There was a time when organizations questioned the need to migrate from legacy private branch exchange (PBX) telephony systems to Voice over IP (VoIP). Today, the question is not if, but when, and most important, how to implement the technology.

“One of the biggest advantages used to be reduced call charges,” says Bipin Mistry, vice president of strategy and technology, 3Com. “But now what’s happening over time with VoIP is not if it should be adopted, but when.”

The real benefit is that organizations can now have a single infrastructure to manage. In addition, users can determine someone’s availability so they can communicate with them easily. That translates into a more productive workforce.

“It’s tied to applications,” says Mistry. “And it’s tied to how [organizations] will do their business over time.”

In fact, according to Infonetics Research, Voice over Broadband (VoB) continues to be the top application driving investment in VoIP and IP Multimedia Subsystem (IMS) networking equipment.

“The overall next-generation voice equipment market is maturing,” says Stephane Teral, principal analyst, Infonetics Research. “The worldwide VoIP and IMS equipment market will more than double by 2010, when it will hit $6.8 billion.”

VoIP’s Offerings

“VoIP allows you to use networks to digitize voice/phone conversation using Internet or network connections,” says Dave Endler, VoIP security expert at TippingPoint. It also encompasses video and fax capabilities.

“It’s a little bit cheaper to maintain because in many instances you’re using your pre-existing data network to ferry data,” he says. A key advantage over legacy phone networks is the ability to converge with a lot of other enterprise systems, such as e-mail.

According to Brent Byrnes, regional manager for Federal Unified Communications, Cisco, customers used to have PBXs in multiple facilities, geographically dispersed. “With VoIP, initially it was all about reducing costs of communicating between multiple facilities,” he says.

“What we’ve seen over the last 10 years is a complete shift over what customers are trying to accomplish. We’re seeing another step [toward] network convergence. If you simplify it, you can boil it down to bringing together voice, video and collaborative data.”

Today, the driving factor for VoIP is the ability to deliver services more rapidly. “As customers move to an IP infrastructure, it changes the way that people see the network and these applications impacting their [operations],” says Byrnes.

And while cost is still a factor, the goal is to deliver services more rapidly and become more public-focused and available for direct interaction. “It’s not just about voice; it’s about collaborative data, voice and video,” he continues.

A simple example of how VoIP can drive communications is with Microsoft Outlook. You can link a phone number in an e-mail and instead of responding to the e-mail or picking up the phone, you can double click on the number and call that person from within the e-mail.

“It’s a more immediate way of communicating,” says 3Com’s Mistry. “Think of VoIP as a communication tool; that’s where the market is going.”
“With new phone installations, VoIP has probably overtaken the legacy phone network,” TippingPoint’s Endler concurs.

“It’s an easy alternative to legacy systems. It’s cost effective and a lot of the carriers are moving in that direction,” he adds. “A lot of the manufacturers are starting to roll it out as part of routing and switching products.”

**Video Conferencing Options**

IP telephony is sparking the increased use of video conferencing. The market has transitioned in the last few years from room-based video systems, where users can go to a meeting room to initiate a call, to users dialing in from their desks at various locations.

This provides telecommuters and remote staff with the option of video conferencing for meetings. “It lets you work with someone else who is video-enabled to have a real-time video session,” says Cisco’s Byrnes.

“The advantage is that users gain additional insight by being able to see the people they’re communicating with,” he adds. “Given the cost of travel, this is more important since people can interact face-to-face without being in the same room.”

Studies have shown that the percentage of communication that’s visible enables you to more effectively convey a message. In addition, you can have multiple types of video devices; you don’t have to have the same equipment to communicate.

“IT brings people together in a common collaborative environment,” Byrnes says.

“One of the most attractive features of VoIP is that it offers the capability of integrating communications directly with core workflow and [operations] processes, faster decision-making, faster and better customer service, improved communications with remote [staff] via video and converged conferencing, and makes rich communication features available to mobile and remote [staff],” says Steve Timmerman, vice president of corporate marketing at ShoreTel.

Beyond the communication factor is the ability to leverage an IP network and consolidate multiple sites into one. “If the customer has three locations, they can put them into one VoIP system and manage that as one,” says Jan Leistikow, director of product management for converged communications at Avaya.

“There are significant economies of scale, but being able to manage just one system and having one place for data traffic is the number one reason [organizations] are migrating to VoIP,” she adds.

Another key factor is mobility. Users can move across an enterprise campus and have their characteristics show up on the phone where they are moving.

Organizations can also have capabilities where they can extend features to a cell phone so users can travel and get the same features that they have at the desktop. “It’s easy to add or change users,” says Leistikow.

“For the most part, when people are making a buying decision around a communication system today, I think they want to make sure that it’s VoIP enabled,” she says. “Whether they use all the functionality is another thing, but they want to know that when they are ready to use VoIP capabilities, they can easily deploy [them].”

**Planning for Security**

Although the capabilities are there, most VoIP systems don’t come out of the box completely secure, so it’s important to know what an organization’s security concerns are to set them up properly.

“Because VoIP essentially allows you to use your existing network for this purpose — and that includes a lot of different types of software — you could actually expose your network to security threats if you’re not aware of all the possible security breaches,” says TippingPoint’s Endler.

“For example, a lot of voice systems send traffic over your network,” he says. “If you don’t enable encryption, someone sitting on the same network could watch the traffic and reconstruct your conversation.”
In addition, from a security point of view, it’s important to bring the management of the organization’s systems into one infrastructure with one set of security policies.

“Most [organizations] have standard data policies that can be applied to their VoIP solutions,” says Kevin Johnson, senior manager, security planning and strategy at Avaya. “That saves them a lot of ongoing daily tasks, and it also lets them have one policy to meet regulations.

“When they start to treat the voice equipment like the data equipment, with login, authentication, ID, audit trails and encryption, they can view systems as one in the same,” Johnson adds.

Consolidating the administration for both voice and data can keep the network secure without managing multiple login databases. “The end goal is to ensure that a single policy is put into place,” Johnson says. “Make sure that all VoIP servers and gateways are accessible and you can perform your network assessment via a single console.”

Also, VoIP security is more than just about the VoIP phones and the servers that they connect to. It’s also about the security of an organization’s pre-existing data network. Segmenting the traffic is one of the key security best practices.

“Keeping data traffic away from voice traffic is important,” says TippingPoint's Endler. “Voice traffic should be on its own separate VLAN. Make sure services are disabled that don’t need to be enabled, such as web server; there’s no reason for the web server feature to be enabled on any VoIP phone.”

Endler also recommends patching your infrastructure in a timely manner. “There are a lot of security vulnerabilities that come out on a pretty frequent basis. Most vendors provide patches, but if you don’t keep up-to-date with those patches, hackers can exploit those vulnerabilities.”

And because it takes time to apply those patches, Endler suggests two different types of security devices within a VoIP network. “One is a VoIP-aware firewall, so it can figure out which types of VoIP traffic should be going through to which devices,” he says. “The second is an intrusion prevention system, which analyzes traffic to make sure there’s nothing malicious in the traffic itself.”

VoIP security is strengthened by a broader organizational emphasis on security. “Organizations need a security approach that encompasses key elements of any security solution. Build a secure network and implement a secure call structure on top of that,” Cisco’s Byrnes says.

“Include certification testing, which ensures that your solution meets particular security needs, encrypt the signaling as well as the communication path and endpoint security authentication, and take necessary steps to secure the underlying transport mechanism,” he adds.

**Ready for VoIP?**

One of the first steps is to determine whether the entire network is ready for voice traffic.

“Do a bandwidth assessment to see if this network is ready for voice traffic depending on the number of users and calls the system would need to be able to handle,” says Avaya’s Leistikow. “Then determine what kind of upgrade would be necessary to handle bandwidth needs.”

3Com’s Mistry adds, “If you have an Ethernet backbone and up-to-date switches, most of the switches available today have been VoIP enabled. They automatically detect VoIP traffic and apply the right QoS settings.”

If you’re not sure you have the right infrastructure, he recommends running a voice audit. “It’s a quick sanity check to make sure that capability is available on your current network,” he says. “If you have it, then it’s just a matter of picking the VoIP platform that suits your needs.”

Some organizations opt to deploy VoIP in segments. If this is the direction you choose to go, Mistry recommends keeping your traditional telephony system running and transitioning over to VoIP gradually.

“That gets your communications and data infrastructure in place. Then figure out how to move toward unified communications and use a systematic approach,” he says.
ShoreTel’s Timmerman suggests moving to “pure IP” as soon as possible. “But you can roll out site by site if budget is a constraint. Don’t invest in an interim technology like hybrid or converged architectures.”

When it comes to evaluating systems, it’s best to look at where the organization wants to be in the next couple of years. “If you just want a straight telephony system, then there are several options,” says Mistry.

“You should consider the usability and the ease of deployment. If you’re looking further out — you want VoIP and you want it to evolve over time as needs change — then you should consider a system that is standards-based and has the longevity and scalability that you need,” he adds.

Typically, he says, a traditional voice system would be swapped out within seven years. What you want is a future-proof system that can tie into all your applications as well as a system that has a high level of redundancy and can scale across multiple sites as your organization grows. “It should be easy to deploy and have a high level of scalability.”

In addition, Mistry recommends looking for systems that support current standards, such as Session Initiation Protocol (SIP).

“The more standards you drive into the environment, the more open the environment is, the more capabilities you have to pick alternate vendors in terms of applications that you want to drive,” he says. “A closed system limits you to whatever a particular vendor wants to do from a communications standpoint.”

**Increasing VoIP ROI**

Allan Sulkin, president of TEQConsult Group, an enterprise communications consultant in Hackensack, N.J., offers some ways organizations might be able to increase VoIP ROI.

- Evaluate the status of the network and any planned upgrades. “IP telephony will always save you money,” but switches, routers and other network devices purchased more than five years ago may need to be replaced.

- Take advantage of new field projects. When an organization moves to a new location or opens a branch office, it avoids the problem of having to maintain redundant telecommunications systems, and the cost of IP phones is not much higher than that of typical desk phones.

- Don’t count on immediate headcount reductions. Combining voice and data will reduce the number of people who have to support the network. “But you may have to go through a period of time when you actually need more people” because IP telephony requires skills that may not be available in the organization’s networking or telecommunications departments.

- Go for more functions, not fewer. The more functional the VoIP service, the bigger the bang for the buck, and therefore the better the ROI. For instance, an organization can reduce travel costs by including web collaboration tools and video conferencing.

- Include user productivity aids. Combining the desk phone with softphone functions on users’ PCs, for example, will let staff see if colleagues are available to talk — and where and how to reach them.

Let CDW•G help you save time by having professionals assemble and install your network hardware.

**CALL 800.808.4239 TO TALK TO A SPECIALIST TODAY.**