



Technology Update

# The Top Five Challenges to IP Telephony Success

And How to Overcome Them

**NORTEL**  
NETWORKS™

Implemented properly, Internet Protocol (IP) telephony is the enabler of increased productivity and heightened customer relationships. Running on a converged, application-optimized network, IP telephony now scales to 200,000 users. It spans the entire range from corporate headquarters through regional branches, remote offices and telecommuters.

But there are also challenges inherent in IP telephony such as end-to-end delays, echo and insufficient throughput (to name a few). If IP telephony is not properly engineered and implemented, it can result in lost productivity, frustrated customers and curtailed revenue.

Here is a list of the five principle barriers to IP Telephony Success, as well as proven methods to overcome them:

## Barrier #1 Avoiding the Chasm of the Last 100 Meters

A few years ago, desktop networks were built on shared media hubs using a variety of cabling schemes that incorporated best-effort networking. Today, Ethernet is the norm while wireless LAN usage is exploding. The result: while the backbone may be highly reliable with an abundance of bandwidth, the last 100 meters to the end user at the desktop, laptop or mobile device is often weak.

The prevailing expectations for reliability and security, as set by traditional voice networks, are:

- Always-on dial tone (as a guaranteed service indicator)
- 150 msec one-way delay maximum
- Calls are private
- Calls with high quality of service, and real-time responsiveness - guaranteed

The real measure, then, of the performance of IP telephony systems—and the underlying network—must be how well the above user requirements and expectations are met.

## Have you considered?

High reliability in IP telephony backed up by enterprise-class security can be achieved via switched Ethernet and wireless LANs using the following guidelines:

### A. Structured in-building wiring to the desktop

Category 5 (or better) structured wiring should be used to the desktop. This ensures that high-quality voice can be delivered over full duplex 10/100-Mbpslinks. Structured wiring is also important in meeting emergency 911 needs, which require a correlation between the physical location of the IP telephone, and the location code or ALI (Automatic Location Indicator) database location being sent to the 911 PSAP center.

### B. Dedicated switched Ethernet to each telephony desktop

Only switched Ethernet QoS-enabled switching with dedicated ports to each desktop should be used for IP telephony. Shared-media Ethernet hubs must never be deployed due to packet collisions that will impact voice quality by dropping voice packets. The Ethernet connection, however, could support a soft client in a desktop PC – or separate IP telephone and PC – sharing the port via a three-port QoS-enabled switch. The wiring closet Ethernet switch should be in a secure location to avoid eavesdropping and other security breaches.

### C. IP telephony powering

Power outages pose a serious concern and may have an enormous cost to a business in terms of loss of productive output, loss of work-in-process,

and lost revenue. For certain industries such as health care, even the occasional power outage is unacceptable. In such industries, it is standard practice to provide battery and even generator backup for telephony systems. Powering of IP telephones and the use of uninterrupted power supplies (UPS) can provide increased reliability for IP telephony, matching what can be done over PBX. Powering of IP phones can also ease cabling at the desktop.

### D. IP Telephony over WLANs

Wireless LANs operate over a shared radio spectrum, providing mobility for data devices, IP phones, and PC-based soft clients. Running IP telephony on WLANs must address two key requirements – QoS and security over the radio portion. QoS is being addressed by IEEE 802.11 for WLANs, which will result in an 802.11e standard. However, Symbol Technologies, Inc. has implemented Enhanced Packet Prioritization (EPP) QoS technology in its 11-Mbps AP-1431 Access Point product, which will support 802.11e. EPP prioritizes packet transmissions from access points to mobile units and is very useful for media content (for example, IP telephony and streaming video) that can be prioritized over a heavily loaded access point. As with public wireless hot spots, users of QoS-enabled WLANs should expect less than toll-quality voice some of the time, particularly in busy mobile PC-intensive environments. On the other hand, high quality-voice can be expected in controlled environments such as retail.

Another important consideration with 802.11 WLANs is encryption and authentication. Native security, wireless application protocol (WAP) or use of IP security measures (IPsec) via IP virtual private network (VPN) soft clients in PCs meet the encryption needs for IP telephony and data alike. For authentication, 802.1x and its extensible authentication protocol

(EAP) is the recommended approach.

## Barrier #2 Minimizing Packet Delay, Loss and Jitter

Many enterprises have not implemented any form of QoS. Because of this, the traffic may experience differing amounts of packet delay, loss and jitter. This can cause speech breakup, speech clipping, and pops and clicks – or worse. Even if bandwidth is over-engineered, growth of traffic, rapid changes in traffic patterns and network connection failures may result in impairments that impact IP telephony (such as packet loss and excessive delays).

Fidelity (the clarity of the signal) has improved over the decades as the telephone network has moved to digital operation. Therefore, the industry talks about toll-quality voice as an objective of IP telephony, referring explicitly to the user experience over circuit switched networks. Users want this level of fidelity, and in some cases users will reluctantly tolerate lower levels if they gain sufficient value (such as mobility with cell phones).

In IP telephony, voice packets are transmitted over digital transmission facilities with very good error performance; the percentage of voice packets that contain errors (and are therefore discarded) is extremely low. The fidelity of the voice is dependent on the performance of the coder/decoder (codec) and rate of lost packets. Codecs convert the analog signal to a digitized bit stream at one end of a call and return it to its analog state at the other. While bit rates of 64 kbps have been used for years in digital system, state-of-the-art codecs can deliver acceptable quality voice at bit rates as low as 8 kbps. The occasional lost packet (e.g., one percent) is problematic for telephony, since this only impacts a

short sample of speech; beyond this level, packet loss will be very disruptive to voice communications. Lost packets arise when noise corrupts the packet or —most likely in today's environment—when a switch or router in the path drops packets due to congestion or failure conditions, or when an IP telephone or Media Gateway discards a voice packet that has been delayed beyond some acceptable limit.

Clearly, QoS plays an integral part in the success of any IP telephony implementation.

### Have you considered?

The following guidelines will help you implement QoS uniformly across the network, thereby avoiding these pitfalls:

#### A. QoS via 802.1p/Q

The IEEE 802.1Q standard adds four additional bytes to the standard 802.3 Ethernet frame that provides Ethernet QoS via a three-bit field and a virtual LAN (VLAN) ID. Most Ethernet switches support this standard. Ethernet QoS can be accomplished via the three 802.1p user priority bits, to create eight classes of service for packets traversing Ethernet networks. Ethernet QoS can also be accomplished by prioritizing traffic based on the VLAN ID only. For IP telephony, a binary value of 100 for 802.1p is recommended with both voice bearer and voice signaling. VLANs can be used to separate traffic for ease-of-management and security purposes.

#### B. IP QoS via Differentiated Services

Different types of applications (including IP telephony) have different characteristics and require different types of QoS behaviors to be applied to them at every router and switch along the path. Differentiated Services (DiffServ), for example, defines a number of different QoS

behaviors and their corresponding QoS mechanisms, called per-hop behaviors (PHBs). These PHBs are identified by an IETF-standardized DiffServ control point (DSCP) carried in each IP packet. Even if there is plenty of unused bandwidth available, IP QoS is required, since IP telephony performance may be impacted during times of congestion and traffic peaks and after loss of bandwidth after failures. The simplest approach is to construct two traffic classes – one for IP telephony and the other for best-effort data traffic.

#### C. Nortel Networks Service Classes

End-to-end QoS management can be quite complex. Nortel Networks has simplified QoS by creating standardized, default QoS configurations and behaviors for its products in the form of end-to-end network service classes. These are called Nortel Networks Service Classes (NNSCs). NNSCs have been defined based upon the most common types of applications. They provide default mapping between DiffServ and different link layer QoS technologies that a particular interface uses.

#### D. IP address prioritization

IP telephony traffic can also be prioritized by its IP address. This approach is ideal for devices with statically assigned IP addresses that rarely, if ever, change. IP PBXs, VoIP gateways, and communications servers are VoIP devices that would have their IP addresses statically assigned. Routers and switches can be configured to filter/classify and prioritize all packets originated from IP addresses.

#### E. Switch and router performance

Even under heavy load, routers and switches should provide IP telephony traffic with very low latency. In addition, they should support wire-speed

operation (even with short packets) when packet classification (QoS) is activated. Turning on various packet classification schemes on some software-based routers can have severe impacts on performance, including VoIP packet loss and delay. Routing switch technology with deep packet filtering prevents performance degradation even at Gbps speeds.

## Barrier #3 Putting an End to Unreliability

The telephony world refers to 99.999 percent base system reliability based on a mean time between failure measured in tens of years and redundant common control for large systems. But this metric alone doesn't reflect the realities of most enterprise IP networks.

An IP network may fail in terms of performance:

- If it is 100 percent up, but there are non-hardware failure conditions, such as a remote site, which make being physically connected logically unreachable (perhaps due to routing information protocol hop count limits)
- If it is 100 percent up, but there is congestion in the network resulting in increased packet loss and excessive delays
- If it is 100 percent up, but IP routing convergence after failures takes too long

Consequently, an end-to-end system-level view of IP telephony reliability is a vital necessity.

## Have you considered?

A comprehensive approach to reliability is required in order to meet the expectations of IP telephony users. The following guidelines should be followed in deploying networks, which meet IP telephony requirements as they relate to reliability:

### A. Backbone node reliability and availability

Backbone node reliability and availability should be comparable to availability levels delivered with traditional telephony systems, recognizing that networking techniques can be used to fill the gap. This is achieved by designing switches to deliver the following:

- Very high component MTBF
- Highly reliable, robust base software, and real-time operating system software
- Redundant power, fans and temperature sensors
- Redundant switch fabric and common control with sub-second switchover
- Hot swappable capability of all core system elements
- Automatic short system boot and restart times
- Short software upgrade service outage time

### B. Rapid detection and recovery below Layer 3

A sound design principal is to provide resilience at the Layer 1 level and provide rapid recovery from failures at that level. In this way, link failures can be handled without impacting the Layer 3 routing system. Three technologies play key roles in achieving this:

- Ethernet link aggregation allows multiple 100/1000 Mbps Ethernet links to be configured as a trunk group between wiring closet switches and backbone nodes, and between backbone nodes. Automatic traffic rebalancing takes place if one of the links fails.
- Optical dual ring technologies can provide very high resilience for extended campus and data center environments. These offer 50-ms recovery from failures on a SONET and wavelength basis.

- Resilient packet rings (RPR) is a Layer 2 solution that combines optical ring and Layer 2 technology to provide 50-ms recovery from failures by using a counter-rotating ring.

### C. Dynamic routing over designed networks

Some of the key IP networking standards that enhance fault-tolerant networking include high-performance dynamic routing protocols, protocols for route balancing across paths, and for LAN redundancy. These protocols should be carried over networks that are designed to put an upper limit on the number of routing points between end users. This puts a ceiling on the delay across the network and speeds up routing convergence times.

## Barrier #4 Minimizing Risk on Public Packet Networks

Meeting IP telephony QoS, security and reliability requirements across public packet networks requires special attention. While leased lines are always an option to interconnect sites, virtual private lines using Frame Relay, ATM and, increasingly, IP-VPNs and Optical Ethernet are attractive alternatives. A high degree of flexibility is required in interfacing to public networks for high availability and QoS.

## Have you considered?

The following guidelines apply to real-world IP networks that support IP telephony across the cloud:

### A. Engineering the bandwidth

Typically, LAN bandwidth is inexpensive and is a fixed one-time cost. However, in the MAN or WAN, bandwidth is expensive and results in a monthly recurring cost. QoS allows the enterprise to use expensive WAN bandwidth most cost-effectively. The

bandwidth used for voice calls is dependent on the codecs used and how these are configured for different types of calls. How facsimile is handled also needs to be factored in. Traditional voice engineering methods can be used to determine the number of calls that need to be engineered over the WAN link, factoring in calling communities of interest, the number of busy hour call attempts, and the average call holding time. On under-utilized T3-and-above leased lines, for instance, adding IP telephony traffic uses up available bandwidth. For highly utilized high-speed links and lower bandwidth (T1 or less) connections, though, the amount of VoIP traffic should be limited to a percentage of the bandwidth of the connection. Rule of thumb: for low-bandwidth (less than 1 Mbps) connections, no more than 50 percent of the available bandwidth for voice traffic should be used; for connections more than 1 Mbps, up to 85 percent of the available bandwidth for voice traffic can be used.

### B. Flexible QoS mapping at the WAN edge

Running IP telephony over leased lines leaves QoS and traffic management totally under the control of the enterprise. Support for flexible QoS mapping when working into carrier packet services should be addressed as follows:

- DiffServ, in conjunction with Frame Relay traffic management, is used to provide QoS over Frame Relay networks. In addition, a separate mesh of virtual circuits (VCs) should be established for IP telephony with appropriate committed information rate to minimize interaction between voice and data traffic. The IP telephony VCs should run at a higher priority.

- If ATM is to be used, then IP telephony traffic should be carried over constant bit rate or real-time variable bit rate VCs. These VCs should be sized appropriately. Note that ATM can support both voice and data over a single VC, provided the ATM VC is selected to support the most stringent multi-service application.
- Optical Ethernet provides Ethernet connectivity with support for IEEE 802.1p/Q. The high-speed, low-latency attributes of this service make it ideal for MAN/WAN connectivity among metro sites.
- Using IP-VPNs over the Internet is very attractive for remote access and for connectivity to remote office.

### C. Reducing delays through packet fragmentation

In mixed voice/data IP networks, packets must be fragmented prior to traversing bandwidth limited (less than 1 Mbps) connections to minimize voice delay and jitter. There are several protocols that can be used to fragment packets.

### D. Reliability across the WAN

Extending the reliability of the campus across the WAN can be a major challenge. While IP routing is the last line of defense, lower-layer mechanisms are required to minimize the impacts and failures and meet IP telephony requirements. With serial links, various multi-link redundancy options are available. These provide scalable bandwidth and enhanced reliability.

### E. Secure IP telephony across the Internet

Security concerns of running voice over the Internet can be taken off the

table because all traffic leaving the site across an IP-VPN is authenticated and encrypted. For remote offices, redundant access links and dynamic routing over encrypted tunnels can provide a high level of reliability.

## **Barrier #5 Looking Inward – Organizational Barriers to IP Telephony and Their Implications**

The greatest technologies will not yield the desired result unless they are engineered and operated appropriately. Traditional IP networks evolved from PCs to PC LANs to bridged, and ultimately switched and routed networks. At the same time, applications evolved from e-mail and file transfers to ERP, CRM and now IP telephony and collaboration.

Due to the real-time requirements for IP Telephony and other applications like Video, existing practices and procedures are likely outdated and may have to be redesigned when implementing IP telephony.

## **Have you considered?**

As each new networking and telecommunications technology has come along, enterprises have had to rethink, and evolve their internal procedures and engineering practices. The same holds true for IP telephony. The following guidelines may prove useful in smoothing the transition from best-effort networking to always-on, application-optimized converged networks.

### A. Network convergence drives organizational convergence

Deploying IP telephony solutions on top of a converged network requires a mixture of skill sets, including a good understanding of what the IP telephony end user wants from a feature and performance perspectives. Also, IP telephony application engineering, as well as network engineer-

ing, operations and planning, is required.

### B. Designing the network in line with the business

IT planners must consider networking for IP telephony in the broader context of application optimized networking across the enterprise. They must establish business-driven reliability objectives, as well as security and QoS policy management directions. For example, they must establish levels of network redundancy that are affordable and justifiable to meet business needs.

### C. Operational evolution

Enterprises need to establish operational procedures that recognize the transition from best-effort networking to always-on, application-optimized converged networks. Scheduling maintenance windows and avoiding equipment resets as the first step for fault recovery are but two examples of areas that need to be addressed.

### D. SLA management for converged networks

The increased reliability and performance requirements of converged networks put added pressures for the establishment of strong SLAs with service providers. Once established, there is a need to validate that these commitments are being met. This requires a combination of management tools and reporting, and a real-time window on how the network is performing.

### **For More Information:**

To obtain a copy of the white paper, "Designing Converged Networks For IP Telephony," or to find out more about Nortel Networks IP Telephony and convergence solutions, contact:



26610 Agoura Road, Suite 210, Calabasas, CA 91302

<http://www.nortelnetworks.com>

Copyright © 2003 Nortel Networks. All Rights Reserved. Nortel Networks, the Nortel Networks logo and the Globemark are trademarks of Nortel Networks. Information subject to change without notice. Nortel Networks assumes no responsibility for any errors or omissions that may appear in this document. Printed in the USA.