Deploying VoIP in the Enterprise

Abstract

Data networks are becoming increasingly viable for supporting telephony and the advantages of converged networks are continuing to make themselves apparent. A successful IP Telephony deployment is assisted by an awareness of where you are going-this comes from considering all of the elements required to deploy and maintain a converged, Voice-over-IP capable network. These elements are discussed in the this white paper, along with guidelines for setting up a pilot project and performing an incremental rollout of IP Telephony.

Benefits of Converged Networks

Data networks are becoming increasingly viable for supporting telephony and the advantages of converged networks are continuing to make themselves apparent. Therefore, the time to consider strategies for making the transition to converged networks is now! Reference deployments have been made with great success, and this has helped to create some rules of thumb for assisting in an IP Telephony rollout. A successful deployment is assisted by an awareness of where you are going—this comes from considering all of the elements required to deploy and maintain a converged, Voice-over-IP (VoIP) capable network.

These elements are discussed in the following sections, along with guidelines for setting up a pilot project and performing an incremental rollout of IP Telephony. As you move towards enterprise-wide deployment, you often want to keep elements of your existing infrastructure intact until the time is right to completely replace it. You should leverage your existing infrastructure to ensure a smooth, low risk transition to a converged network.

There are many compelling reasons for implementing IP Telephony; the potential for reduced cost in maintaining a converged network is one; others include:
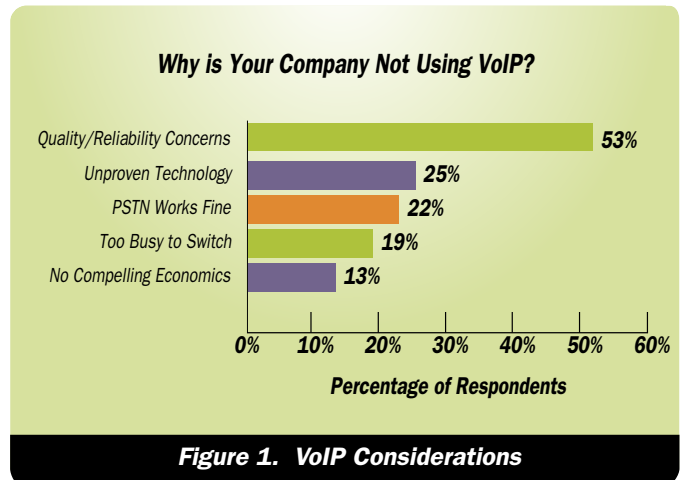
- Bypassing long distance toll charges for inter-office calls within the enterprise
- Least cost routing of off-network calls via the enterprise network
- Replacing costly Private Branch Exchanges (PBXs) that may only serve a few users in a branch office
- Replacing outdated PBXs at a much lower cost and reduced maintenance
- Creating a next generation contact center for improved customer relationship management (CRM)

The typical size of VoIP deployment has grown from a few stations for pilots in 1999, to production roll-outs in 2001 ranging from 30 to 100 stations. Several large enterprises have successfully deployed thousands of stations, over multiple locations, and in the process some of them have migrated entirely from traditional PBXs to IP Telephony.

Most large enterprises are considering VoIP as they review their telephony and network infrastructure budgets and strategies. This goes hand-in-hand with vendor readiness reaching critical mass. Major communications equipment vendors now have stable solutions to complement their traditional TDM voice switching gear. Enterprises have a choice of proven solutions.

The business reasons to move ahead are very compelling—the potential for cost savings from toll bypass and from folding your datacom and telecom staff into a staff that maintains a single converged network are persuasive. Enterprises are rightly

moving cautiously (see Figure 1), but as the following statistics show, the reasons for doing so are generally more to do with the state of the industry and valid concerns about having a suitable network infrastructure to support the voice, than they are with the perceived benefits. It is worthwhile to be certain you have the convincing economics (in terms of ROI) before embarking on a large IP Telephony deployment. You need to start by evaluating the role that IP phones will play in your network, and before beginning a large-scale deployment you must ensure the network infrastructure can handle it.

Why is Your Company Not Using VoIP?

Quality/Reliability Concerns	53%
Unproven Technology	25%
PSTN Works Fine	22%
Too Busy to Switch	19%
No Compelling Economics	13%

Percentage of Respondents

Figure 1.   VoIP Considerations

Best of Breed Approach

Deploying IP telephony is a critical business decision where one-stop shopping does not make sense. With so many facets and possible scenarios to the solution, maximizing the potential to save money while maintaining the flexibility to embrace new applications, means choosing best of breed IP Telephony solutions from vendors with a depth of experience in telephony. The potential for vendor lock-in from a one-stop-shopping approach is high, and can inhibit your choices and negotiating power later on.[1]

In some cases, enterprises discover the need for features only upon deployment—these features tend to find their way into IP PBX products or telephony solutions built by traditional PBX vendors, and not as quickly by infrastructure vendors who may happen to have a proprietary telephony solution. Before replacing a PBX on the strength of promising ROI claims, it is worthwhile to look closely at all the capabilities it was giving you.

For instance, one of the things a PBX can do for you is to multiplex ISDN circuits from a trunk group coming in from the PSTN. These can be used by data devices inside the enterprise network. You may use them for ISDN dial-up between routers as a backup for the IP WAN, or for extra

---

[1] Cisco Systems and Voice: The Untold Story. Gartner Group Research Note July 2002.

WAN capacity on demand, or for traditional H.320 (ISDN-based) video-conferencing. Not all vendors have recognized the need for this, and have thus not built such capabilities into their pure IP solutions. Consequently, their customers might subsequently have to budget for ISDN multiplexers they had not counted on. Similarly many traditional PBX vendors have put features in their IP components that provide support for legacy peripheral cabinets, so you preserve the investment on analog and digital phones, even after you've replaced the PBX. For these and other reasons, blending voice and data on a converged network no trivial task. It requires pragmatic choices in selecting the voice equipment, and an infrastructure that meets the stringent reliability and Quality of Service (QoS) requirements demanded by telephony applications.

A high level look at VoIP architectures in both the LAN and WAN environments will show why this is so. The infrastructure choices for VoIP should be made in the early stages so you are ready to deploy, as the ideal telephony solutions for your business become apparent. The right infrastructure, must meet your long-term IP Telephony goals, supporting all manner of advanced IP voice applications.

Experimental VoIP Scenarios

The most simple test implementation of VoIP on the LAN might look like the following diagram. Phone conversations are converted to a stream of IP packets and sent over an Ethernet network. This network is usually restricted to a building or campus.


Figure 2. Simple Pilot Configuration
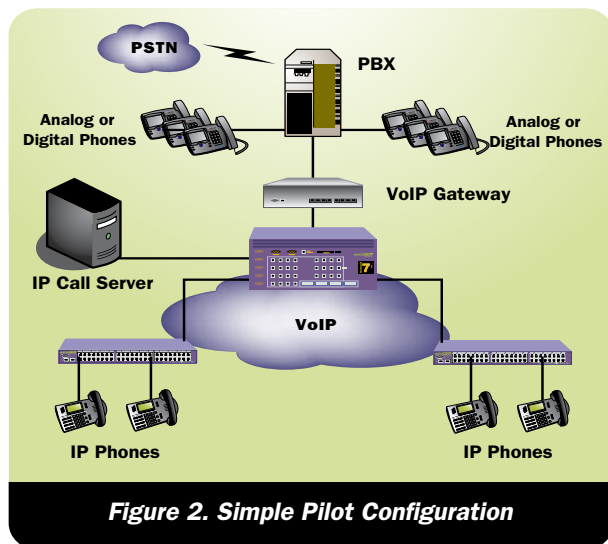
You can always take small steps like this one to experiment with VoIP in your enterprise. Gateways between the telephony and data networks can be verified in this way. Regardless of the method that is used to convert the voice traffic, one fundamental process will remain the same: VoIP traffic will always traverse the LAN and WAN as a stream of IP packets.

Voice traffic is converted to VoIP traffic by different devices, depending on the architecture of the solution. In toll bypass applications, gateways convert voice between the PBX and IP network. In most IP Telephony deployments it occurs at the IP phone as well. And in the case of architectures involving analog phones and phone hubs, VoIP conversion occurs at the phone hub.

For a business that is considering voice and data convergence, putting VoIP on the WAN is as important as VoIP on the LAN. VoIP on the WAN is where the advantages of toll bypass show themselves. The reasons for this are primarily economical. Cost savings can be immediate when long distance phone calls are diverted from the public switched telephone network (PSTN) and sent over an existing IP-based WAN. It is believed that around 90% of VoIP deployments thus far have been toll-bypass applications.

Running VoIP traffic on the WAN can be done in several ways. If the voice traffic is coming from a PBX, then a VoIP gateway will be required to convert voice traffic from the PBX into IP packets for transmission over the IP-based WAN. Similarly, a VoIP gateway will be required at the other end to convert VoIP traffic back into the format used by the PBX. The IP-based WAN can be a private data network (leased lines; a frame relay service or an ATM service), a public IP carrier or the public Internet.

Figure 3. Simple Toll Bypass Scenario
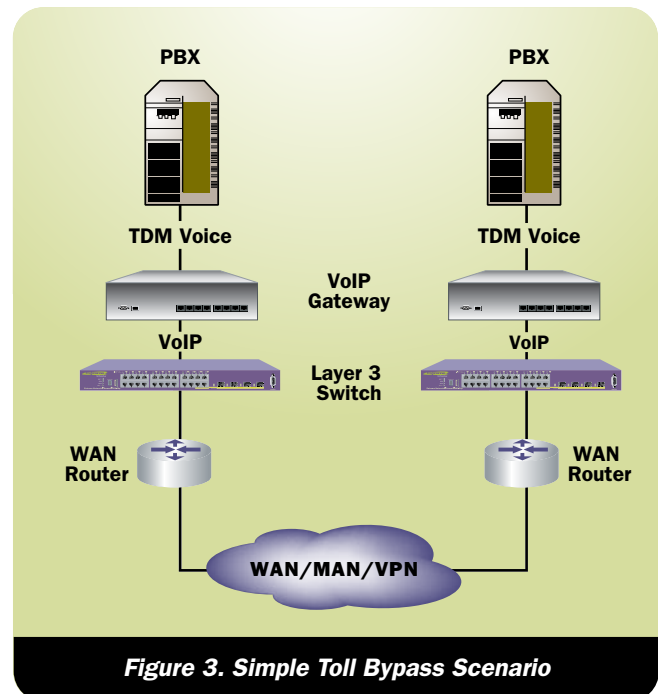
You may have already experimented with these tentative approaches to implementing VoIP in a partial way, and thus reap some of the cost savings. The next steps will further integrate your voice and data networks and get you further down the road to realizing the full potential of IP Telephony.

Phone Connectivity Options

To progress from tentative, partial rollouts to a fully converged network, you have to make some choices as to how your phones are going to be configured at the desktop and how they will be connected to the network. One configuration is to have the IP phones use a dedicated switch port connection; this option requires two drops to each desktop, one for the phone and one for the PC. This provides a level of physical redundancy at the cost of an extra switch port.

Because of the lower cost, a common alternative is to daisy-chain the desktop PC to the IP phone, essentially sharing the network switch port and cable. This aids in rapid deployment and facilitates maintenance later with Moves, Adds and Changes (MACs), but requires a more intelligent switching infrastructure.

To achieve this, the IP phone basically has a three port switch built in, so that there is a 10/100 port connection from the phone to the network switch, a 10/100 port connection that connects to the desktop PC, and the internal port that connects to the phone itself. Most vendor IP phones support this mode. Of course, if you are using a soft phone (driven by software in the desktop PC), the only connection is to the PC.

You do not need to use the same configuration at each desktop, but the connectivity option you choose may affect the feature sets available to you and the maintainability of the network at the edge.
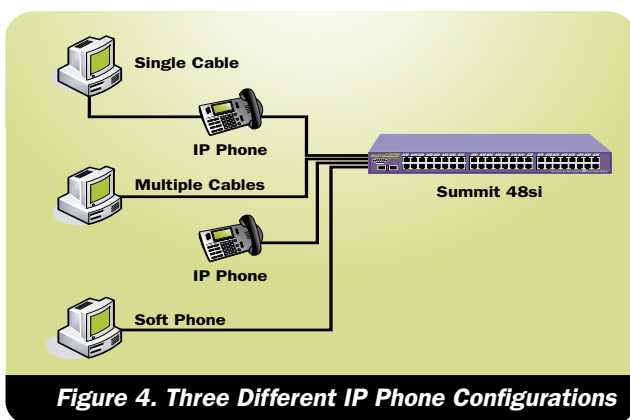
Figure 4. Three Different IP Phone Configurations

Analog phones, which you may still use in some areas, must connect to an IP network via a voice hub. The voice hub will digitize and packetize the analog signals, and additionally provide control and/or call signaling to other voice hubs, call servers and other H.323 clients (such as IP phones), as well as gateways to the PBX or PSTN. Alternatively, depending on which telephony vendor you select, you may be able to re-use your analog phones by connecting IP call servers or a related component to legacy peripheral cabinets. In this case the conversion to IP occurs at the device aggregating the peripheral cabinets.
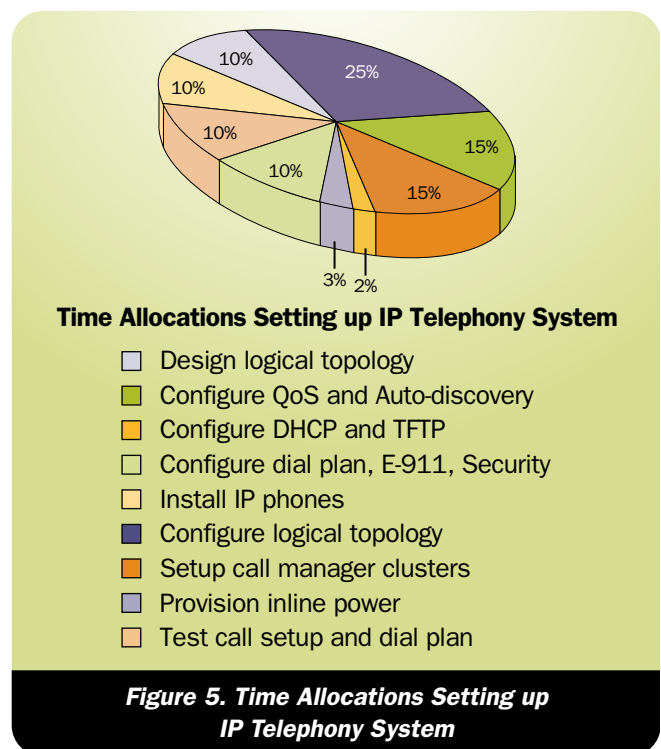
Elements of a Converged Network

A typical campus IP Telephony implementation involves the creation of at least one VLAN for the voice service on every switch that may have an IP phone attached to it. The end-to-end QoS needs of voice are very different from those of data; this demands that each switch be configured with QoS profiles for voice. As a rule of thumb the picture looks approximately like this, although the order in which these tasks are performed are site dependent:

- Configure the logical topology for VoIP
- Create and assign QoS profiles for all devices that might have to support phones
- Set up your call server clusters or IP PBX to manage features and dial plans for the phones
- Set up a DHCP service for address assignment
- Set up power handling for the phones
- Implement security for your dial plans and to prevent unauthorized network access
- Implement an E911 plan
- Install and set up the phones
- Test the system and dial plan

A related issue has to do with the ongoing maintenance of the IP Telephony system. One of the promises of VoIP on a converged network is reduced cost of MACs. This is difficult to realize without tools to simplify and automate deployment.

Figure 5 shows an approximate breakdown of the time it takes to fulfill the requirements of these areas.

Time Allocations Setting up IP Telephony System
- ☐ Design logical topology
- ☐ Configure QoS and Auto-discovery
- ☐ Configure DHCP and TFTP
- ☐ Configure dial plan, E-911, Security
- ☐ Install IP phones
- ☐ Configure logical topology
- ☐ Setup call manager clusters
- ☐ Provision inline power
- ☐ Test call setup and dial plan

**Figure 5. Time Allocations Setting up
IP Telephony System**

These topics and their related issues are discussed in more detail in the following sections. You should note that logical topology and VLAN configuration, along with QoS provisioning, comprise approximately 50% of the MAC/VoIP Deployment task set.

Topology Configuration

Configuring the logical topology of your enterprise network for high availability and VoIP includes designing the Layer 2 and Layer 3 topologies including VLANs and subnets. It also includes setting up your spanning tree (Layer 2) and routing rules (Layer 3).

Virtual LANs (VLANs) are essential in a converged voice/data network. Creating a voice VLAN provides the easiest configuration and management options for IP phones. Separate VLANs for voice and data also allow you to logically separate and prioritize VoIP traffic over data transactions. All IP Telephony vendors recommend configuring separate voice VLANs.

An example of an enterprise wide network with voice and data VLANs is shown Figure 6. The deployment scenarios vary dramatically, from simple toll bypass, in which only PBXs are tied to one another across the corporate IP WAN, to enterprise-wide IP telephony, in which all phones are IP and the PBXs are completely displaced with IP-based call servers (providing voice mail, call forwarding, conferencing, etc.) and gateways between the PSTN and the IP network.

Voice VLANs are configured as overlays across a network that can be either routed, VLAN-separated, or a hybrid. The telephony VLAN supports only the telephony application components and traffic. However if it is enabled, it provides application isolation for QoS and administration, and also allows specific DHCP service to keep MACs easy and cost effective within the call server zone. Ideally, an IP telephony VLAN should also be its own subnet, fully routable across Layer 3 links or to interconnect voice VLANs that have been separated for administrative or other reasons.
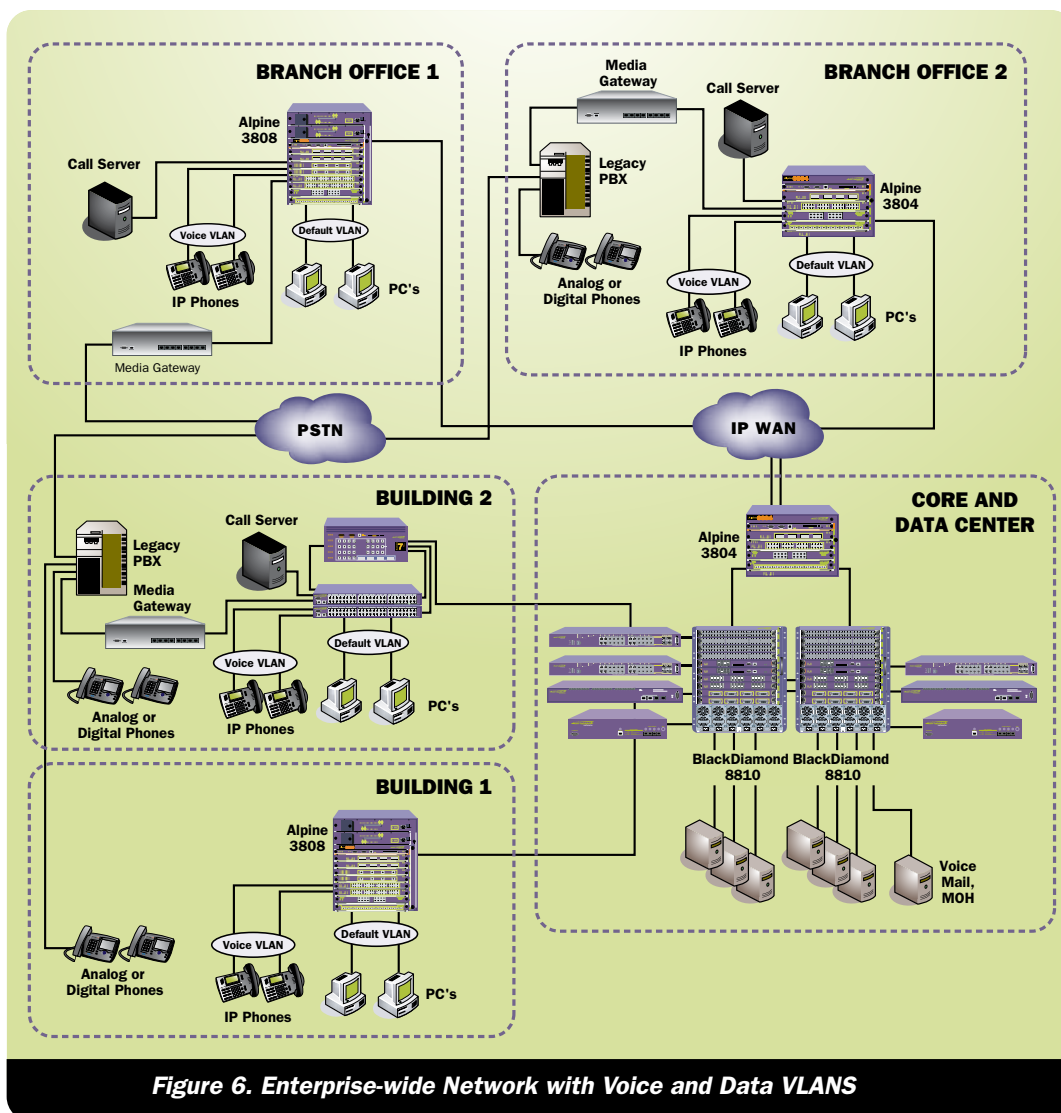
Figure 6. Enterprise-wide Network with Voice and Data VLANS

QoS Profiles

VoIP VLANs contain much more, of course, than the edge switches connecting the phones. They also must include all aggregation and core switches end to end between all the IP phones throughout the enterprise.

All relevant devices that might have to forward voice traffic must be configured with QoS profiles. Doing this once across the network may mitigate the need to make changes at the edge for each IP phone MAC. But as more phones are added at the edge, or if large numbers of phones are moved from one switch to another, QoS profiles at the aggregation layer and core will need adjustment to guarantee more aggregate bandwidth.

Call Servers

Call setup and control is a key IP Telephony function. It can be provided by a centralized call server with optional backup servers, or can be distributed throughout the network, depending on implementation. Alternatively, an IP PBX, or an IP Telephony enabled interface for a standard PBX could also offer direct attachments to the IP network and provide call management services.

Call servers manage the features and dial plans of the phones, and are responsible for call-setup and call-hand off to the IP phones. Setting up a call server involves configuring rules for communicating between different call servers, ensuring redundancy, and configuring device (phone) pools. You must build a table containing a list of IP phone Media Access Control addresses and the phone extension that should be allocated to each phone. As new phones are added to the network they need to be defined to the call manager in this table.

DHCP Service Configuration

You can assign IP addresses for the phones using either DHCP or static configuration. Since the phones will require a lot of IP addresses, you will probably prefer to use DHCP so addresses can be reused. This is another reason why telephony VLANs should be on their own subnet if possible—it will be easier to track IP addresses used for phones.

Phones use the DHCP servers to get information about what "call servers" exist. Some telephony vendors have implemented extensions to DHCP to assign phones to their appropriate VLANs in conjunction with IP address assignment. Features like this will continue to make deployment and configuration of IP Telephony more Plug-and-Play.

Inline Power

Most traditional phones operate during power failures; because the phones are powered from the PBX itself. In an IP Telephony environment, not only must uninterruptible power be supplied to the call servers and gateways, but each IP phone may also need similar power protection in order to operate, in local power outages.

Policy-Based QoS

Even though raw bandwidth capacity can be plentiful in a LAN/Campus network, you still need to provide a guaranteed level of packet throughput to VoIP for it to function well. Without proper QoS settings, the bursty, bandwidth hogging potential of certain data and video applications increases the latency and jitter of voice to unacceptable levels.

Once a packet takes longer than about 200 milliseconds to travel to its location, voice quality starts to become unacceptable. Too much latency makes it difficult to maintain a dialog. This is especially noticeable on cell phones, when people try to interject comments while someone else is talking: the difference between a pause and a break in the dialog is hard to distinguish with high latency. As latency increases, people "talk over each other" more.

Extreme Networks Policy-based QoS relies on several components to achieve the desired results that allow network administrators to get the proper control over managing the bandwidth characteristics various applications demand. Stated simply, policy based QoS consists of robust traffic classification combined with bandwidth management treatments:

Classification + Treatment = Policy-based QoS

These policies allow network administrators to control the bandwidth various applications use and maintain latency and jitter control over the applications that need it. Extensive classification without robust treatment capabilities are quite useless. Imagine having a carpool lane when there is only a single lane; that's similar to no classification. Imagine no traffic laws on a multi-lane freeway, without minimum or maximum speed limits; that's similar to no treatment capabilities.

Broadly speaking, classification can be made using either explicit information (such as 802.1p DiffServ code points) or implicit information (such as membership of a voice VLAN, or TCP/UDP ports).

Treatment refers to prioritization and bandwidth management, which is handled in Extreme Networks switches via min and max bandwidth control, in conjunction with eight queues on every switch port (in the i series chipset switches). After traffic is classified, it is assigned to one of these priority queues for servicing. Each queue may also be rate-shaped using bandwidth controls, thereby also controlling latency.
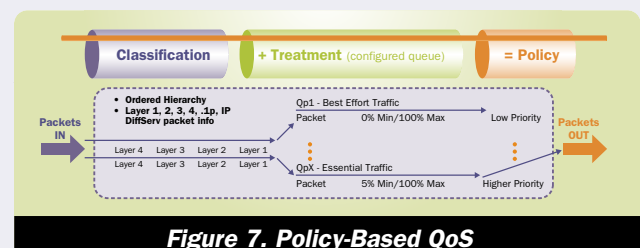

Figure 7. Policy-Based QoS

Reliable power delivery through inline power to IP phones is critical for service survivability and E911 services support. Inline power reduces the risk of lost power to the phone and reduces the support costs associated with troubleshooting phone outages.

With inline power support at every seat, enterprises avoid having to verify and possibly change power availability at the wiring closet every time an IP phone is added or moved. This long-term goal of ubiquitous power is a single piece in the puzzle of eliminating support costs associated with service deployments.

There are two types of inline power solutions today (illustrated below):
- Mid-span powered hubs
- Ethernet Switches with integrated inline power

The industry is moving inexorably towards integrated inline power, but the IEEE standard for this support (802.3af) is still in flux, the few solutions available today may be obsolete within a year.[2]

In the short term, especially during the transition from legacy PBX exclusively to IP Telephony, it may be prudent to wait for the standards to finalize, and for vendors to deliver standards based phones and switching equipment. While you have the majority of phones powered by the PBX, the need for always-on IP phones in the event of an emergency, may not be pressing enough to justify a premature vendor selection for switching equipment that supports inline power. During the early stages of IP Telephony roll-out, mid-span hubs offer lower port densities, more flexibility in terms of relocating devices, and lower risk exposure, should they ultimately become obsolete when the standards are final.

VLAN Manager and VoIP Manager

Extreme Networks switches have been designed from the beginning to support network convergence. With eight hardware-based queues per port, each with the ability to offer a minimum and maximum bandwidth allocation, Extreme Networks ability to support VoIP along side other mission critical applications is unparalleled in the industry.

Moreover, Extreme Networks has automated as much this the process as possible. As part of the EPICenter® network management suite, Extreme Networks continues its tradition of award-winning provisioning tools with VoIP Manager, helping enterprise networkers configure VoIP networks in the most efficient way possible.

VLAN Manager and VoIP Manager are both fully integrated into the awardwinning EPICenter management solution, which provides full end-toend FCAPS. You can create VoIP VLANs through EPICenter's VLAN Manager, and VoIP Manager inherits these VLAN definitions.

In addition to creating and configuring VoIP VLANs and QoS profiles end to end, VoIP Manager calculates end-toend min/max bandwidth requirements based on the G.7xx compression algorithm used, number and location of IP phones. VoIP Manager also provides status reporting for all VLANs on a per-switch and per-port basis.

Extreme Networks' Infrastructure Security

When IP Telephony is deployed, network ports are exposed from semipublic or public areas—for example, there may be an IP phone in the lobby. Extreme Networks has advanced security capabilities.

Access Control Lists (ACLs) filter out inbound traffic (such as HTTP, FTP, Telnet, SMTP etc.) that may not be relevant to an IP phone. Thus, the network remains secure even in the case of Layer 2 address spoofing, and phones are protected against Denial of Service (DoS) attacks.

With the recent enhancements to ExtremeWare's Layer 2 Address Security, a port can be limited to a number of MAC addresses that are learned by the port (e.g., one address for a pure IP phone port). The MAC address of an IP phone can be learned dynamically when the phone is installed, and the port is then "locked down" to this MAC address, even after a reboot. This provides an excellent level of security against port abuse.

In cases where ports are allowed for data clients as well, phone discovery is combined with user level access security. Network Login is an excellent user level security feature in ExtremeWare that requires no client software, and thus works even in semi-public environments such as universities and libraries. Network Login works with any client device and operating system that supports DHCP and a web browser. In addition, Extreme Networks is following the emerging standard for 802.1x (port based network access control) that will play an important long term role in enterprise environments. The combination of Network Login and 802.1x on the same port will allow deployment of user based security immediately, without requiring network client device changes.

---

[2] Cisco Systems and Voice: The Untold Story.
Gartner Group Research Note July 2002.

Implementing Security

Voice security is at least as sensitive a topic as data security. Users expect that all voice communications are confidential (no one is listening in), even when they don't have the same expectations of an e-mail containing the same information. Just as one needs to protect the infrastructure against rogue access points being inserted in the network, one should also prevent unauthorized MACs of IP phones, especially while automated procedures (QoS adjustment, automated E911 tracking, etc.) are not available.

Password or access list changes may be needed to accommodate a MAC. Even if a phone changes VLANs, some authentication updates may have to be made to accommodate its new physical location. Also, there may be some database updates needed for accounting or billing purposes. This is especially true (as with QoS) if the switch now supporting the phone was not aware of the VLAN before the move. The call server may need to generate a new security profile based on the phone's new physical location.

Dial Plan and E911 Considerations

There are various other considerations including setting up a dial plan architecture, E911 and RADIUS/TACACS considerations, and selecting and installing any necessary gateways for connecting to legacy PBX or key systems.

An E911 service has to provide automatic number and location information (ANI and ALI) to the 911 operator (PSAP: public safety answering point) when an emergency call is made. Most traditional PBX's were/are only able to provide this support with third-party assistance and a lot of administration.

To appreciate the unique issues of E911 support in IP Telephony, consider how emergency calls are handled with a traditional PBX. When an emergency call is made, information is typically sent to a security staff relating the caller's physical location on the campus with their extension number. When an emergency team (e.g., police or fire department) arrives, an employee can meet the team and direct them to the emergency.

IP Telephony offers two basic approaches to handling emergency calls: on-net to campus security or off-net to the carrier Point of Presence (POP). With on-net campus security, usually an individual in the company assists the 911 respondent; with off-net approach, the number and location of the individual in distress is made available to the PSAP.

The issue to be solved here is that an IP phone can be moved without any centralized administrative intervention. A database has to be maintained to map the IP phone's unique Layer 2 addresses to a physical location now being served by a port on a switch. This is not the case with a traditional PBX, which just maps a port to a phone.

Extreme Networks E911 Support and "Rapid MACs"

With Extreme Networks infrastructure, E911 database information can be maintained very rapidly, whenever a phone is moved. Plugging and unplugging a phone generates "Link up" (when the phone is plugged in) and "Link down" (when it's unplugged) alerts. This provides information to E911 applications to detect IP phone movements allowing databases to be updated automatically.

The benefits and implications of turnkey E911 support include more rapid MACs. MAC activity includes two main components:

- Physically relocating station equipment or new construction
- Software-related updates, such as switch/router QoS or authentication configuration, E 911 database updates, and call manager-related functions such as display names, call coverage, phone numbers etc.

The process might start with a call or e-mail to a help desk. A typical Service Level Agreement (SLA) might call for software changes within half a day and physical changes within 24 hours. Many of the software changes with a VoIP MAC will be similar to a PBX-based MAC, but can be automated to a greater degree with sophisticated infrastructure tools that take advantage of the intelligence of your converged network.

End-to-end, policy-based QoS configuration is another area where Extreme Networks is ahead of the field in both rapid deployment and rapid MAC support – see the VLAN Manager and VoIP Manager for more information.

The dial plan architecture includes dial plan groups, calling restrictions, and on-net route patterns. This area includes defining which gateway to use when someone makes a long distance call, or which PSTN trunks to use for domestic versus international calls. For a "least cost routing" example, consider the following: If someone in Chicago wishes to calls off-network to a customer in San Jose, the call can be routed over the enterprise network and get handed off to the public phone network via a gateway in the San Francisco office (the nearest office to San Jose), thereby being charged only for a local call instead of a long distance call from Chicago to San Jose.

Configuring Phones

The phones now have to be configured. This is a task that will vary depending on your architectural choice at the desktop— single cable, multiple cable, or soft phone.

This is an area where management tools can help with VLAN assignment and QoS configuration.

Testing the IP Telephony System

Before deployment of even a part of the VoIP infrastructure is complete, extensive testing has to be done on the IP Telephony system including on-net and off-net calls, the dial plans, E911 emergency calls, and fail-over conditions.

Rolling Out VoIP Successfully

When evaluating an IP Telephony system, you might start with a standalone network to learn how to configure the products and interconnect the VoIP equipment with your existing telephony and data infrastructure without disruption of voice or data

services. This lets you to evaluate voice quality in a controlled setting (see Figure 8).

But, once you've narrowed down the telephony platform of choice, you must run a pilot involving user advocates from various business functions. This is critical for verifying the network can deliver the required voice quality amidst different data traffic conditions.

The pilot project must be planned carefully. The best candidates for a pilot project are new workgroups that do not yet have telephones, or workgroups needing unique capabilities that are best delivered using a VoIP solution, but it is important to include as wide a mix of user types as possible, because they have different data application behavior to compete with voice. In the example shown below, the legacy PBX continues to serve the rest of the users, and a VoIP gateway transparently interconnects the legacy PBX to the IP network. This VoIP gateway may be standalone, or integrated into an IP PBX or call server. Most IP Telephony vendors advocate isolating voice traffic from

Figure 8. Example VoIP and Data Configuration
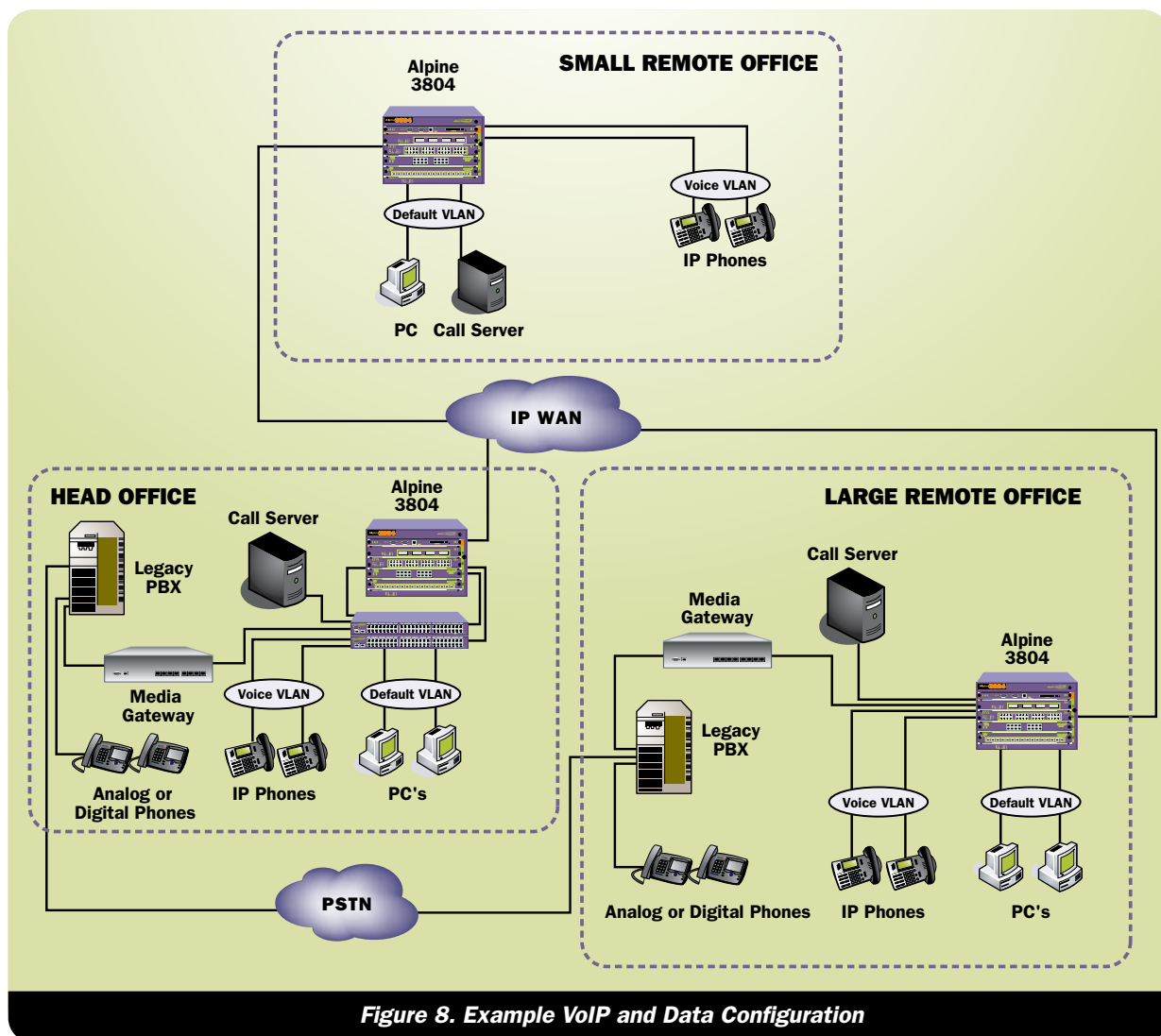
data using voice VLANs. Wherever possible, a single VLAN spanning the company is advantageous, as it minimizes configuration. This is easily done with Extreme Networks even over Telco WAN links, because of our Ethernet everywhere approach. Ports connected to telephony equipment that does not do tagging should be configured as untagged members of the voice VLAN. Ports connected to workstations and servers are left as members of the default VLAN. Each VLAN should be in a unique IP subnet. If you connect a second switch to this network, be sure the ports connecting the two switches are configured for tagging on the voice VLAN, and no tagging on the default VLAN.

Considering the complexity of a full-blown VoIP deployment, VoIP should be deployed across the enterprise in phases. The key to successful deployment is proper bandwidth provisioning and QoS. Keep voice traffic in a separate VLAN, and make sure it is given priority over data traffic. If a WAN is in use, make sure that voice QoS is maintained end-to-end across the wide area network.

Conclusion: Success Factors in VoIP Deployment

The key in choosing the right solution for a converged network is not to confuse convergence with "one stop shopping." IP Telephony is an application, and should be treated as such—just as you would seek advice from business consultants and ERP system vendors to find a strategic ERP solution, you should be going to telephony experts and system integrators to address your telephony application requirements.
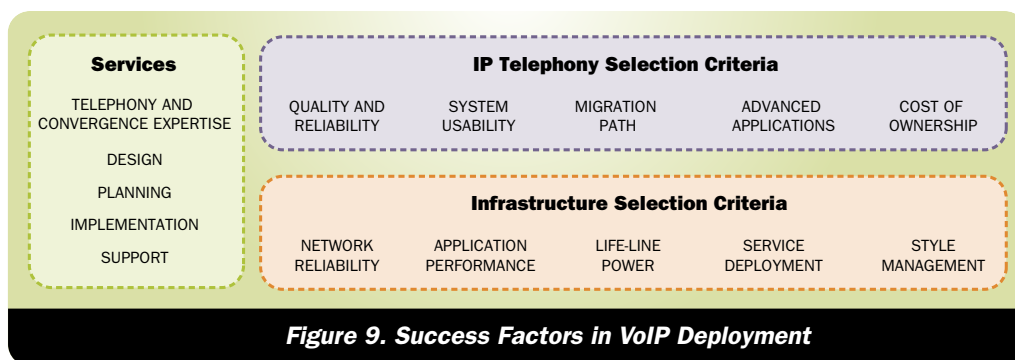
At the end of the day, a consistent network architecture and best-of-breed applications do far more to lower your TCO—and keep application performance high—than any single vendor solution can. Thus, it makes sense to separate the network

choice from the application choice. Your VoIP deployment success factors can roughly be characterized as falling into three main areas: integration services, IP Telephony, and the network infrastructure (Figure 9).

Voice experts should be consulted for IP Telephony equipment selections, and network infrastructure equipment should be selected based on its ability to serve all enterprise needs, while delivering strict performance guarantees to the most critical applications. This gives you the best applications and the most suitable network to run them. You also need special services to create a VoIP network: telephony and convergence expertise help tremendously with the design, planning, implementation, and the ongoing support of the converged network.

In terms of IP Telephony selection, the areas to consider are the quality and reliability of the equipment (and whether it supports your required applications), the usability of the system (which speaks to how readily it will be accepted), and how easily the telephony solution can be upgraded (migrate) to your desired future system—these future application needs should be anticipated now. Finally, the TCO of the system must be computed to the best degree possible. Important TCO factors are upgrade costs and personnel costs to configure and maintain the converged network.

In many ways, of course, the network infrastructure decision is even more critical. Performance and reliability are obviously key, as phone systems must be available at all the times and voice quality has to be maintained on a policy basis with special attention to latency and jitter. But there are also some unique needs in terms of the ability to power the phones, deploy and maintain the system, and manage and maintain the security of the network as a whole.

Services	IP Telephony Selection Criteria				
TELEPHONY AND CONVERGENCE EXPERTISE	QUALITY AND RELIABILITY	SYSTEM USABILITY	MIGRATION PATH	ADVANCED APPLICATIONS	COST OF OWNERSHIP
DESIGN	Infrastructure Selection Criteria				
PLANNING					
IMPLEMENTATION	NETWORK RELIABILITY	APPLICATION PERFORMANCE	LIFE-LINE POWER	SERVICE DEPLOYMENT	STYLE MANAGEMENT
SUPPORT					

Figure 9. Success Factors in VoIP Deployment