

I D C E X E C U T I V E B R I E F

Managing Data, Voice, and Converged IP Networks

January 2004

Adapted from *Worldwide IP Data Network Configuration Management Forecast, 2002–2007*
by Elisabeth Rainge, IDC #29608

Introduction

New technical capabilities are useless to your employees without the infrastructure to support them. Therefore, many companies are adding capabilities such as voice over Internet Protocol (VoIP), IP telephony, conferencing, data integration, and rich media to their networks. These applications increase the load on networks, but this load cannot be measured just in megabytes. There are also increased demands in terms of:

- **Real-time communications.** Latency is acceptable for email, but not for voice communications and conferencing.
- **Business continuity.** As more important data moves across networks, companies need to preserve that information and ensure quality of service (QoS) if the network goes down.
- **More diverse networks.** The combination of traditional wired networks, wireless LANs (WLANs), and broadband to home and branch offices adds new layers of complexity in terms of management and interoperability.

Companies are trying to take care of all these needs on a budget while still taking advantage of existing investments. This will require a great deal of network planning and management in order to keep costs down while maintaining uptime. Diverse networks populated with diverse applications create unpredictable problems and also raise concerns around compatibility and peak network capacity.

Reaching these goals will require a comprehensive IP network maintenance plan. Most companies that have large networks are familiar with the basics of configuration and management. Moving forward, companies must have a maintenance plan that projects these basic concerns across their growing needs, ensuring uptime in the present and increased capacity in the future.

Modern Network Loads

Advanced Applications

This category includes:

- **VoIP** allows users to access voice communications over the Internet or other computer networks. It can offer significant cost savings by allowing companies to avoid long distance charges that come with standard telephone calls.
- **IP telephony** is a subset involving the use of IP PBX hardware or media gateways that can communicate with traditional telephone systems. IP telephony systems are generally designed to replace all the features of a traditional telephone; most also add a suite of other functions as well.
- **Advanced conferencing, scheduling, and collaboration** are becoming a major part of daily business life. Unifying voice and data communications can allow users to interact in new ways and from new locations. These applications are a driving force behind the move to converge voice and data onto the same networks.
- **Rich media** use is increasing, especially audio and video streaming for conferencing, training, and other functions.
- **Unified communications (UC) and unified messaging (UM).** These tools allow users to manage voice, email, Web, and fax communications and make these types of communications available through both speech and traditional desktop user interfaces.
- **Training features.** Many organizations are seeking to improve training while saving money by using their networks to support training needs. Important training features can include low-bandwidth uses such as text and higher-bandwidth items such as audio, video, interactive testing, and conferencing functions.

Needs

Such advanced applications place demands on networks, including:

- **Greater overall bandwidth.** Voice and rich media take up more room than email and basic Web traffic. But merely adding bandwidth tends to be simple compared to other demands.
- **Real-time interaction.** VoIP, conferencing, and rich media have little tolerance for latency or dropped packets, which quickly degrade their quality to levels that make them useless.
- **Support of external users.** Perhaps the main driving force behind unified communications and other advanced communications applications is to provide support for mobile and remote employees. Furthermore, many companies are using conferencing and collaboration to improve interaction with

customers and partners. Supporting users outside the network who log on from different platforms and connection types places demands on the network in terms of flexibility and interoperability.

- **Increased backup and recovery needs.** As companies do more business — and more important business— across their networks, the need for uptime increases. The penalty for information lost due to network crashes also increases. Companies must make sure that they have up-to-the minute storage of networked transactions and collaboration.

Networks

Organizations must offer new applications and capabilities to users who are connecting across increasingly diverse networks. Diverse network environments can create interoperability problems and also demand a wider range of IT skills to maintain. Modern organizations will typically find themselves managing more than one of the following environments:

- **IP virtual private networks (VPNs).** IP VPNs are rapidly growing WAN technology that are replacing frame relay as a standard for wired network technology.
- **WLANs.** WLANs provide wireless peer-to-peer and point-to-point connectivity within a building or campus environment. They are increasingly being used as an alternative to wired networks, especially in new offices, branch locations, or large worksites.
- **Broadband** access to branch or home offices. As companies open more locations and support more home office workers, they will increasingly deal with cable, DSL, and other forms of consumer-level Internet connections.
- **Optical infrastructure.** Many companies are investing in next-generation optical infrastructure. Overall revenue and growth prospects are highest in multiservice provisioning platforms (MSPPs), metro dense wavelength-division multiplexing (DWDM), and optical cross connects.

Considerations

Companies must address all of these issues in the face of several complications, including:

- **Cost savings.** Most organizations do not have large amounts of money lying around available for network upgrades, let alone building the perfect network from the ground up. Instead, IT departments are tasked with creating smoothly running networks by joining existing investments. These previous investments often involve diverse, incompatible technologies.

- **Complexity.** Companies are looking to improve usability for end users and simplify maintenance for IT staff. In fact, many companies overbuilt capacity during the 1990s and are now trying to get a handle on their network resources. Many firms have also found themselves in possession of overly complex, multivendor environments due to mergers, acquisitions, or downsizing.
- **Uptime.** Minor network downtime may be a minor inconvenience for traditional Web or email use, but even momentary outages mean dropped calls when it comes to IP telephony. Even the occasional dropped packet of delay quickly makes IP telephony applications useless.
- **Quality of service (QoS).** While companies have many types of applications they must run over their networks, IP telephony is one of the most important and, in some ways, the most complex. Providing QoS starts with ensuring voice quality, but it plays into every aspect of the system, from testing to ensuring there is adequate network hardware. It should also involve a human element, determining how to best design the applications to support how employees will actually use them.
- **A highly fragmented service provider environment.** Companies will have a hard time finding a single provider that can offer a wide variety of services. Companies looking for outsourced services may have to seek separate providers for network support service, VoIP, and unified communications.
- **IP telephony challenges.** Organizations must address compatibility and interoperability issues among IP telephony products and solutions in multivendor environments as well as the challenges of configuration and administering IP telephony.

Designing the Network

Whether or not they are using services through a provider (such as VoIP or UC), many organizations are seeking outside help in keeping their diverse networks up and running. Whether they do so in-house or via a service provider, companies must address a wide range of network maintenance activities.

Network Configuration Management

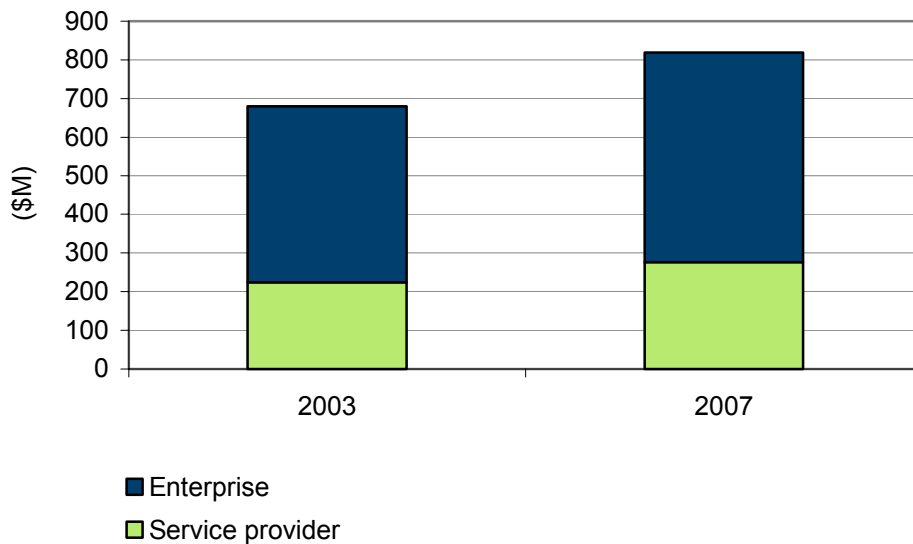
IP data network configuration software plays the dual role of strengthening customers' connection to their existing infrastructure and showing customers how the infrastructure can be modified to meet future needs. It represents a fast-growing network maintenance activity with a growing proportion of services going directly to enterprises rather than service providers (see Figure 1).

Important network configuration management tasks include:

- **Network element management.** These services help manage the various devices and assets on the network via device notification, configuration, policy, and performance information.
- **Network design and simulation.** These tools include discovery and documentation applications that are popular for their inventory capacities and technical modeling tools that are striving to gain relevance by analyzing real-time data.
- **IP address management.** These applications help companies keep track of their IP properties and find vulnerabilities of domain network services (DNS). They also help optimize networks and integrate DNS and Dynamic Host Connection Protocol (DHCP) tools.

Figure 1

Worldwide Network Configuration Management Revenue by Customer Type, 2003 and 2007



Source: IDC, 2004

Design and Implementation

Even if organizations cannot afford to build the ideal network, they can still engage in the following process to assess their network readiness:

- **Design and planning.** Organizations must create a detailed network plan, addressing both current and future needs. Such a plan must take ongoing work and testing into account, ensuring adequate network resources even during upgrade periods.
- **Testing.** This phase addresses not just overall network load but traffic spikes as well as interaction between different applications. The idea is to measure the network against likely usage.
- **Implementation of upgrades.** This phase must occur according to a carefully devised schedule that does not interfere with the day-to-day business of the company.
- **Fault and performance management.** Moving forward, the network must be able to route around problems and maintain fast throughput even when under heavy loads or hostile network attacks.
- **Security management.** Modern, heterogeneous networks can be difficult to secure. Security procedures must address standard security needs as well as the interaction between diverse networks and potential new security holes opened by new applications.
- **Training and certification.** Staff must be trained to use the new network. Training is particularly important for IT staff members who must support the network going forward, especially if they must be certified in new technologies.

Network Maintenance

To make sure that performance is maintained across a global, diverse network supporting advanced communications and multivendor technology platforms, companies must ensure a network support infrastructure that addresses:

- **24 x 7 coverage.** Increasingly, corporate networks will have users all over the world. There is no appropriate hour for downtime.
- **Rapid response times.** Any problem that requires more than two to four hours to fix is considered disastrous by modern standards. The maintenance plan must include ongoing measurements, including a specific mean time to repair.
- **Heterogeneous network support.** Diverse networks can present diverse problems. The maintenance plan should include capability to troubleshoot and isolate network troubles across the network layer to help ensure network availability, along with fast support for every type of network technology that a client may have in use.

- **Remote diagnostics and support.** While companies open numerous branch offices and spread across the globe, many still keep their IT staffs centralized. Remote management and automated diagnostic tools can allow rapid resolution and response via the network itself, often preventing the need for an onsite visit.
- **Multiple support delivery.** Most organizations are seeking to save money and improve response times by offering support via email, text chat, Web-based FAQs, and even VoIP. Companies are also enabling case tracking, product and service release notes, online discussion forums, certified solutions, personalized Web services, and natural language support tools.
- **Predictive/preventive maintenance.** These services include inspections, testing, checkups and other tasks intended to divert problems before they happen. These tools also help ensure greater reliability/availability for mission-critical operations as well as proper application configuration of servers, gateways, and endpoints.

Physical Network Support

For physical network support of both hardware and software, companies must ensure:

- **Onsite support.** Demand for traditional onsite services will continue to grow, though over time remote services and predictive support will head off much of this need. The need for onsite support will persist because onsite engineers will continue to perform basic support tasks such as hardware replacement, physical inspections, and board swap-outs .
- **Inventory and asset management.** These services ensure that necessary parts are available to address diverse network environments. They can also provide centralized warranty and contract renewal tracking.

Conclusion

Corporate networks can no longer be measured in megabytes per second in throughput. Rather, organizations must think about the particular applications they want to support and then determine the specific needs of these applications in terms of real-time interactivity, extra bandwidth, and other complex concerns.

Even if companies cannot build the perfect network, they should test their existing network against these needs and make focused upgrades. This task can include working with outside providers, even if only on certain aspects of the network infrastructure.

COPYRIGHT NOTICE

The analyst opinion, analysis, and research results presented in this IDC Executive Brief are drawn directly from the more detailed studies published in IDC Continuous Intelligence Services. Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. Contact IDC Go-to-Market Services at gms@idc.com or the GMS information line at 508-988-7610 to request permission to quote or source IDC or for more information on IDC Executive Briefs. Visit www.idc.com to learn more about IDC subscription and consulting services or www.idc.com/gms to learn more about IDC Go-to-Market Services.

Copyright 2004 IDC. Reproduction is forbidden unless authorized.