

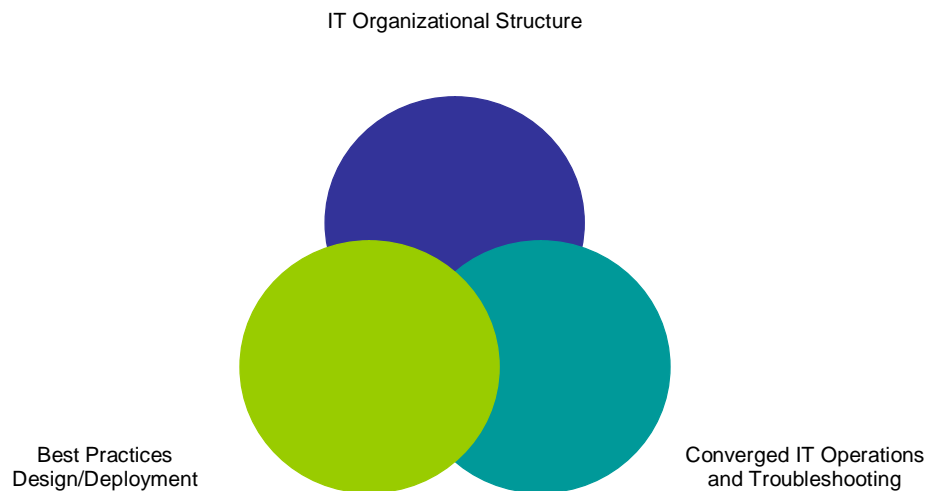
VoIP Networks: The Art of VoIP Troubleshooting

By Stephen Leaden, President Leaden Associates, Inc.
February Issue, Business Communications Review

VoIP Troubleshooting ... The statement conjures up the thought of troubleshooting a traditional TDM-based network, troubleshooting in the traditional voice sense of the word, or fears of the unknown and the changes your organization will require to adapt to such an environment.

VoIP troubleshooting requires a holistic, visionary view of Telecommunications. I am sure you have heard many times from vendors at trade shows: “voice is just another application on the data network”. In fact, it is. Voice packets in an IP world need to be prioritized, and the rules that apply to managing a data network now apply to the voice network as well.

Some individuals think of VoIP Troubleshooting as the end game, as an operational area only. How untrue! The operational phase is only the third phase, in my opinion, of a three-pronged approach to developing a complete VoIP troubleshooting model.



As the above diagram indicates, VoIP now requires a fully converged organization, best practices associated with design and deployment, and converged IT Operations and troubleshooting.

IT Organizational Structure - The Converged Organization

Prior to deploying a VoIP network (WAN and IP Telephony), the IT organization as a whole requires a fresh look at the current organization and skills necessary for a fully supported VoIP model. VoIP is a truly converged environment based on extensive knowledge of LAN, WAN, network management, and security.

A traditional TDM infrastructure runs parallel to the data infrastructure; the converged environment is exactly that, converged. Separate networks for switched voice and packet data are now combined using packet technology. Companies now must migrate from parallel, independent teams to fully converged teams that support together both the voice and data infrastructure.

New processes and procedures must be developed around such a converged environment. Organizational models will vary, but the converged network should include disciplines from the following areas:

- The data network group – brings the data expertise and current data infrastructure baseline environment together
- The voice network group – brings the telephony environment, applications, carrier-related functions, and carrier billing to the network
- The project management group – facilitates deployment of the overall converged network and manages the details associated with the successful migration
- The operations group – brings the ongoing support elements and processes to the network and ongoing management of servers and VoIP applications
- The help desk group – brings the help desk function, now cross-trained for voice and data troubleshooting and is supplied with the necessary tools to support such an environment.

It is critical, within all of the group functions listed above, that cross training and cross-involvement of all voice and data disciplines be presented to the groups at every opportunity.

Finally, change control/change management is the largest change in the organization and will require the ability to track and monitor all system changes and determine if such a change has impact on other devices on the network. Regular monthly meetings discussing any changes pending within the quarter will help facilitate this function.

Best Practices Design/Deployment

The single, most practical way of troubleshooting today's VoIP network is to avoid the trouble to begin with. Developing a network design that is resilient, redundant, and cost effective provides this ability. One should consider a five 9s (99.999%) uptime approach wherever possible when designing the new network.

Traditional TDM PBXs are built around a five 9s model (99.999%), or an outage of less than 5 minutes per year, while WANs are commonly built around a three 9s network, or less than 9 hours annually. The difference is significant. Dial tone is a God-given right and is "always on". To manage a network to less than this is an attempt to change business culture, a significant feat, at best.

The newly converged network must live up to the challenge of a converged environment that approaches the five 9s model wherever possible.

In order to prepare for a VoIP-enabled network deployment, a VoIP Assessment first needs to be performed. This will identify the current environment and network goals, including at least the following:

- Review of the current switch/router environment
- Review of current and planned data network for topology and bandwidth
- Evaluation of policies related to possible security vulnerabilities
- Determination of acceptable level of risk in relation to cost
- Consideration of the physical environment in terms of vulnerability to break-ins
- Use of VoIP assessment tools to identify bandwidth and segmentation needs for the end-state network

When designing the converged network infrastructure consider:

- *Upgrade or replacement of routers, LAN switches* - Upgrade or replacement of routers, LAN switches as necessary to accommodate QoS (switches, routers), PoE (switches), Layer 3 protocols, multiple VLANs
- *Centralized vs. decentralized models* – consider centralized or decentralized voice mail, voice servers/CPU's, PSTN at each site, and Unified Communications,
- *Security measures* – VoIP-enabled networks are subject to the same issues a data-only network has. Be sure to include in the security measures:
 - o Access Control Lists (ACLs) and voice-enabled firewalls and intrusion detection/prevention systems, ensuring that system access is restricted to eligible users.
 - o For Virtual Private Network (VPN) remote worker applications, encryption technologies need to be identified across the enterprise.
 - o Network Address Translation (NATs) hide actual IP addresses, and strong authentication is used to secure VoIP gateways. NAT requirements will vary depending on the manufacturer used.
- *Traffic engineering* - Traffic engineering that will properly design the total amount voice and video port allocation and bandwidth per site, based on traffic engineering models, bandwidth-related characteristics, busy hour, expected growth, and seasonal variation requirements, anticipated data bandwidth for nightly back-ups, peak file transfer periods, and other requirements for proper design of the network total voice and data bandwidth requirements,
- *The CODEC to be used* – You will need to determine at the LAN and WAN levels the CODEC(s) to be used – choose primarily between best quality and best speed that will match to your network goals and bandwidth requirements. Consider half-duplex vs. full duplex (recommend full duplex for best use of bandwidth) and the highest possible Mean Opinion Score (MOS score). Common CODECs and associated MOS scores include:

Codec	Default Data Rate	Default Datagram Size	Packetization Delay	Default Jitter Buffer Delay	Theoretical Maximum MOS *
G.711u	64 kbps	20 ms	1.0 ms	2 datagrams (40 ms)	4.4

Codec	Default Data Rate	Default Datagram Size	Packetization Delay	Default Jitter Buffer Delay	Theoretical Maximum MOS *
G.711a	64 kbps	20 ms	1.0 ms	2 datagrams (40 ms)	4.4
G.729	8 kbps	20 ms	25.0 ms	2 datagrams (40 ms)	4.07
G.723.1 MPMLQ	6.3 kbps	30 ms	37.5 ms	2 datagrams (60 ms)	3.87
G.723.1 ACELP	5.3 kbps	30 ms	37.5 ms	2 datagrams (60 ms)	3.69

MOS – Mean Opinion Score (ITU P.800) - 4.0+ is considered toll-quality speech.

The two most widely used CODECs include G.729 (best speed) and G.711 (best quality). You should allocate at least 30k with header per voice channel using a G.729 CODEC, and at least 80k using a G.711 CODEC at full duplex.

- *Data network topology and structure* - Data network topology and structure, such as MPLS, ATM, frame relay, or an Internet-based IPVPN network. It is particularly important to use a network topology that provides QoS. Note that IPVPNs provide best effort only and typically cannot be attached to a QoS-based SLA.
- *Features/technologies to be deployed* - Features/technologies to be deployed should include, but limited to:
 - o Standard telephony features
 - o Contact center features & Web Agents
 - o Integration of all voice, FAX, and e-mail messages in a centralized environment
 - o Network Management
 - o LDAP directories, nodal and network element management, SNMP, and traffic reporting
 - o Web-based administration
 - o IP audio conferencing
 - o IP videoconferencing
 - o Unified Communications for converged desktop, presence, IM/chat, MS Live Communications Server, other
 - o Network number portability
 - o Simplified network routing
 - o Softphones
 - o Remote hop-offs
 - o Remote offices, remote workers
 - o Virtual office applications
 - o IP trunking

- Centralized control of soft move and changes, reducing ongoing costs considerably.
- *UPS requirements* – PoE is now a local closet concern rather than a centralized power concern (TDM). Many larger TDM environments ensure uptime of at least 4 hours (in the event of a power outage) with battery back up. The new, localized PoE environment should match (or exceed) the current environment using the appropriate UPS. Electrical and HVAC requirements may need modification in line with this as well.
- *Network Management Tools* – one of the most critical components in the design of the new/upgraded network is robust network management tools. Some of the tools are native to the manufacturer (Cisco for example), while other products are third party and provide specific tools and data to help facilitate the converged voice/data network. Some of the third party manufacturers include NetIQ Chariot/Attachmate, HP Openview w/VoIP Probe, Empirix Hammer, Fluke Enterprise LANMeter, and Finisar Explorer among others. Tools should be able to provide fault management, configuration management, performance management, and security management among others.

Don't underestimate the importance of tools like these – data network-only tools will only provide data-centric information and will not provide the ability to isolate VoIP-related problem areas quickly. Tools can either be purchased or provided as a managed service by the chosen carrier.

Network management tools should thoroughly measure all end-points on the network and measure for availability, latency, packet loss, and jitter and perform traditional network management functions such as auto-detect of network devices, continuous ping, trace route, DNS lookup, network scans, and SNMP. Below you will typical SLAs required to maximize voice quality on a VoIP network over the WAN infrastructure that should be measured as part of the network management model:

Requirement	Description	Parameter, etc
Availability	Percentage of IN uptime on the annual basis	= or > 99.9%
Latency	Allowable packet delay	< 120 millisecc.
Jitter	Variations of the packets delay	< 3 millisecc. (ITU G.825)
Packet Loss	Packets not correctly formed packets presented to the IN at demarc.	For VoIP: < 1%. Data packet loss will vary depending on CoS.

- *Network Health Check* – ALL VoIP network implementations require a network health check – different tools have different requirements – all will test the network and populate simulated voice traffic to check the health and readiness of the network. The results of a network health check will indicate any areas where there is a network deficiency and will grade each site tested for appropriate MOS scores. Any MOS score at 3.9 or above will pass the acid test and will provide acceptable voice quality.
- *Deployment for sniffers, TFTP servers and syslog servers at all sites* - Deploy sniffers, TFTP servers, and syslog servers at all sites to measure UDP and other traffic populating the network. Sniffers can be deployed to mirror specific voice-affiliated LAN ports or entire PBXs and can measure IP traffic within a specific period. The type of traffic populated during a network event can be better isolated using sniffers at all critical corporate sites.

Ethereal is one example of an open-source protocol analyzer software tool, and is available for a free download (www.ethereal.com) and can monitor these packets using a stand-alone PC. Ethereal runs on all popular computing platforms, including Unix, Linux, and Windows.

TFTP servers are used for storing configuration files and software images for network devices. Routers and switches are capable of sending system log messages to a syslog server. Both facilitate the troubleshooting function when problems are encountered and can be used to perform a root cause analysis (RCA) when required.

- *The chosen manufacturer and channel partner(s)* – Using an RFP with key specification and question criteria, you will be able to identify the SLAs, knowledge, certifications, knowledge base, geographic presence, partnership status, and escalation procedures for troubleshooting and getting to root cause quickly. Questions to consider:
 - o How many IPT systems has the channel partner installed?
 - o What level of distribution is the channel partner (Silver, Gold, Platinum etc.)?
 - o What is the profile of the engineering and field staff and what credentials/certifications do they carry?
 - o What is the channel partner's strategy for deploying VoIP across multiple sites consistently to the manufacturer's standards?
- *Staff Training* – staff training and cross training voice-to-data and data-to-voice is critical in a converged network model. Certification in specific technical disciplines is highly encouraged over time.
- *Other considerations* - Other considerations to include when design the VoIP network include:
 - o Redundant or back-up WAN links
 - o Disaster Recovery models – LAN, WAN, PSTN, virtual office, IP phone reroute to second PBX, hot site
 - o Redundant data switches, stacked where possible

- Separate VLANs to reduce the amount of broadcast traffic the IP phone will receive, minimizing network collisions
- A robust IP scheme that includes IP addressing for all voice clients, data clients, servers (voice and data), routers, switches, printers, scanners, other.

Converged IT Operations and Troubleshooting

Last (and finally), the Converged IT Operations group will perform VoIP troubleshooting on an ongoing basis. Network tools will be used in a converged environment and provide automatic notification via e-mail, pager, cell, home phone when network parameters are measured outside the SLAs established by the Network Management team. The following areas should be monitored on a 24x7 basis by the selected tools:

- The IP PBX – The chosen vendor should include Site Event Buffers (SEBs) and will automatically notify the VAR NOC center if any system-related alarm conditions arise (T1 down, CPU down, etc.). NOCs will typically notify the individual on-call when an alarm event “hits”.
- The WAN – The chosen carrier will have the capability of providing network managed services, some of these include VoIP over the WAN. For SLA and network integrity purposes, we recommend such for managing a multi-site network,
- The Network Infrastructure – Network Monitoring Tools identified earlier help monitor for network characteristics, including network availability, bandwidth available, packet loss, delay, jitter.

PEPs and patches updates need to be scheduled on a regular basis to address known issues and prevent new issues from taking place. PEPs and patches should be the same current release on all VoIP PBXs and switches across the network for consistency purposes.

The following table provides problems and whether the problem occurs intermittently, periodically, or continuously (www.voiptroubleshooter.com):

Problem			Problem occurs		
Loss	Jitter	Out of Order	Intermittently	Periodically	Continuously
Low	Low	Low	Grounding problem		Loss Plan
Low	High	Low	LAN congestion	Route flapping	Access Link Congestion
			Access Link congestion	Softphone timing	LAN congestion
High	Low	High	Route flapping	Route flapping	
Low	High	High			Load sharing

Problem			Problem occurs		
High	Low	Low	Link Failures	Route flapping	Bad Ethernet Cable
			Bad Ethernet Cable	Router - RED	Duplex Mismatch
High	High	Low	Access Link congestion	Route flapping	LAN congestion
					Access link congestion

A Couple of Real-World Troubleshooting Examples

- Dropped Calls
 - o Description – Calls drops, gets disconnected during call
 - o Root Cause – Bad T1 card in PBX
 - o Solution – Temporarily shut down T1 circuit and card until replacement arrives; route all calls through second T1 card and analog overflow
- Poor Call Quality for Remote Worker
 - o Description – Broken or choppy speech using remote worker hard phone or softphone
 - o Root Cause – Not enough bandwidth during peak period, remote VPN software and VPN router required fine tuning
 - o Solution – Added bandwidth for remote worker, modified VPN software and VPN router configurations, changed best speech to best bandwidth CODEC.
- No connectivity from IP Phones to IP-PBX
 - o Description - All IP Phones down in the branch office
 - o Root Cause – Bad Layer 3 data switch, key connection cable from PBX to data side connected to switch; all data clients and printers also down.
 - o Solution – Replaced connector cable to similar VLAN port on second switch in stack
- IP Phone reset
 - o Description – IP Phone(s) reset/reboot
 - o Root Cause – Broadcast storm exceeds levels of set tolerance.
 - o Solution – Isolated with sniffer level of broadcast traffic, reviewed VLANs for traffic separation, obtained latest patches for IP PBX and IP Phones that further insulate this issue.

Conclusion

After reading this, you may say to yourself, is this all really worth it? From my personal experience, the answer is a resounding Yes. The outcomes include:

- A converged, functional IT organization, with cross-trained rather than one that is disparate,
- A more robust, more resilient data network capable of handling voice, data, and video in a single IP environment, capable of approaching five 9s reliability,

- More robust network management tools capable of centrally managing and reporting all data and voice components,
- Features and technologies tailored to an IP environment, including remote workers, softphones, Unified Communications, LDAP directories, and IP trunking among others,
- ROI that takes advantage of a converged infrastructure, reduced conferencing costs, reduced long distance costs, efficient soft moves and changes, and reduced costs for remote workers.

The old cliché “failing to plan is planning to fail” could never be more appropriate for a transition such as this. Make sure you plan to troubleshoot VoIP through organization change, and best practices design and deployment, and the troubleshooting process will be a whole lot easier.

Stephen Leaden is President of Leaden Associates, Inc., an independent, objective IT consulting firm specializing in VoIP design and deployment and leveraging financial value derived from newer technologies available. Stephen has been in the IT/Telecommunications field 25 years, and is Past President and member of the Society of Telecommunications Consultants, an ethics based association of independent Telecommunications and IT consultants. Stephen can be reached at (845) 496-6677 or at sleaden@leaden.com.