



WHITE PAPER

THE TOP MYTHS OF IP COMMUNICATIONS

As voice, video, and data networks have begun to converge, more organizations are seeing the value in deploying IP business communications solutions, including IP telephony, unified messaging, voice mail, customer contact solutions, and audio, video, and Web conferencing.

Questions about these technologies have arisen, as well as some common myths. Here, we'll share the facts surrounding these myths and provide information that can help you make an intelligent decision about deploying a converged network and IP Communications solutions.

THE MYTHS:

1. Customers should wait to deploy IP-based business communications until the standards are more mature.
2. An IP-based business communications implementation is more expensive than implementing a traditional time-division multiplexing (TDM) communications system.
3. There is no single compelling application ("killer application") for IP-based business communications today.
4. IP-based business communications systems are less secure than hybrid systems with a mix of IP-based and traditional communications.
5. Deploying IP-based business communications means throwing away your investment in traditional voice solutions.

MYTH #1

Customers should wait to deploy IP-based business communications until the standards are more mature.

The perception here is that standards processes for telecommunications and data networking is a complex and mysterious art, steeped in decades of tradition and secret voting. As a result, many people are concerned that because of the relative newness of IP Communications, the current standards for these solutions are not mature enough to justify investing in the technology. The fear is that if you invest in an IP Communications solution now, by next year, everything will change, and your investment will have been worthless.

THE REALITY

Fundamental standards for IP-based communications are already in place; new standards will continue to emerge.

In the world of technology, it can often take far less than a year for a standard to become obsolete. In the case of IP Communications, most of the standards that are critical to the success of the solution have been around for some time. In fact, many people are surprised by the number of standards it takes to place an IP phone call today.

Let's start with the newest standard—inline power over Ethernet. 802.3af was finalized by the Institute of Electrical and Electronics Engineers (IEEE) in early 2003, and Cisco Systems® was one of the first vendors to support the new standard with the new color Cisco® IP Phone 7970G.

When the phone boots up, it uses Dynamic Host Configuration Protocol (DHCP) to obtain its IP address from the appropriate server, just like a PC does. The phone then downloads its operating system using Trivial File Transfer Protocol (TFTP)—again, just like many other network devices. Then, it sets up an 802.3p virtual local-area network (VLAN) to segregate the voice traffic from the data traffic for optimum quality of service (QoS) and security.

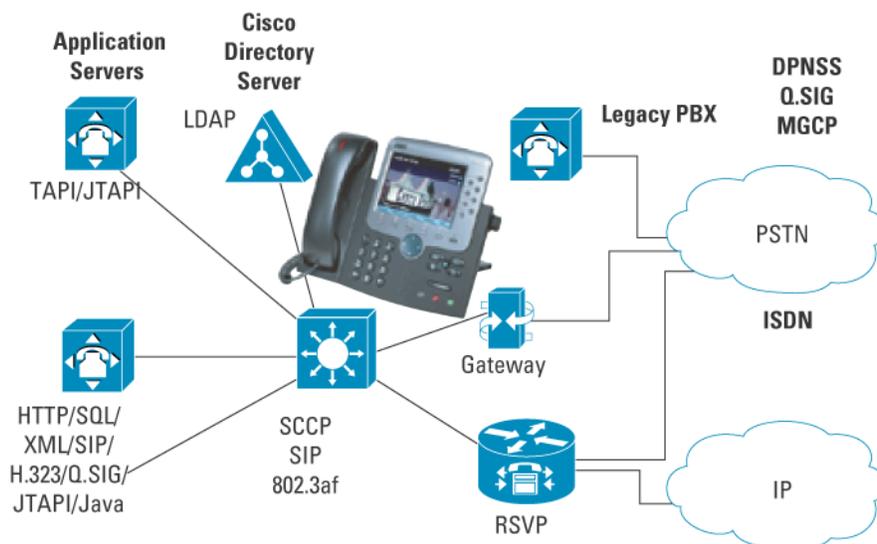
Cisco intelligent switches and Cisco CallManager Version 4.0 also support a new identity-based standard called 802.1x authentication, so that endpoints within the network are first authenticated, preventing “rogue” endpoints and rogue software loads on endpoints. With Transport Layer Security (TLS) Secure Sockets Layer (SSL) and Secure Real Time Protocol (SRTP), the signaling of communications call setup, and processing to and from Cisco CallManager and other endpoints, is protected and secure. Cisco has also implemented Advanced Encryption Standard (AES) for the Cisco IP Phone 7970G, so that secure voice encryption is provided where needed on a call-by-call basis, or for specific endpoints.

The next standard comes into operation when the user takes the phone off the hook, causing the phone to send a message to the Cisco CallManager call processing software using Cisco Skinny Call Control Protocol (SCCP). SCCP isn’t a standard, but Cisco IP phones also support the newer Session Initiation Protocol (SIP); in fact, Cisco has sold more SIP endpoints than any other vendor.

The Cisco IP Phone talks to Cisco CallManager via SCCP, and in the future will also communicate via SIP. Gateway devices talk to Cisco CallManager using H.323 or Media Gateway Control Protocol (MGCP). In the Cisco solution, all gateways and endpoints are controlled by Cisco CallManager, saving additional time and management costs.

Cisco CallManager also provides support for several open packet telephony standards that enable customers, partners, and developers to easily extend the features and capabilities of their communications environments. For example, Lightweight Directory Access Protocol (LDAP) is used to perform directory lookups and place calls. Most applications are supported using a combination of inherent IP phone services, Extensible Markup Language (XML), Telephony Application Programming Interface (TAPI), and Java TAPI (JTAPI) standards (Figure 1).

Figure 1



As you can see, most of the standards used to make an IP phone call are not new. As new protocols become standards, they can be easily added to the total IP Communications system. The investment you make today will be protected for years to come.



Support for many different IP and voice protocols also enables Cisco IP Communications solutions to integrate tightly and flexibly into each customer's business communications environment to maximize investment in existing applications and processes. For example, LDAP directory support enables customers to use their Microsoft Active Directory and Outlook distribution lists to make phone calls and to send or receive voice messages.

Cisco has teamed with leading collaboration software vendors such as Microsoft and IBM to drive open standards that enable even tighter application integration for more productivity and for capabilities that don't exist in a TDM world. For example, Microsoft Customer Relationship Management (CRM) customers can now use Cisco CallManager Express and Cisco IP Contact Center (IPCC) Express solutions to generate screen pops and to natively dial contacts from within Microsoft applications.

MYTH #2

An IP-based business communications implementation is more expensive than implementing a traditional TDM communications system.

Today's IP phones seem more expensive when compared to traditional circuit-switched key system and enterprise phones. With IP phones, the intelligence resides in the physical set rather than in set-line cards within enterprise and key system controllers; this can give the appearance that the bulk of the solution cost is tied to the endpoints. The end customer sees only a higher phone cost for voice over IP (VoIP), rather than the comparison cost based on averaging the line card and the phone costs for the enterprise. As a result, price sensitivity becomes a significant barrier to IP telephony adoption. The small and midsize business markets, with their even greater price sensitivity, would be expected to adopt IP telephony at a much slower rate unless a suitable system was offered to this market at a compelling price.

THE REALITY

IP Communications solutions are proven to offer lower TCO and high ROI.

The typical IP phone today costs the same or less than an equivalent digital desk phone set. When you factor in the lower overall total cost of ownership (TCO) that results from an IP Communications solution running on a converged IP network for voice, video, and data, an IP Communications solution can save organizations a substantial amount of money.

For example, Cisco customer SouthTrust Bank in Birmingham, Alabama was able to replace 750 traditional PBX and key systems with a single, centralized Cisco CallManager implementation for their branch offices throughout the Southeast. This resulted in more than US\$5 million in savings in the first year alone, including savings of 20 percent in local and Frame Relay circuits; 51.3 percent in moves, adds, and changes; 93.9 percent in conference call charges; and 38.4 percent in long-distance costs. In addition, SouthTrust Bank expects that it will reduce overall voice and data systems maintenance costs by about 15.4 percent annually. The bank was also able to benefit from automatic disaster recovery by deploying a backup Cisco CallManager cluster in its disaster recovery location.

While "offsite" at the Superbowl, NFL Films uses a converged network and a Cisco IP Communications solution that includes Cisco CallManager and Cisco Unity™ unified messaging software. This gives the company the same access to communications capabilities as are available at the headquarters facility in New Jersey—at a fraction of the cost and time traditionally spent setting up temporary communications in the field. NFL Films estimates saving approximately \$400,000 as a result of installing a Cisco IP Communications solution instead of a traditional PBX with similar user features, largely due to the decreased need for cable, installation labor, and back-end equipment. And long-distance telephone bills have been reduced by approximately 60 percent since IP telephony was fully implemented.

The ability to increase employee productivity was another benefit of the solution. Like many organizations today, NFL Films personnel are inundated with communications channels—telephone, fax, voice mail, e-mail, pocket pagers, mobile phones, and PDAs. While the explosion of communications choices has enhanced worker capabilities, keeping track of incoming calls and messages can be overwhelming—and extremely time-consuming. Cisco Unity unified messaging helps workers by bringing all contact channels together into a single inbox. Workers can listen to their e-mail messages over the phone and check voice messages from the Internet.

“I think a lot of our people don’t even remember their voice-mail password anymore because they now get their voice mail through e-mail,” says Steve Eager, director of network systems administration at NFL Films. “We estimate that Cisco Unity is saving our workers roughly an hour a day by eliminating the steps previously required to access all their messages throughout the day.”

H.J. Heinz, Europe did not set out to use IP telephony. In fact, the company’s European Service Delivery team had not even considered using IP telephony for its global voice implementation prior to bidding out an expired contract. A provider responded with a Cisco technology-based IP telephony and managed LAN solution, which was the best match for H.J. Heinz. Heinz’s first IP telephony site was installed in January 2001; since then, the company has deployed full IP telephony installations at eight sites in Holland and five sites in the United Kingdom, with 7000 IP phones installed throughout Europe. Heinz’s decision to move to IP telephony helped to achieve its goals—provide uniformity of service to users throughout Europe, gain better control over voice costs, stop “cost leakage,” and gain pan-European network visibility. IP telephony enabled Heinz to make moves, adds, and changes 86 percent faster than a traditional PBX; decreased call hold time by 87 percent; gained a time savings of 10 percent for the nontechnology staff responsible for managing remote phone systems by centralizing phone management; and realized a 25 percent productivity improvement by effectively using IP telephony-enabled voice mail.

Cisco has more than 15,000 IP Communications customers today; more than 60 percent of Fortune 500 companies are using Cisco IP Communications solutions in their organizations. While some of these are “greenfield” sites (where the customer had a new building that needed connectivity), all of the companies had different challenges and scenarios that led them to select a converged network running an IP Communications solution. Some customers replaced a Centrex, PBX, or messaging platform that had reached the end of its useful life. Some customers needed to improve customer service or intracompany communications, which influenced the decision to have a more robust network solution that could streamline communications options and increase productivity. Some customers had a need for a compelling application that would transform the way they did business for a better competitive advantage. For all of them, however, it wasn’t simply about saving money on wire pulls—it was about driving ROI by getting more value for less money.

Examples of customers using Cisco IP Communications solutions are available at:

<http://www.cisco.com/go/ipc>

MYTH #3

There is no single compelling application (“killer application”) for IP-based communications today.

After all, if there were, wouldn’t everyone be using it? And should organizations wait until that application is discovered to make the investment in a converged voice, video, and data network running IP Communications solutions?

THE REALITY

There are many applications available today that cut costs, increase productivity, and improve customer satisfaction.

The true power of IP Communications lies in the convergence of voice, video, and data applications for the user. The architecture of IP Communications allows applications to be integrated with organizations' existing applications, from existing e-mail, CRM, and calendar systems to vertical applications such as inventory lookup, hotel wake-up calls, and school attendance. Just like there is no single reason for the adoption of the Internet, there is no single reason to adopt IP Communications. The most compelling application will vary by enterprise, and even more by user.

Applications like Cisco IP Contact Center, Cisco MeetingPlace conferencing, and Cisco Unity unified messaging integrate with organizations' existing e-mail, calendar, and CRM systems, allowing them to save time and money and to improve customer service.

Cisco IP phones have shifted customer acceptance from the existing, traditional key-based interface to a new, enhanced user interface that uses display-based access to features and provides value-added services, using XML capabilities. XML-based services on a Cisco IP phone can be customized to provide users with access to information such as stock quotes, employee extension numbers, or any Web-based content.

Cisco IP phone applications have been developed for use in information-laden vertical market industries, notably in education, retail, hospitality, and government (Figure 2). The many applications being deployed 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, in hospitals, in bank branch offices, and in other work environments with many hourly wage employees.

The enterprise applications that are readily available on desktop PCs, such as e-mail, unified messaging, corporate directories, conference room booking, and expense reporting, can also be provided on IP phones. In this way, the phone serves as an always-on communications and information vehicle for business-critical and time-sensitive communication with employees—anytime and anywhere. The simplification of menu-driven information access improves efficiency and expedites day-to-day business processes.

Figure 2



Examples of these XML applications are available at the Cisco IP Communications Applications Central Web portal, at:

www.cisco.com/go/apps

At this portal, you can see mini-demos of several applications, register for free trials of many of them, view and read case studies of customers using these applications in their environments, and find a development partner that can create an application best suited to the needs of your organization.

MYTH #4

IP-based communications systems are less secure than hybrid systems with a mix of IP-based and traditional communications.

For many people, there's just no arguing the fact that IP Communications solutions are less secure than hybrid systems. The sentiment seems to be, "When was the last time an Internet worm took down your PBX?"

THE REALITY

IP Communications solutions are secure and reliable.

Security is an important issue—whether or not you are running voice on your data network. But the real myth is that hybrid systems are more secure than end-to-end IP Communications solutions.

Everyone is familiar with how a traditional digital PBX is put together. With these systems, you have to protect against toll fraud, masquerading, and war dialing. And with traditional systems, unauthorized access or eavesdropping can often be accomplished with a simple pair of alligator clips; but, you probably don't have to worry about Internet worms. However, some people think that you don't need to worry about network security if you opt for one of the "hybrid" migration strategies being promoted by the traditional vendors.

Typically, the first step in the hybrid migration process is pulling the CPU and call processing out of the cabinet and putting it on a dedicated LAN. You must then make sure that LAN is completely secure, since an attack on the call processing component affects every user on the system—not just IP phone users.

In this scenario, not only do you have the same security considerations as if the entire solution was on the IP network, but you also have to manage two separate networks, without realizing the benefits of having an integrated solution on a single, converged network.

There's no denying that security is an important factor in deploying IP telephony, whether you are deploying a native IP solution or a hybrid solution. Cisco is the only vendor that addresses security at all levels of the IP Communications infrastructure—the IP network, the voice systems, and the applications, providing the "defense in depth" necessary to make your IP Communications systems as secure as they can be.

When protecting against the types of vulnerabilities common to voice and voice-related systems, it's important to focus on three critical components:

- **Privacy**—Via secure connectivity. Technologies such as IP Security (IPSec) and SSL virtual private networks (VPNs) help to ensure that communications over both the wide-area network (WAN) and LAN are secure.
- **Protection**—Via threat defense systems. Technologies such as firewalling and intrusion prevention systems combat threats from both internal and external sources.
- **Control**—Via trust and identity systems. Access control servers and the Cisco Network Admission Control (NAC) program enable organizations to control access to information, letting the right people get the right information at the right time.

Secure connectivity starts with Cisco IP phones and Cisco CallManager call processing software. Cisco IP phones support automatic classification of voice traffic into a high-priority queue to minimize latency and jitter. They are the first point at which the network is dynamically partitioned into two separate logical networks—one for data and one for voice. With the appropriate solutions deployed, when a user makes a phone call, the call signaling is both encrypted and authenticated with Cisco CallManager. If desired, the voice traffic



can also be encrypted for maximum privacy. For further protection, the software image running on the phone can only be installed if it has the appropriate signature. All of this is made possible by trust and identity capabilities based on industry-standard digital certificates and related authentication and authorization technologies.

Protection against threats is afforded throughout the system as well. On the Cisco CallManager side, Cisco Security Agent is used for intrusion protection and the NAC architecture helps to ensure that corporate security policies are enforced consistently across the enterprise. In the network, host intrusion detection sensors detect and identify unusual activity, and isolate it before it can affect the network. Using stateful packet inspection, Cisco firewalls lock down unneeded application ports and help to ensure that only authorized traffic is allowed to reach critical internal segments.

Because of the unique reliability and security capabilities of the Cisco solution, it is possible to achieve higher levels of security than that possible with traditional TDM based PBX systems. By applying security according to the guidelines in the Cisco SAFE blueprints it has been proven that a Cisco IP Communications solution can be the most secure IP voice solution available. In recent laboratory testing performed by Miercom, an independent testing firm, for Network World Magazine an IP Communications solution from Cisco received the highest possible rating of “SECURE”, and was judged to be more secure than any other IP-based telephony solution tested.

For more information about securing your network for IP Communications, visit:

www.cisco.com/go/ipcsecurity

MYTH #5

Deploying IP-based communications means throwing away your investment in traditional voice solutions.

Since all companies already have a voice communications system of some kind, many people think that a movement to IP Communications means throwing away all the money they’ve spent over the past 10 or 20 years building that voice infrastructure. The feeling is that you have to forklift out your old voice system to put in an IP Communications solution—making the move to adopt this technology a relatively big commitment.

THE REALITY

IP Communications solutions offer migration at an organization’s preferred pace.

This is an example of applying the old way of thinking to an entirely new paradigm. In the TDM world, telephony was thought of as a series of boxes that were located in each building in the company. Each box had a certain number of shelves, each shelf had a certain number of line cards, and each line card had a certain number of ports.

In the IP Communications world, think of telephony as a service in the network. The service is available from anywhere in the network, independent of location. For example, a multisite business may deploy the call control software only at the central site, then enable the remote sites to access the service remotely over the network.

In the end, every supplier in the industry agrees that the piece of sheet metal called a PBX that is bolted down in the basement today will disappear eventually—no boxes, no shelves, no line cards, no ports.

By integrating with most major legacy PBXs and voice-mail systems, as well as mission-critical business applications, Cisco IP Communications solutions empower customers to migrate based on their business needs instead of technology limitations.

Additionally, the idea of location-independent services in the network means that a company can use a building-block approach for migrating its communications to IP on a site-by-site, group-by-group, or application-by-application basis. In fact, 99 percent of Cisco customers migrate their networks to IP Communications using this approach.



For example, a company may decide to start by upgrading a greenfield site to IP Communications. Perhaps an organization is moving a regional office, or the PBX in the remote site has recently come off of its lease. In this scenario, the company can deploy Cisco CallManager call processing software in the regional office, install IP phones or softphones, and then voice-enable the data router to connect the regional office to the traditional voice system.

The next step might be deploying IP call control at the headquarters, and moving some of the users from the old PBX over to the new system with IP phones. Cisco CallManager will use one of the standard protocols—Q.SIG DPNSS, Digital Private Network Signalling System, or ISDN—to interoperate with the TDM PBX.

Then, over an appropriate time frame, the company can move users over to the IP Communications system. Some Cisco customers do this one floor or one building at a time, over a period of weeks or months.

Once that centralized call control infrastructure is in place, the customer can extend telephony service out to other remote sites. The process is simple—download a new image to the remote data router to support Cisco Survivable Remote Site Telephony (SRST), which will provide fallback support for the Cisco IP phones in the event of a WAN failure. Then, put some IP phones in a box, and send them to the remote site! As long as the appropriate data infrastructure is in place, the phones simply boot up when they are plugged into the Ethernet, and a dial tone will immediately be available.

For other voice applications, like voice mail or automatic call distribution (ACD) for a contact center, the customer can migrate the applications next—or in some cases, can start with the applications first! Cisco Unity voice mail and unified messaging software, Cisco IPCC customer contact software, and Cisco MeetingPlace voice and Web conferencing applications support both IP Communications and TDM voice.

Successful customer migration to IP Communications is as much about process as it is about technology. Understanding this, Cisco has developed detailed plans and processes that make migration smoother, faster, and easier for companies of all sizes. Using these proven migration methodologies, Cisco and its channel partners deliver superior customer success and satisfaction. At the end of the process, you have a converged voice, video, and data network. You decide whether it takes a week, a month, a year, or more, and no forklift is required.

For more information about planning your migration to a native IP Communications solution, visit:

Cisco Interoperability Portal:

http://www.cisco.com/warp/public/779/largeent/avid/inter_operability/

Cisco Migration Guide:

http://www.cisco.com/application/pdf/en/us/guest/netso/ns326/c643/ccmigration_09186a00800a1133.pdf

The Cisco IP telephony deployment case study:

http://www.cisco.com/offer/tdm_home/pdfs/iptelephony/cisco_case_study.pdf



SUMMARY

THE MYTHS

1. Customers should wait to deploy IP Communications until the standards are more mature.
2. An IP-based communications implementation is more expensive than implementing a traditional TDM communications system.
3. There is no single compelling application (“killer application”) for IP-based business communications today.
4. IP-based business communications systems are less secure than hybrid systems with a mix of IP-based and traditional communications.
5. Deploying IP-based business communications means throwing away your investment in traditional voice solutions.

THE REALITY

- Fundamental standards for IP Communications are already in place; new standards will continue to emerge.
- IP Communications solutions are proven to offer lower TCO and high ROI.
- There are many applications available today that cut costs, increase productivity, and improve customer satisfaction..
- IP Communications solutions are secure and reliable.
- IP Communications solutions offer migration at an organization’s preferred pace.

Let Cisco and its partners show you the value of a converged network and Cisco IP Communications solutions—a complete enterprise-class system that securely integrates voice, video, and other collaborative applications into this intelligent information network architecture. This system—including IP telephony; unified messaging and voice mail; IP-based audio-, Web, and videoconferencing; and customer contact solutions—takes full advantage of the power, resilience, and flexibility of organizations’ IP networks and boasts an inherent intelligence that enables organizations to solve problems, conduct transactions, and complete tasks more automatically. The result is a highly effective and collaborative business environment that significantly improves the way companies interact with their employees, partners, and customers, enabling organizations to set themselves apart from their competitors, while achieving a measurable ROI.

For more information about Cisco IP Communications solutions, visit:

www.cisco.com/go/ipc

**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 Web site 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 © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Cisco Unity 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 Web site 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. (0402R) 204079_ETMG_LF_06.04

Printed in the USA