# VoIP and IPT Best Practices for Implementation

## A Guide to Ensuring a Solid Foundation for Unified Communications

***Gary Audin, Delphi, Inc.***

## Executive Summary

Migration is the movement from one place or condition to another place or condition. Migrating from the TDM PBX to VoIP and IP Telephony (IPT) will not be a one-time, instantaneous process. Rather, it is a continually evolving process that may take place over months and even years. Plans must be made, alternatives considered, best practices followed, facilities prepared, and systems must be procured and installed. Installing VoIP/IPT systems is not a plug-and-play implementation. Proper preparation is essential.

VoIP/IPT migration is a four-stage process (figure 1):

1. Assessing and preparing the infrastructure to ensure its readiness to support VoIP and installing the upgrades are mandatory in stage one.
2. Setting up a pilot system to acquire experience with this new technology and to compare vendors and resellers (integrators, channels, and partners) is optional but highly recommended.
3. Product selection and implementation is another mandatory stage.
4. Operation and administration, as well as planning and installing an expanded number of sites and stations, software changes and adding applications is also a mandatory stage.

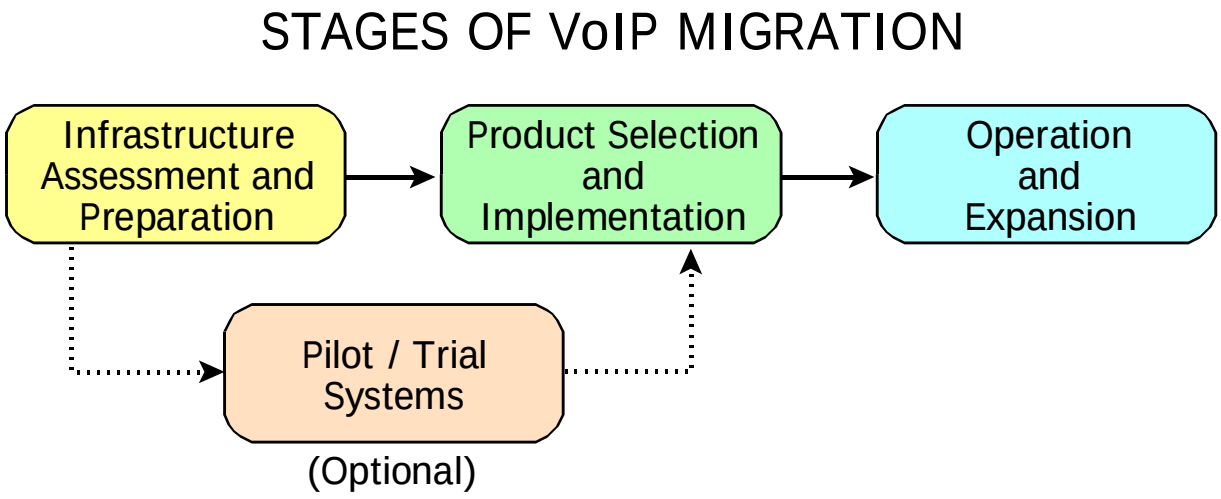


Figure 1

Each stage has recommended best practices that should be followed. This paper provides a digest of the considerations from existing VoIP/IPT implementations for each of the four stages and presents a checklist of Best Practices. The Best Practices that are part of this paper are divided into the following nine categories:

1. Assessing the LAN and WLAN
2. Completing the Closet
3. Assessing the WAN
4. Improving the WAN
5. Planning and Testing the Pilot IPT System
6. Ensuring Secure Operation
7. Organizing for Convergence
8. Best Practices During Selection and Deployment
9. Best Practices After Deployment

Everyone reading this document should review categories 1, 2, 6, 7, 8 and 9. If VoIP/IPT will be operating over WAN, then categories 3 and 4 should be read as well. If a pilot/trial is planned, then category 5 should be reviewed.

## Planning Before Migrating to VoIP/IP Telephony

It is always good to plan. Without adequate planning, there will be cost overruns, failed implementations, service disruptions and dissatisfied users. Poor planning can also end careers. Planning for a VoIP/IPT implementation has some unique issues that are not typically part of the IT staff's or CIO's experience. Changes in organization, responsibilities and budgeting need to be made. Unifying IT and telecom management can reduce finger pointing. There are different voice and data budgeting mindsets to overcome. This is the result of the different cultural and historical backgrounds of IT and telecom departments.

The telecom staff is used to delivering reliable, high quality voice services but does not focus heavily on the underlying TDM technology because it works so well. IT must now consider and deliver different levels of Quality of Service (QoS) over the IP network that were not necessary in the past. IT will need to manage more servers and – assuming IP phones are used – probably twice as many IP endpoints.

In order for the Total Cost of Ownership (TCO) to be accurate, investment in the staff, their training and organization must be calculated. It is likely that the increase in training will make the staff more valuable. Although the headcount will probably not change with VoIP/IPT implementation, salaries will increase. Most of these issues will become more apparent in large IT organizations. The smaller the staff, the less impact VoIP/IPT will have on the IT organization because small staffs already know each other's job. The organizational silos by job function for the smaller IT/telecom staff usually do not exist.

Very likely, the typical enterprise will consider at least two vendors: a legacy TDM vendor and an IP data vendor. Each vendor has some advantages, but they are not all equal. Even if the

enterprise does not issue a RFP, the enterprise should look closely at the offerings of their incumbent legacy and IP data vendors before making a selection.

Migrating to VoIP/IPT is not just about technology. There are best practices to follow as the VoIP/IPT implementations progress. Preparing the infrastructure, modifying the LAN closets, and upgrading the WAN performance are all new investments.

It is wise to work with a trial or pilot system, not only to evaluate the vendor and their products, but also to determine the readiness of the enterprise's networks and staff for the implementation.

The best practices list in this document covers a wide range of issues, considerations and recommendations. Use it as an evaluation tool to help avoid gaps in the planning, budgeting and execution of the VoIP/IPT system.

## Best Practices Defined

Best Practices is a term used to define recommendations for procedures and tasks that will increase the likelihood of success for a project and/or operation. It is a management concept comprised of a list of considerations. It outlines a process that is more effective than other methods, processes or activities when attempting to deliver a particular outcome. The idea is that with the proper procedures, validations and testing, a project can be successfully completed with fewer problems and unanticipated complications.

Following the Best Practices recommendations will not guarantee success, but it will reduce problems, simplify the process, contain risk, keep the implementation on schedule and keep the project on budget. Best Practices may not be applicable to all enterprises migrating to VoIP/IPT.

However, a Best Practices list can be used to verify that the implementation team is following procedures that will produce a higher degree of success. Best Practices can be viewed as a checklist of suggestions. For example, the Best Practices list for traveling in a car includes closing the door, putting on the seat belt, turning on the ignition and, finally, ensuring it is safe to move the car. You don't have to follow the list of safety suggestions, but the outlined procedure is safer than other procedures for driving the car.

## Issues in Preparing the Data Networks

Few enterprises know the performance capacity of existing enterprises' IP networks especially as it relates to network jitter. Most data networks have some bandwidth bottlenecks. The effect of these bottlenecks for the data user is that access and up/downloads are slow. The slower network does not modify the delayed information. Voice over IP traffic, however, will be seriously affected by poor network performance. When speech is carried over the same poorly performing network, that speech is garbled, words are missed and the speech can sound robotic.

Network problems and impairments are commonly associated with the WAN. LAN implementations have fewer performance problems. The WAN investment will mostly be the expenses for adding more bandwidth and QoS and expanding the network management systems.

Moving to VoIP/IPT will place stress on the design and operation of the existing data infrastructure. The Ethernet LAN and closets will definitively be affected. The WAN will also be affected if it is to be used for site-to-site IP trunking for voice traffic. Infrastructure performance becomes critical for VoIP voice quality. Factors that can be tolerated with data transmission will cause voice users to hang up and not use the voice services. Much of the work to be performed is in determining what really exists in the data networks, how well it performs for VoIP traffic, and what needs to be done to improve the operations. Most VoIP/IPT vendors find that their customers' data networks are not ready for VoIP/IPT.

Another, no less important issue, is reliability. The enterprise is used to delivering a very reliable and stable voice network. Many enterprises believe that they experience 99.999% availability for their telephone systems.

Although this may not always be the case (very few enterprises have measured their availability) very high reliability is expected. The most reliable call requirement is for the 911 call. There is no equivalent to 911 calls on the data network. VoIP/IPT systems are not available 99.999% when the data network and electrical power are included in the calculation. Data networks have typically not been designed to meet the 99.999% availability level. It takes more design work on the part of the enterprise to produce a highly reliable/available and stable VoIP/IPT system and network.

## Assessing and Preparing the LAN

The VoIP/IPT system and components operate over an Ethernet LAN. The best configuration is to use LAN switches rather than hubs. The LAN switch can deliver QoS and Power over Ethernet (PoE) and also operate full duplex. A hub cannot deliver any of these features. VoIP/IPT devices will work through the hub, but with the aforementioned disadvantages. Almost all of the components will operate on category 5 or better copper cable. Most vendors recommend, and some require, that category 3 cable be replaced with category 5 or better cable. There are rare instances where a fiber-optic connection will be used for a server, but not the gateways or IP phones.

There are probably spare ports on the LAN switch. Inventory these ports to determine how many are available for the IP phones. Does the LAN switch support PoE? It is common with older LAN switches that only ½ the ports can support PoE. The switches may need to be upgraded or replaced. LAN switches with PoE will also require more electrical power and air conditioning. The LAN switch comes with reports of its utilization and operation. Access these reports to measure the activity on all the LAN ports to ensure there are no bandwidth bottlenecks.

It is recommended that the voice devices be separated on their own Virtual LAN (VLAN) supporting IEEE standard 802.1q. This reduces competition with the data traffic for bandwidth and can increase security by isolating the voice devices from the data devices. Implementing IEEE standard 802.1p provides Class of Service (CoS) for prioritizing voice traffic over the data traffic. Check the present LAN switch capabilities for 802.1p and 802.1q. The switches may need to be replaced to support these functions.

The primary conclusions relating to preparing the LAN are:

a. An inventory must be taken to determine if the LAN switches are ready for VoIP/IPT components.
b. A financial investment will most likely be necessary before implementing VoIP/IPT.
c. The upgrades for VoIP may not be part of the IT budget and there will be some issues as to which group – IT or telecom – will pay for the upgrades.
d. The LAN management systems will need to be improved to support VoIP traffic and monitor the network impairments that affect the voice quality.

## What are the Closet Needs for VoIP/IPT?

VoIP implementation will affect the closets: the LAN closets and the telephone closets. The telephone closets on each floor – the Intermediate Distribution Frames (IDF) – will continue supporting the legacy phone, FAX and modem connections. It is unlikely that these closets can be eliminated until all legacy devices have been replaced.

The Main Distribution Frame (MDF) is the room that houses the legacy PBX, has cable connections to all the IDFs, and has the connections to the communications carriers and PSTN. The MDF room cannot be eliminated either. Removal of the legacy PBX cannot be accomplished until the IPT system is successfully operational. The MDF room will still be needed to connect to the carriers and PSTN. The MDF room should also accommodate the VoIP gateways that connect to the legacy devices and PSTN trunks. It is possible that the call server/manager can be located in the MDF, but it is better to locate the server in an IT data center.

The LAN closets are a different matter. These will be the central location where the IP phones connect for support. LAN switch changes were discussed in “Assessing and Preparing the LAN,” earlier in this paper. PoE will demand greater power and air conditioning. The LAN closet’s power capacity will probably be inadequate. Each PoE power supply can easily require 20- to 30-amp service. The 110-volt power and receptacles will probably have to be changed to 208- to 220-volt service. This will produce a corresponding increase in heat output. One PoE LAN switch can produce 6000 BTU, requiring the equivalent of one bedroom air conditioner per PoE LAN switch. Is the LAN closet’s air conditioning capable of handling the increased heat load?

The legacy PBXs usually have a battery backup system that can operate for 2 to 6 hours during a power outage. The enterprise that wants to match this power backup must install an Uninterruptible Power Supply (UPS). The difference is that a UPS should be located in each of the LAN closets supporting IP phones. UPS needs to be located in the MDF for power backup

of the gateways. It is assumed that the call server/manager in the data center will already be connected to the data center UPS. If the WAN is used for VoIP, then the routers will require UPS as well. This is distributed, not centralized, UPS. This raises the cost for the UPS. The enterprise should consider a centralized UPS management system that connects to all the distributed UPSs. The UPSs will require regular testing and monitoring. Battery replacement will be required every 5 to 7 years as they age.

The enterprise should be prepared for two factors that will increase the electrical bill. The first increase is due to the energy needed to power the LAN switches, PoE and IP phones. The second increase is a result of the continued escalation in utility charges, as much as 15% per year. The enterprise should consider LAN switches with power management features to help reduce energy costs.

Other questions to consider when evaluating the closet preparation are:

- What is the sequence of configuration installation?
- Are the wiring blocks cabled correctly?
- Did the vendor assume that the enterprise already had certain components in place?
- Are the VoIP products independent or dependent on the enterprise's choice of LAN/WAN components and vendors?
- How does IT know when the closet is ready?

## WAN Assessment and Improvement

The WAN is the more likely candidate to need performance improvements. IP WANs were not designed to carry real-time voice traffic. Further, 99% of the applications running over the WAN operate through TCP. TCP automatically retransmits erroneous packets, resends lost packets, slows down when there is limited bandwidth (flow control) and guarantees and verifies the delivery of packets. Most data applications can also tolerate some network delay (latency) if it is not too great. TCP-based applications are commonly transmitted between a desktop and a server, not desktop-to-desktop. Performance measurements are therefore between the desktops and the server over a star-configured network around the server(s).

Voice traffic is carried over UDP, which performs none of the TCP functions. UDP guarantees nothing, assumes there is always enough bandwidth and does not retransmit anything. You might say that the UDP designer's attitude is "send and hope." This is not a bad design. Voice traffic ***cannot*** work effectively over TCP. The delays alone would make voice conversations awkward. Since UDP operates without taking any responsibility for assuring packet delivery, network impairments can seriously affect voice quality performance. The performance measurement for voice traffic is from desktop-to-desktop, phone-to-phone, over a meshed, peer-to-peer network. Signaling and voicemail traffic go to a server.

Performance assessment of the WAN ***must*** be completed before VoIP calls are deployed. Most VoIP/IPT vendors require this assessment before implementation because their experience has demonstrated to them that most data networks do not perform well enough for voice traffic. Another performance assessment must be carried out after the WAN improvements have been installed to determine if the improvements deliver adequate

performance and capacity for VoIP traffic. The assessment should be run again after deployment to measure the performance of the WAN with voice traffic.

Performance assessments should be run periodically – about every three months – to look for degrading performance and increasing data traffic that will affect the voice quality performance. In the long run, it will be less expensive for the enterprise to procure their own performance assessment tools rather than using a service or consultant. The presently owned network management system may be upgradeable to support VoIP performance measurements.

The network engineers that design and operate the WAN must be trained in the performance requirements for VoIP. These network engineer/operators will also be responsible for monitoring and policing the QoS. They should be trained to use the assessment tools. The WAN management systems must be upgraded or augmented with expanded features for VoIP network management.

## Considering the VoIP/IPT Pilot

A VoIP/IPT system is new technology. Most enterprises set up a trial or pilot installation before proceeding to full implementation. The pilot stage is optional but highly recommended. First, the data staff must become familiar with the expectations they will have to deliver for the security, reliability and performance of the data networks. Secondly, the enterprise has to be confident in the vendor, integrator and reseller. It is relatively new technology for the vendor, integrator and reseller as well.

The pilot will be useful in verifying that the system works as advertised and is mature enough, especially in software, for successful deployment. There will always be factors that weren't considered – or were considered minor -- that will become a greater impediment to success than expected. These need to be discovered during the pilot stage. The pilot will also point out the weaknesses of the enterprise staff and determine if the present IT and telecom organizations are ready to migrate to VoIP/IPT. There are Best Practices in this stage that are different from the assessment stage.

## Delivery of Voice Quality through QoS

VoIP speech transmission will require better IP network performance than most IP networks can deliver. This does not mean the IP networks are badly designed; it means they were designed for data, not voice traffic. Voice traffic is less tolerant of network impairments than data traffic. Both voice and data traffic will be competing for the same bandwidth and router and LAN switch resources. Many enterprises think that buying enough bandwidth will solve the impairments and performance problems. This can work within the LAN by providing 100 times more bandwidth than the user needs. It is primarily a one-time cost.

The WAN is a different situation. Bandwidth comes at a higher cost-per-bit than on a LAN, and the cost recurs each month. Buying excessive amounts of bandwidth will work, but who can afford it? Therefore, there must be a mechanism to assign preferential treatment to some

traffic; voice traffic must receive better treatment than data traffic. This is called Quality of Service (QoS).

There is a subset of QoS, called Class of Service (CoS), that essentially places certain packets in the queue ahead of other packets. This is how a LAN with 802.1p operates. CoS may be all that is needed on the LAN switch. If the utilization of the LAN is low – less than 15% – CoS may not be a benefit since the all traffic is treated well when there is little competition for the bandwidth.

CoS will work on the WAN, but may not be adequate for voice traffic. This leads to the need for other preferential treatment. Voice traffic should not only be at the head of the queue, it should experience higher reliability and less latency, jitter and packet loss. Effective QoS techniques such as Differentiated Service (DiffServ) and Multi-Protocol Label Switching (MPLS) can deliver better service for voice packets. But QoS should be assigned sparingly. If it is over-applied, every packet will receive good service and there is no preferential treatment. The speech packets should have precedence over signaling packets (SIP, H.323…). Interactive data packets should have precedence over file transfer packets. Both should be treated less preferentially than voice and signaling packets. A minimum of two levels of QoS should be supported: one for voice, and a lower QoS for data. Many MPLS service providers offer up to five levels of QoS service.

Some network engineers assume that QoS implementation is enough when combined with extra WAN bandwidth. It is if the QoS policies are properly monitored and enforced. The performance that QoS delivers will vary based on the network health and competing traffic. When a network failure occurs, the QoS may not be properly configured or not work at all. Monitoring QoS means constant daily observation of the network performance and collection of useful statistics.

Performance per call is the ultimate measurement of call quality. This measurement is called the Mean Opinion Score (MOS). A MOS of 4.0 or greater (the highest MOS is 5) indicates an acceptable call quality. As the MOS decreases below 4.0, there may be some user dissatisfaction. At a MOS of 3.5 or lower, most users will complain frequently or not use the phone at all. So implementing QoS is not enough if the MOS is not satisfactory.

There are tools and techniques available from the VoIP/IPT vendors and from third parties that can report the MOS per call for each direction. The information gathered is stored with the Call Detail Record (CDR). The MOS can also be processed in real time. When the MOS falls below 4.0, the network operators can be alerted. If the MOS falls below 3.5, alarms should be issued for immediate attention. This means that the QoS implementation should be measured by constantly monitoring the MOS for all voice calls.

MOS is not the only measure of user satisfaction. When there is a failure of dial tone or access to the PSTN or voicemail or the network does have enough capacity to carry the call, the user will see these events as additional factors in the performance of voice service delivery. Delivering a dial tone without the other services is very close to having no voice service at all.

The reliability and health of the network are also major factors that affect the satisfaction of the user.

## Security and Vulnerabilities

The protection and security of information and resources requires constant vigilance. You are never finished. There are many issues with VoIP/IP Telephony networks:

- The VoIP/IPT devices, servers, gateways and phones share the data network and inherit the data network's security problems.
- There will be data attacks on voice devices, such as Denial of Service and malware.
- Voice speech ports on the firewall can be used to attack the data network by pretending to be voice packets.
- It is easier to eavesdrop on IP calls than on TDM calls.
- The centralized TDM PBX is gone. VoIP/IPT resources are spread around the network, making them more vulnerable to security attacks.
- VoIP/IPT operating systems are less secure than TDM operating systems.
- Systems (PBX) administration can be positioned at multiple locations and can be accessed by web browsers.
- There will twice as many IP addresses to manage.
- Denial of Service attacks can stop dial tone, disconnect calls, block feature access and cause VoIP endpoints to cease operation.

A good resource and overview of the issues is the "Security Considerations for Voice over IP Systems", National Institute for Standards and Technology (NIST) publication SP 800-58 available at http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf.

Ethernet and IP networks were not designed with integrated security. If you refer to the original design documents, security is assigned to the endpoints, not the networks. Therefore, Ethernet, TCP, UDP, and IP are vulnerable to security attacks. The FTP, SMTP, Telnet, HTTP, etc. application protocols do not have built-in security features. These are designed as peer-to-peer protocols that do not require intervention by, nor use of, a server. Security for these protocols is an attachment, not integrated.

Security is, in part, the protection from attacks generated outside the enterprise. Firewalls will be required. The firewall must be modified to support the VoIP signaling protocols, support UDP traffic, perform dynamic UDP port number allocation per call and modify network and port number translation. Alternatively, the enterprise may want to consider Session Border Controllers (SBC) instead of firewalls to carry VoIP traffic from untrusted to trusted networks.

Security implementations can also hinder voice quality. Encrypting speech adds to latency. Firewalls usually do not support QoS, nor do they have the performance to ensure voice quality. Firewalls can add latency, jitter and sometimes packet loss. Laboratory tests show that Intrusion Prevention Systems (IPS) will reduce voice quality when the security controls are fully implemented. The only way to improve voice quality in these tests was to reduce security. Using a VPN to carry voice will improve security, however, the VPN tunnel can encrypt the QOS labels and therefore QoS cannot be implemented.

Security vulnerability testing is becoming common for the data network, servers and desktops. Vulnerability testing of the VoIP/IPT servers and endpoints is also becoming common. There are many instances where a security attack has been successful because the enterprise and vendor staffs did not have the imagination to predict the attack.

An example is that two IPT vendors had situations where their IP phone speakerphones could be turned on remotely without the phone ringing and the caller could listen to the conversations going on in the room. These security problems have been fixed.

What other possible vulnerabilities exist that have not even been imagined? Security is a never-ending job. There are best practices that can significantly help prevent and mitigate these security issues.

## Migrating to VoIP/IPT with Your Vendor/Integrator

The migration to VoIP/IPT is a team effort by the enterprise and the vendor/integrator. Every implementation starts at a different place with unique factors, as well as common considerations. The age of the existing legacy system, cabling, closets, power delivery will vary from site to site and from enterprise to enterprise. Every implementation will begin with different advantages and limitations, requiring different amounts of financial investment, staff and organizational changes, and costs of ownership.

Use the nine Best Practices lists for the evaluation of the enterprise's readiness and to ensure that the vendor/integrator has performed their part of the planning process. The lists are also helpful in preparing the RFP. Many of the Best Practices include suggestions for features and functions that should be included in the RFP and, in some cases, features that may cause some problems later, for example, producing security weaknesses when using the feature.

## VoIP/IPT Best Practices List

These best practices lists are designed to provide the reader with a series of items, considerations and factors to peruse when planning the migration to VoIP and IP Telephony. The lists are meant to be thorough, but there will always be some consideration that is unique to an individual installation.  Use the lists to verify that you have considered each item. Several of the items may not be appropriate for your installation. However, the verification process will increase confidence and reduce potential planning errors.

The lists are divided into nine categories. Each category has a list of recommendations, suggestions or considerations relevant to that category. The nine categories are provided so that each of the Best Practices lists can be distributed to the appropriate staff for review and analysis. Three columns are provided for the reader to determine if the recommendation is evaluated and applicable, not verified, or not applicable for this VoIP/IPT implementation.

It is strongly suggested that each item's verification be documented. All too often, a verbal confirmation turns out to be incorrect and deployment is delayed. Networks change,

configurations are modified, a planned upgrade has not yet been made, and the hardware or software has not arrived. All these can lead to a delayed, costly and poorly implemented VoIP/IPT deployment.

| Best Practices | Evaluated | Acted Upon | Not Applicable |
|---|---|---|---|
| **1. Assessing the LAN and WLAN** | | | |
| **Measure LAN Utilization** – Reports are available from the LAN switches that provide utilization measurements. Check the LAN utilization on the switch-to-switch-to-router connections during the voice busy hour and ensure it is below 15%. | | | |
| **Inventory the LAN Switch Ports** – If the IP phone has only one port, then the LAN switch will need to be expanded by nearly twice as many ports, one extra port for each IP phone. A two-port IP phone can share a single LAN port with a PC. | | | |
| **Buying PoE** – LAN switches may only be able to support about 50% of the ports with PoE. Ensure that there are enough PoE ports for IP phone expansion. The power supply is the limiting factor. Install fault-tolerant power supplies so that if one power supply fails, the PoE continues to operate without any loss of IP phone power. Assume that other devices such as WLAN access points, security cameras and environmental controls will be connected to the LAN switch in the future and require PoE. This will require more PoE ports and more robust power supplies. Don't just plan PoE for IP phones. | | | |
| **Configure for a VLAN** – Most IP phones will support IEEE 802.1q VLAN capability. Configure the VoIP/IPT devices on a separate VLAN. This will improve voice quality performance and security. | | | |
| **Implement LAN QoS** – Most IP phones will support IEEE 802.1p QoS. If the IP phones are on a separate VLAN and the LAN utilization is low (below 5%) then this may not be required. If the LAN switch already supports 802.1p as well as the phones, then turn it on, since there is no significant advantage to turning off 802.1p. 802.1p can be useful on the connections among the LAN switches and the switch connections to the routers since there may be bandwidth contention on these connections. | | | |
| **Avoid Duplex Mismatches** – Watch for half duplex connections that reduce the capacity of LAN switch connections. Ensure, don't assume, that all the connections to the IP phones, gateways and servers are configured full duplex. This is an extremely common problem because installers assume the connections are full duplex when they perform auto-configuration and so do not verify the installation. | | | |
| **LAN Security** – Store configuration information and tables in a secure system. Validate all changes ***before*** they are made. Ensure that changes can only be sent from a very limited set of desktop addresses. Verify configurations and tables after a restart/reboot. | | | |
| **WLAN Planning** – A WLAN can be saturated by too many simultaneous calls. The 802.11b WLAN saturates with seven to eight calls, and the 802.11a/g WLAN saturates with 21 to 22 calls. The number of access points may need to be expanded to cover the number of WLAN IP phones. It may sound contrary, but it is a better idea to devote the 802.11 b or g WLAN for data and a separate 802.11a WLAN for VoIP calls. This reduces bandwidth competition, keeps the data devices running at higher speeds and ensures there is enough capacity to carry VoIP calls. Look for WMM Power Save on the WLAN phone to extend battery life. | | | |

| | | | |
|---|---|---|---|
| **WLAN QoS** – QoS on the WLAN is more difficult to deliver. IEEE standard 802.11e should be implemented for QoS on the LAN. Even with WLAN QoS, the packet loss rate can be as high as 10%, which causes retransmissions and lower usable bandwidth. Plan for 100Kbps per direction (200Kbps) for G.711 uncompressed calls and less for compressed voice. Roaming among access points can cause problems such as temporary signal loss, which can be mistakenly interpreted as a lost call. | | | |
| **WLAN Security** – Consider implementing IEEE Layer 2 LAN standard 802.11i that uses dynamic key assignment with Advanced Encryption System (AES). Implement an authentication protocol such as the Extensible Authentication Protocol (EAP). This encryption is separate from the VoIP encryption. | | | |
| **Upgrading the Management System** – The installed management systems should be analyzed to see if it can deal with the performance and configuration issues that will occur with VoIP and IP Telephony such as PoE operation. | | | |

| **Best Practices** | **Evaluated** | **Acted Upon** | **Not Applicable** |
|---|---|---|---|
| **2. Completing the Closet** | | | |
| **Cabling** – Upgrade all cabling to at least category 5 and 100Mbps operation. Operating at 1Gbps on category 5e or 6 will be necessary if the PC behind the IP phone, on a two-port IP phone, requires higher speed. IP phones run well at 100Mbps. | | | |
| **Power Considerations** – Check with the facility staff to be sure there is enough AC power in each closet for PoE support. In some cases, 208/220VAC may be necessary to operate the PoE switches. Also ensure that the correct power receptacles are installed. In older buildings, it may be necessary to have the local electrical utility run more power cables to the building. This can be a problem in Europe and older urban buildings in the U.S. and Canada. | | | |
| **Air Conditioning** – PoE switches generate a great deal of heat. One large PoE LAN switch produces 6000 BTU, meaning that this single switch requires the equivalent of a one bedroom-size air conditioner per switch. The added air conditioning capacity will increase the power the electrical utility must to deliver to the building. Duct work may have to be modified to handle the expanded A/C. | | | |
| **UPS/Battery Backup** – Most legacy PBXs have battery backup that allow the PBX to operate for two to six hours. Duplicating the same power backup, that is configured for the legacy PBX, will require battery backup in the server room, routers, LAN closets and gateway locations. Diesel and gas electrical generators require about 10 seconds to begin operation. Without battery backup, VoIP/IPT devices and data network components (switches and routers) will have to reboot, thereby extending the outage time. Battery backup for 30 to 60 minutes should normally be enough if there is no generator operating. Beyond 60 minutes, the equipment rooms and closets generate too much heat to continue operating without generators to power the air conditioners. Procuring DC-powered LAN switches that operate off the battery system can reduce utility costs as much as 30%. Another value of battery backup is eliminating server restart times and phone re-registration that occur with AC power fluctuations. | | | |
| **MDF and IDF Space Planning** – The Main Distribution Frame (MDF) and the Intermediate Distribution Frames (IDF) will continue to exist as long as there are legacy devices and carrier connections. No additional space will be required. | | | |

| | | | |
|---|---|---|---|
| **Closet Floor Space** – The floor space in the telephone wiring closets (IDF) will not change. The floor space where the old PBX was installed will be oversized because the MDF will become relatively empty once the old PBX is removed. It is the LAN closet and possibly the server rooms that may require more space. If backup batteries are installed in the LAN closets, there may not be enough space available. Also the weight of the batteries may require additional physical support on the lower floors to hold up the batteries' weight. | | | |
| **Gateway Installations** – The media gateways connect to the legacy phones, fax machines, modems and other devices and so should be installed in the MDF where all the legacy cabling is terminated. This is much better than re-cabling the legacy connections to a LAN closet or data center room. The trunk gateways connecting to the PSTN should be installed in the MDF because that is where the carrier connections already exist. | | | |

| **Best Practices** | **Evaluated** | **Acted Upon** | **Not Applicable** |
|---|---|---|---|
| **3. Assessing WAN** | | | |
| **Measure Router and Link Utilization** – Reports are available from the routers that provide utilization measurements. Check the router port utilization on the switch-to-router connections during the voice busy hour. Also check the trunk utilization between routers. If the Trunk utilization between routers averages over 30% during the voice busy hour, then either an alternate link is necessary or the link bandwidth needs to be increased. Do not look at daily or weekly reports as these skew the results and understate the real utilization. Look for utilization measurements in 15 minute increments. Too long a measurement interval will not show the peaks and valleys of traffic, only an average. | | | |
| **Performance Testing** – Performance testing to determine latency, packet loss, packet burst loss and jitter is mandatory. Most VoIP/IP Telephony vendors will require at least two performance tests, one on the existing WAN and another after the WAN is improved. This will be part of the contact or a separate charge. It is better to purchase a vendor acceptable performance measurement package as the enterprise really needs to run performance tests for troubleshooting and collecting performance trend information after the vendor leaves. | | | |
| **Traffic Simulation** – Some performance packages/tools include VoIP call traffic generators. If a number of WAN connections are to configured for VoIP, then the enterprise should own a traffic generator tool. The tool is used to determine the maximum number of calls that be carried by the WAN link or path at an acceptable Mean Opinion Score (MOS). Traffic simulation tools are also useful before a new site is cutover and during troubleshooting performance problems. | | | |

**Capacity Planning** – Every vendor has a calculator or table that is used to determine the bandwidth needed for a VoIP call. The calculator will cover different packet sizes and compression types. The following table is an example of this calculator and can used for most bandwidth provisioning. The cRTP column includes the bandwidth reduction when RTP header compression is used. Header compression is only of real value when the voice and header are both compressed.

**Packet Voice Transmission Requirements**
(Bits per Second per Voice Channel)

| Codec | Voice Bit Rate | Sample Time in msec | Voice Payload | Packets per Second | Ethernet Kbps | PPP or Frame Relay | |
|---|---|---|---|---|---|---|---|
| | | | | | | RTP Kbps | cRTP Kbps |
| G.711 | 64Kbps | 20ms | 160 bytes | 50 | 88K | 83K | 68K |
| G.711 | 64Kbps | 30ms | 240 bytes | 33.3 | 80K | 77K | 67K |
| G.711 | 64Kbps | 40ms | 320 bytes | 25 | 76K | 74K | 66K |
| G.729A | 8Kbps | 20ms | 20 bytes | 50 | 32K | 27K | 12K |
| G.729A | 8Kbps | 30ms | 30 bytes | 33.3 | 24K | 21K | 11K |
| G.729A | 8Kbps | 40ms | 40 bytes | 25 | 20K | 18K | 10K |

**Verifying Network Health** – Routers keep track of erroneous packets and packet loss. Check the router reports for the occurrence of erroneous packets since they will indicate the health of the trunks between the routers. Keep in mind that erroneous packets look like packet loss to the IP phone. Also check that the router does not frequently change paths, as this is an indicator of continually changing trunk and network card conditions and needs to be repaired.

| Best Practices | Evaluated | Acted Upon | Not Applicable |
|---|---|---|---|
| **4. Improving the WAN** | | | |
| **Performance Goals** – The performance required from the LAN/WAN networks is partially dependent on the ability of the receiving endpoint (IP phone or gateway) to compensate for the network impairments. There are four factors, with corresponding performance goals, important for acceptable voice quality:<br><br>**Performance Factor** — **Goals**<br>Latency (end-to-end network delay) — 100ms or less<br>Jitter (delay variation) — 20ms or less<br>Packet loss — ½ to 1 % or less<br>Packet burst loss — Less than 4 packets lost in one group<br><br>The final goals will vary; for example, network latency needs to be less than 80ms when larger (30ms) voice packets are used with encryption. Check with the endpoint vendor to determine the acceptable performance goals that your particular configuration of endpoints can tolerate. | | | |
| **Bandwidth Planning** – The signaling protocol is primarily used during call setup and does consume enough bandwidth to affect the network. The bandwidth of the calls will probably be about 24 to 26Kbps for G.729 compressed calls. The actual bandwidth will depend on the packet size (20, 30 or 40ms). If the RTP header is compressed, some bandwidth savings can be accrued. However, implementing this will require router changes. Silence suppression (voice activity detection, or VAD) can further reduce bandwidth requirements, but it should only be used for IP trunks carrying 24 or more simultaneous calls between two sites. Even if silence suppression/VAD is used, assume that less than 35% bandwidth savings will be possible, not the 50% or more that some vendors propose in their white papers. | | | |
| **Quality of Service (QoS)** – QoS should be implemented for WAN connections. DiffServ is the most common QoS that vendors support in their IP phones and gateways. RSVP can also be used, but has lost some of its popularity. Be careful that the QoS is properly assigned in the endpoint and implemented in the routers. Be aware that QoS cannot operate through the Internet, but only on private IP and managed-service IP networks like MPLS. When using MPLS, the voice packet should be given Real Time service, the highest QoS. The highest level of MPLS is usually the most expensive and some MPLS vendors require the enterprise to use the vendor's routers on the enterprise's premises. | | | |
| **Service Level Agreements (SLAs) with MPLS** – MPLS is rapidly replacing frame relay services. The SLAs for MPLS services and the vendor's reports are somewhat limiting for the enterprise's use. Most report the average performance over a 30-day period, which does not provide much visibility into the support of VoIP calls. The enterprise should acquire tools for real-time performance measurements over the MPLS IP trunks used for VoIP. This may not improve the SLA delivery, but it will certainly show where the MPLS performance problems exist and how bad they are for VoIP calls. | | | |

| | | | |
|---|---|---|---|
| **NetFlow/IPFIX Information** – NetFlow, implemented in the Cisco operating system IOS, provides a set of services for IP applications, including network traffic accounting, usage-based network billing, network planning, security, Denial of Service monitoring capabilities, and network monitoring. NetFlow provides information about network users and applications, peak usage times, and traffic routing. IP Flow Information Export (IPFIX) is an Internet Engineering Task Force (IETF) standard based on Cisco's version 9. NetFlow is a network function resident in the routers and should be implemented on the VoIP trunks to monitor performance and usage. There are also several packages available from third-party vendors that should be considered for processing NetFlow information. | | | |
| **Router Modifications** – Routers need to be powerful enough to support the appropriate additions for QoS, NetFlow/IPFIX, security and configuration management. Working with the network engineering staff and considering their long-range plans is strategic to the success of the VoIP implementation. The difficulty will be in determining whose budget will pay for the improved routers; IT or telecom. | | | |
| **Trunk Modifications** – Site-to-site VoIP trunking is less common, but is becoming more important, as VoIP implementations continue. Trunk utilization and QoS need to be policed and managed. Trunk utilization measurements should be measured in 15-minute increments during the voice busy hour. The total utilizations should generally be less than 30% for all traffic if there is no QoS implemented. The IP trunk utilization can be higher with QoS for voice, but should not exceed 50%. | | | |
| **Backup Scenarios** – Backup of the LAN is usually expensive. Power supplies are the most likely component to fail, so dual power supplies are recommended. There should be dual routers with dual WAN connections to each site, if that can be afforded. Another approach is to back up the IP phones with a smaller set of legacy phones connected to the PSTN. As another backup alternative, IP phones that can support analog ports could be connected to the PSTN. PSTN access IP phones are not for production purposes but to provide communications service, called "Lifeline," during emergencies. | | | |
| **Management System Upgrade** – Most IP network management systems do not support performance reporting and troubleshooting well. Therefore, the management systems must be upgraded or an additional performance management package must be procured. | | | |

# PILOT IP PBX CONFIGURATION

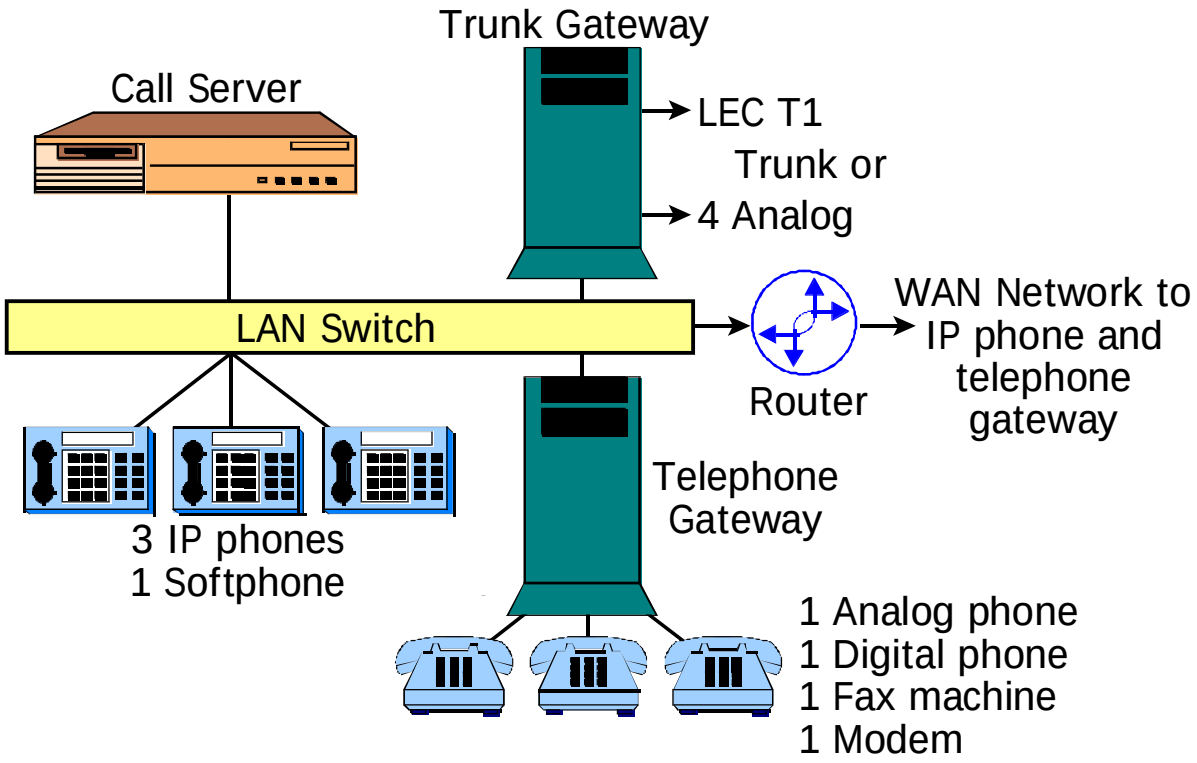


Figure 2

| Best Practices | Evaluated | Acted Upon | Not Applicable |
|---|---|---|---|
| **5. Planning and Testing the Pilot IPT System** | | | |
| **Recommended Configuration** – There is always a cost to pilot a technology. Figure 2 shows the recommended components of a basic IP PBX pilot configuration. | | | |
| **Booting and Registering VoIP/IPT Devices –** The boot times of these devices will vary from vendor to vendor and configuration to configuration. Test to see how long these devices take to boot from a clean start. Test to see how long software downloads to IP phones and gateways could take. Determine the device registration time for the number of IP phones and gateways planned for the network. It can be several minutes long and will increase with the number of endpoints. Perform these tests for locally attached and remotely attached devices over the WAN. | | | |
| **Response to Power Loss –** Shut down the power for the server gateways and phones. Measure the return to service time and note any problems that arise. | | | |

| | | | |
|---|---|---|---|
| **IP Phones** – Work with three different models of IP phones from least to most expensive. The more expensive IP phone models contain expanded features and management and security functions. They will also be the platform for new applications. | | | |
| **Softphones –** Work with a softphone implementation. Run data applications, such as data down and up loads and printing, simultaneously while someone is speaking on the softphone to determine if there is any voice quality degradation. | | | |
| **Gateway Connections –** Gateways connect to legacy devices and PSTN trunks. Test the gateway with both an analog and a digital phone, FAX machine, PC modem and any other device (TDD, alarms, telemetry) that is currently supported by the TDM PBX. These devices do not always work on the gateway. Connect to the PSTN by a T1 or PRI and carry calls to and from the PSTN. If T1or PRI lines are not available use analog trunk connections | | | |
| **Determining Features –** Survey the users to learn what features are presently used. Call centers and help desks have features that others typically don't use. Some executives or their assistants may rely on features that are not commonly known. The pilot system must have these features. Also ask what features are not presently available that would be useful on the new system such as presence, unified messaging and unified communications. | | | |
| **Validating Features –** Test each of the features. Some of the features may be an extra cost, not included in the installed release or version of software and may be non-standard or only available on specific IP phones. | | | |
| **Using Administration –** Practice the administration and management functions. Perform Moves, Adds and Changes (MACs) to become familiar with the procedures. The labor time and complexity will vary by vendor. | | | |
| **911 and E911 –** Connect to the PSTN and confirm that the 911 and E911 services work correctly with the Public Safety Answering Point **(**PSAP). | | | |
| **Applications Connections –** If contemplating a connection to an application server, such as Microsoft's OCS, then that connection will be using SIP for the protocol. This should be tested to ensure it works properly. | | | |
| **IVR Support –** Even though the VoIP call will work, Interactive Voice Response (IVR) may not work, so test several IVR dialogues, including access to voicemail. | | | |
| **WAN Connection –** Locate and test one or more remote IP phones and a gateway across a WAN connection, even though a WAN connection is not in the initial deployment plans. If SIP trunking to the PSTN is to be used, then test the SIP trunk interface and operation. | | | |
| **Who Runs the Pilot –** Voice, data network, desktop and server personnel should be part of the pilot evaluation team. | | | |

| Best Practices | Evaluated | Acted Upon | Not Applicable |
|---|---|---|---|
| **6. Ensuring Secure Operation** | | | |
| **Security Group Involvement** – In larger enterprises, security is often divided into two different groups: network and endpoints. All security groups should not only be concerned with VoIP/IPT security but should be trained in VoIP/IPT technology ***before*** they make decisions that will affect VoIP/IPT security. Security features block or may reduce the call quality. | | | |
| **Data Network Security** – Build a LAN switched, not hubbed, network. Make use of VLANs; one for voice and one for data. Add secure network features to all the VoIP/IPT components. If no calls are allowed through untrusted networks, for example the Internet, configure the perimeter firewalls to block VoIP traffic. Monitor and limit the number of calls over media and trunk gateways. | | | |
| **VoIP/IPT Security Features** – Include security requirements as part of the pilot and RFP processes. Vendors may offer a few or many security features. These features may be options that cost extra and may require mid-range to high-end devices, which are not the cheapest devices to implement the security functions. | | | |
| **Using Encryption** – Several VoIP/IPT vendors offer signaling and speech encryption. Encryption can significantly reduce security problems. Most IP phones can support encryption, but not all softphones can, nor can all gateways. Consider products with Secure RTP (SRTP) standard for implementation. Encryption may not allow third party VoIP devices to operate with the call server because they do not support the original vendor's encryption. Apply encryption whenever and wherever possible. | | | |
| **Firewalls** – If voice calls are allowed to and from and untrusted network, update the firewall to support the signaling protocol in use and dynamic UDP port number assignments. If calls are not allowed, block the signaling and speech ports in the firewall. | | | |
| **Session Border Controllers (SBC)** – The SBC is a firewall alternative for VoIP signaling and speech traffic. It acts as a calling proxy and supports NAT and PAT. It is commonly required for SIP trunk connections. The SBC is primarily a carrier solution and may only be appropriate for larger enterprises. | | | |
| **Software Updates and Patches** – Besides going to the vendor site, go to http://cve.mitre.gov and http://nvd.nist.gov for security patch information. | | | |
| **Server Protection** – Select operating system software that is more secure. Significantly control and limit administrative access. Use strong authentication for administrative access. Maintain the patches. Check with the vendor for server-based security features and what third-party security software is allowed to be resident on the call server. | | | |
| **Gateway Protection** – Look for gateways that support an internal firewall and encryption. Monitor the gateway activity to look for unusual traffic patterns that may be rogue endpoints (phones) or toll fraud. When a security problem is suspected, log all call events on a separate secure server for later analysis. | | | |

| | | | |
|---|---|---|---|
| **IP Phone Protection** – Limit deployment of webphones. Disable unnecessary remote access features. Update default administrator passwords regularly. Prevent local (user) IP phone configuration. Secure the firmware upgrade process. TFTP servers that are used to download firmware can easily be hacked allowing malicious code to be distributed to all the IP phones when they register. Use IP phones with security features. Limit use of web-server access from IP phones. Enable and store the logs of all the call events on a separate server. | | | |
| **Softphone Protection** – Limit deployment of softphones, as these are the most vulnerable of all the VoIP/IPT devices. Require virus and Spyware protection on the PC. Do not delay the PC patches. If possible, do not use softphones at all unless they are well protected. | | | |
| **Vulnerability Testing and Evaluation** – Look for VoIP vulnerability testing tools or services. Run these vulnerability tests at least every three months. There are also tools available that will check the patching status of all VoIP/IPT devices on a daily basis to look for potential vulnerabilities. | | | |
| **Compliance Considerations** – As legislation and regulations increase for IT, they will also increase for voice traffic. If the VoIP/IPT system and network interact with IT systems, check with the auditors to see if there will be any new auditing requirements for the VoIP/IPT environment. This becomes more likely as Unified Communications is added to VoIP/IPT systems. | | | |

| **Best Practices** | **Evaluated** | **Acted Upon** | **Not Applicable** |
|---|---|---|---|
| **7. Organizing for Convergence** | | | |
| **Combining IT and Telecom** – Placing the telecom and all of IT under the CIO is a good start. However, this not enough. The CIO should be briefed on the VoIP technology plus the affects the implementation will have on the infrastructure, TCO, IT/telecom staffs and the end user. | | | |
| **Converged Budgeting** – There will be a cost for infrastructure changes and upgrades for VoIP/IPT. Try to combine the telecom and IT budgets so that budgetary boundaries will not stand in the way. | | | |
| **Cross Training** – Train the telecom staff on VoIP, IP Telephony and IP network infrastructure. They do not need any IP certification. Insist that the IP network engineers and operators attend the VoIP/IPT classes and ***pay attention***. Also have some server, desktop, applications, security and procurement staff attend the VoIP/IPT training. | | | |

| | | | |
|---|---|---|---|
| **Job Descriptions** – In larger combined IT organizations, there may be at least two new or revised job descriptions as follows:<br>1. **Voice Infrastructure Specialist responsibilities:**<br>a. WAN network management<br>b. QoS classification, marking, queuing, policing, enforcement<br>c. Voice/data security<br>d. VLAN administration and management<br>e. Power over Ethernet<br>f. Backup power (UPS)<br>g. Cabling (Cat. 1-6) and electrical signals<br>h. Carrier trunking (T1, PRI, analog)<br>i. Wireless networks (WLAN, cellular)<br>j. Network assessment<br>k. Performance and service level management<br>2. **Voice Applications Specialist responsibilities:**<br>a. Manage all VoIP/IPT servers (call, V-mail, apps)<br>b. Manage call center (ACD, CTI, VRU)<br>c. Support hard IP phones<br>d. Support softphones<br>e. Provide all PBX features and functions<br>f. Support VoIP gateways<br>g. Produce and manage VXML and SALT-enabled applications<br>h. Call quality monitoring and reporting<br>i. Support extension mobility and hoteling<br>j. Integrate application servers (Microsoft LCS, IBM and….)<br>k. Support Unified Communications | | | |

| **Best Practices** | **Evaluated** | **Acted Upon** | **Not Applicable** |
|---|---|---|---|
| **8. Selection and Deployment** | | | |
| **Standards Adherence –** Do not implement VoIP/IPT with proprietary solutions. Select SIP for signaling and G.711 and G.729 for voice compression. There will be non-standard extensions, especially in the feature sets, that may be desirable and cannot be ignored. | | | |
| **Phone Selection –** Two-port IP phones with the desktop connected to the IP phone, then the IP phone connected to the LAN switch, will save on cabling costs and LAN ports. | | | |
| **Backup Operation –** Plan on two servers configured to share the load where one can also provide full backup for the other. Connect the media gateways to PSTN trunks as backup to a failed IP network. For emergency operation, consider IP phones with an analog port connected to the PSTN. | | | |
| **Integrator/Reseller Evaluation –** Ensure the integrator has support for all your locations. Make sure the integrator has the financial ability to handle the size of the planned deployment. | | | |
| **Rollout Sequence –** Start with non-critical departments and legacy devices. Then add PSTN trunking, IP phones, new features and applications and, finally, SIP trunking. Following this order will minimize risks. | | | |

| | | | |
|---|---|---|---|
| **Performance Testing –** Run performance tests to ensure adequate network performance operation for each site prior to deployment. Run tests during the voice busy hour. | | | |
| **Reliability –** Ask the vendor what is not included in their reliability calculations. Request information on the number of patches announced in the past two years to see how often fixes were issued. Have there been any hardware recalls? | | | |
| **Vendor or Third-party Management Tools –** About 50% of IPT systems use vendor-supplied management tools. The other 50% use third-party management tools. Look at those third-party tools because they will usually have better and more comprehensive analysis software. | | | |
| **Phasing Out the Legacy System –** Assume that there will be years of operation with legacy phones, FAX machines and PSTN trunks. Do not eliminate the voice staff and tools that can support these legacy devices and interfaces. | | | |

| **Best Practices** | **Evaluated** | **Acted Upon** | **Not Applicable** |
|---|---|---|---|
| **9. After Deployment** | | | |
| **MACs** – Ensure that the LAN switch can be used to verify and authenticate IP phone Moves, Adds and Changes. | | | |
| **Upgrading the Help Desk** – Train the help desk staff on the operation and problems they will encounter as the enterprise moves to VoIP/IPT. Inventory the functions for which the help desk has responsibility. Create an expanded set of procedures for the help desk to deal with both legacy phones operating through gateways and IP phones. Test these procedures and revise them as necessary. Ask the vendor for information they may have developed for the help desk personnel. | | | |
| **Software Releases, Versions and Patching –** These may require server, gateway or IP phone downtime. Downloading IP phone or gateway software to remote locations can take a long time because of limited WAN bandwidth. Schedule carefully because users assume the voice service is always available. | | | |
| **Troubleshooting Problems** – Develop procedures and train the help desk staff on VoIP/IPT since the problems can be in the network, hardware or software. Problems are therefore much more difficult to locate and resolve. Revise and expand the trouble ticket creation and distribution. Voice quality problems will typically divide as follows:<br><br>**Problem** — **Probability**<br>Echo — 35%<br>Delay — 30%<br>Clipping — 28%<br>Noise — 6%<br>Volume — 1% | | | |

| | | | |
|---|---|---|---|
| **Fixing Performance Problems** – There are several possible methods for increasing call quality. If the call is using voice compression, switch to uncompressed speech. Smaller packets (10ms vs. 20, 30, 40ms) will reduce delay and will also help with packet loss problems. When silence suppression is in use, extend time out at the end of the word or turn off silence suppression. A larger jitter buffer will compensate better when the network jitter is high. However, a larger jitter buffer will increase the latency. When speaking through a softphone, elevate the priority of voice programs in softphones to eliminate interference from resident data applications. Install and enforce QoS for RTP traffic. | | | |
| **Server Connections –** If two servers are acting in a primary/backup configuration, they may not be able to be located far apart (miles rather than 100's of miles), which will not protect the operation from a natural disaster or power failure. Some vendors specify a maximum delay between sites of 20 to 40ms instead of a distance limitation. | | | |
| **Network Performance Assessment –** Data traffic will be constantly expanding. Network performance assessment should be performed every three months to predict congestion and bandwidth problems and to determine traffic trends. For this function, it is better to own the performance tool than to use a consultant. | | | |
| **Use of MPLS –** Multi-Protocol Label Switching is the next WAN service, eliminating Frame Relay. The QoS level for VoIP is the highest and most expensive offered. Most IT organizations are subscribing to the lowest level of QoS and do not recognize the cost for the highest QoS. Determine the price for the highest level before you select a MPLS provider. Another issue is that if the VoIP traffic exceeds the allotted bandwidth, then ***all*** the calls will suffer voice quality degradation, not just the call that goes over the bandwidth limit. To avoid this problem, set up and operate Call Admission Control (CAC) for the WAN MPLS paths. | | | |
| **SIP Trunking –** Plan on SIP trunking to the PSTN instead of T1/PRI connections. If available, SIP trunking is usually less expensive. But be careful: not all SIP trunking interfaces are identical. The interface will depend on the service provider design and the IPT vendor system used. | | | |

## About the Author

**Gary Audin** has more than 40 years of computer, communications and security experience. He has planned, designed, specified, implemented and operated data, LAN and telephone networks. These have included local area, national and international networks as well as VoIP/IPT, UC and IP convergent networks in the U.S., Canada, Europe, Australia, Caribbean and Asia. He has advised domestic and international venture capital and investment bankers in communications, VoIP, and microprocessor technologies.

## About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler at jim@webtorials.com or Steven Taylor at taylor@webtorials.com.

**Published by Webtorials Editorial/Analyst Division**
www.Webtorials.com

**Division Cofounders:**
Jim Metzler
*jim@webtorials.com*
Steven Taylor
*taylor@webtorials.com*