applications developers to build applications for Cisco CallManager and Cisco CallManager Express, which provide customers with many more off-the-shelf applications than are available with any other competitor.

Many applications have been developed for use in education, retail, hospitality, and government. Examples include administrative and attendance solutions for school districts and universities; inventory tracking and lookups for retail branches; concierge, restaurant listings and reservations, and other guest-service applications for hotels; emergency notification and audio streaming systems for government and public-safety personnel; and time-clock applications for use on manufacturing floors and in hospitals, bank branch offices, and other work environments.

In addition, because the Cisco intelligent infrastructure extends out to the IP phones, deploying new applications and services to the phone sets is as easy as distributing software and automating installation on a remote PC. Upgrading business applications, enhancing telephony services, and extending phone-based transactions can be accomplished smoothly and rapidly.

Learn more about the Cisco Technology Developer program and the applications these partners are offering at:
http://www.cisco.com/en/US/partners/pr46/tdp/index.shtml

Cisco and Partners Delivering a Networked Systems Approach

From its beginnings, when Cisco introduced the first multiprotocol router to the market in the early 1980s, Cisco has been the leader in IP networking innovation. As Cisco technology has become the foundation of most enterprise networks and the Internet itself, Cisco has continued to build on its vision: an all-IP network that unifies communications through the integration of data, voice, and video.

This experience and early commitment to IP voice and video is unparalleled in the industry. Whereas traditional vendors first entered the IP telephony market only in 2000, Cisco entered the market in 1997 and since then has led innovations in the IP telephony industry, including:

- First to put XML applications on the phone
- First to provide inline PoE
- First to provide SRST
- First to provide integrated call-processing capability directly into the router
- First to provide automated E911 administration for IP telephony
- First to provide AutoQoS

- First to provide clustering for scalability and geographic redundancy
- First to provide voice and data VLANs
- First to provide integrated video telephony services at the desktop with Cisco VT Advantage
- First to scale IP telephony to large enterprise implementations
- First to offer integrated intrusion prevention solution with Cisco Security Agent
- First to offer a scalable, standards-based encryption solution for both media and signaling protection
- First to provide digital certificates for authentication and key management
- First to provide private secure voice messaging using standards-based public key encryption
- First to provide integrated wireless, security, IP Communications, routing, switching, content, firewall, and VPN services solution at wire speed, with integrated services routers
- First all-IP telephony solution to pass Department of Defense (DoD) JITC PBX1 security and interoperability testing for use in command and control environments
- First to provide Gigabit Ethernet through an IP phone

But what distinguishes Cisco today is not only its early commitment to this technology, but also the fact that Cisco IP networking was designed from the start with a systems approach. Over the years, Cisco has designed an awareness of data, voice, and video media types into every component and layer of the Cisco infrastructure. The intelligent infrastructure constantly looks at all modes of communications, including e-mail, telephony, voicemail, videoconferencing, and many others, and recognizes their unique requirements and interdependencies. The infrastructure then adjusts to meet the specific needs of the organization. This systems approach helps ensure that Cisco delivers the most competitive and secure IP Communications solution to customers.

Benefits of Integrated Services and Support

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

A study conducted by Sage Research (commissioned by Cisco) that included in-depth interviews with customers found that 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. 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."

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 IP Communications solution on a Cisco Intelligent Network follow:

- 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
- Attractive financing and leasing options from Cisco Systems Capital® Corporation

- Cisco in-depth training, certification, and expertise delivered by Cisco and worldwide partners
- End-to-end, 24 x 7 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, IP 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, 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 both IP Communications and the IP networks means that customers can be confident that they have the strongest ally in their efforts to implement a successful, secure, and powerful IP Communications solution.

For more information, visit www.cisco.com/go/ipc 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

205330.BF_ETMG_JQ_8.05

Printed in the USA