

# IP VPNs—Meeting the Network Challenges of a Distributed Organization



www.yankeegroup.com

by Zeus Kerravala | December 2007

## Executive Summary

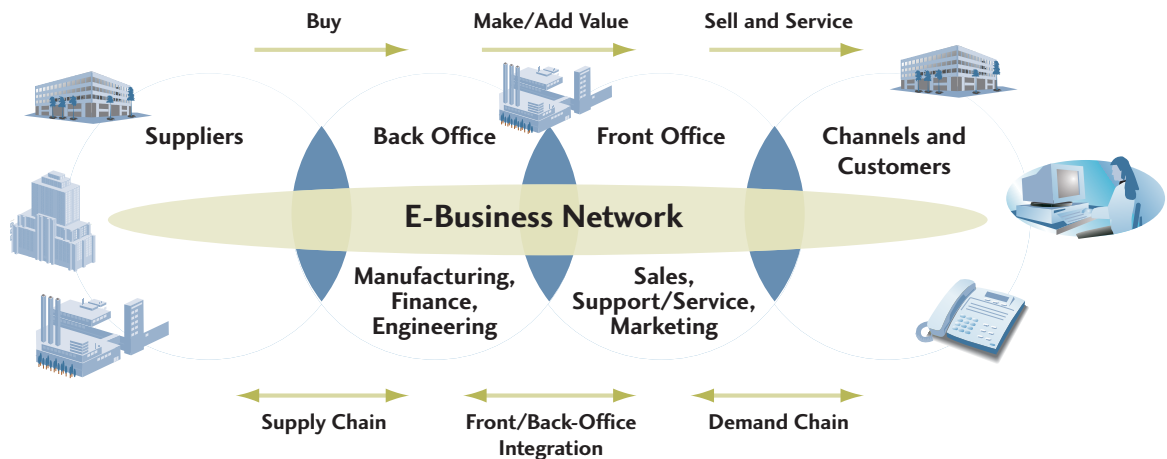
With the widespread adoption of broadband access services, such as cable, DSL, wireless and satellite, distributed organizations are seeking ways to support broadband access at branch locations, secured by VPN technology. The challenge is to provide flexibility and high-speed access at the branches and maintain centralized control at a reasonable cost. Accomplishing this will deliver value to every constituent in the extended enterprise's value chain (see Exhibit 1).

Broadband-based VPNs can provide the much needed network flexibility, security and resiliency that companies require but at a lower cost than a comparable Layer 2 service, such as frame relay and asynchronous transfer mode (ATM). Organizations have an array of VPN choices for managing and deploying a VPN. A managed broadband-based VPN can deliver the reliable, secure access that distributed organizations need—at 50% of the cost of traditional network solutions.

## Exhibit 1

### The Extended Enterprise

Source: Yankee Group, 2007



This custom publication has been sponsored by MegaPath Networks.

© Copyright 1997-2007. Yankee Group Research, Inc. All rights reserved.

This Yankee Group Report is published for the sole use of Yankee Group clients. It may not be duplicated, reproduced or transmitted in whole or in part without the express permission of Yankee Group, Prudential Tower, 800 Boylston Street, 27th Floor, Boston, MA 02199. For more information, contact Yankee Group: info@yankeegroup.com; phone: 617-598-7200. All rights reserved. All opinions and estimates herein constitute our judgment as of this date and are subject to change without notice.

## Table of Contents

- I. Introduction: The Network-Enabled Enterprise ..... 2
- II. The Networking Challenges of Distributed Organizations ..... 3
  - Legacy WAN Technologies ..... 3
  - The Broadband Explosion..... 4
  - Broadband Aggregators ..... 4
- III. Defining VPNs ..... 5
  - CPE-Based DIY IP VPN ..... 5
  - Network-Based IP VPN Service ..... 6
  - CPE-Based Managed Broadband IP VPN ..... 6
- IV. Conclusions ..... 7

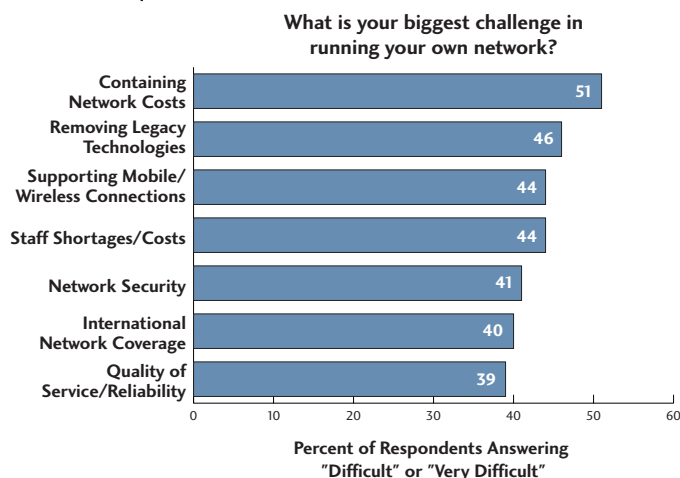
### I. Introduction: The Network-Enabled Enterprise

Today’s enterprises are distributed, networked organizations that feature an increasing number of branch offices, mobile workers and remote locations. The ability of every worker and location to effectively communicate and share information has a direct impact on the value of the organization’s product or service. Therefore, CIOs place a high priority on networking technologies that enable them to broadly deliver new applications, improve efficiency, increase user productivity and simultaneously reduce communication costs and deliver a clear return on investment (ROI). A recent Yankee Group survey shows that containing networks costs ranks as the number one challenge organizations face in running a network (see Exhibit 2).

#### Exhibit 2

Organizations Have Difficulties Containing Network Costs

Source: Yankee Group 2007



As the role of the network has become more important, so has the role of the CIO. CIOs are no longer isolated in an IT department; they are part of the business team and must think about business first and technology second. Cost reduction is one of many critical business drivers forcing CIOs to look at alternate forms of network architectures. In addition to cost control, CIOs must adapt to the following trends:

- **Increasingly distributed enterprises:** Organizations are opening more branch locations so they can reach more customers and increase revenue. This means they need to distribute corporate applications and information to these branch locations. In the past, access to centralized applications from branch environments has been inconsistent. Applications were either not available or performed poorly. According to the Yankee Group *Anywhere Enterprise—Large: 2007 US Mobility and Business Applications Survey*, the biggest challenge organizations face managing collaborative projects is delivering the same applications or application experience to remote employees. Today, the network must be able to distribute information and applications to every worker in every location.
- **Increased use of remote access and telecommuting:** Approximately 40% of enterprise employees work outside the corporate headquarters. Corporations need to provide the infrastructure that can scale to accommodate this growing number of remote workers. Users need access to corporate information regardless of location.

- **Enhanced security:** Moving to a more open network environment where extranets and remote access can be provisioned quickly introduces security vulnerabilities. Network managers need to ensure that security is not compromised for the sake of open access and network simplicity. Additionally, they need to deliver improved security without committing high-priced IT staff to each remote location. Organizations can't afford a decentralized approach to managing technology at branch offices.
- **Better use of network resources:** The traditional hub-and-spoke environments used by most companies today are inefficient because the majority of corporate traffic is backhauled through a central location. Next-generation networks need to be architected to make better use of network resources.
- **Distributed applications:** The migration to client/server-based applications has given rise to a number of IP-centric applications, such as Web 2.0 programs, CRM systems and e-mail. Organizations have adopted these types of applications for their flexibility and ease-of-deployment compared to legacy-mainframe-based applications. As companies continue to develop more IP-based applications and become more reliant on the distribution of them, network connectivity and network agility will grow in importance.

Organizations require a network infrastructure that can seamlessly and securely connect multiple branch sites, mobile users, business partners, customers, suppliers and other members of their extended enterprise. VPNs give organizations the flexibility to deliver this expansive and secure connectivity. However, not all VPN architectures and solutions are the same. The costs, management requirements and access methods can vary considerably.

Many organizations have tried to deploy VPNs on their own using routers or specialized VPN concentrators. Network managers have found that, due to the amount of operational overhead and network management tasks, deploying this type of solution can be complex and significantly more expensive. A compelling alternative is a managed broadband-based VPN service. A managed broadband-based VPN service can meet the necessary business challenges at a much lower cost. In addition, a service that not only manages routers but includes design services, ordering, procurement and other functions of the VPN management lifecycle has a compelling benefit: It can reduce most, if not all, of the perceived risks of a migration to a managed IP VPN service.

## II. The Networking Challenges of Distributed Organizations

Secure connectivity is a challenge for any distributed enterprise, but certain vertical industries that rely on remote locations for their success feel the pain most acutely. Retail, financial services, life sciences and healthcare are just a few examples where secure access from branch offices to corporate IT systems is critical to business success. As businesses needed to connect and deliver applications to more remote locations, they deployed WANs. In the early days of the internet, these corporate networks grew into hybrid public and private IP networks that supported increasingly critical business processes. To extend the reach of applications, companies leveraged legacy technologies, such as private line, frame relay, dialup service, ATM and even satellite services. Each of these legacy technologies has its own strengths and weaknesses.

### Legacy WAN Technologies

A private line is a leased access circuit from a carrier or ISP. Because it is a direct point-to-point connection between two locations, it is a high-performance solution. Organizations also perceive private lines to be very secure, since they are dedicated for their use rather than shared. The high level of security is more perception than reality, since the network can be compromised by tapping the physical line.

The chief drawback of private lines is their expense. Because private lines are dedicated infrastructure, they are, in most cases, the most expensive form of WAN connectivity. Private lines also provide very little design flexibility, and redundancy is difficult and expensive to build in. Lastly, since it is a point-to-point connection, there is still no support for remote and mobile users.

### Frame Relay and ATM

Frame relay offers a less expensive alternative to private lines by leveraging a service provider's frame relay network. A service provider delivers connections between locations with virtual circuits within the frame relay network. This costs less, since it is a shared infrastructure. It's also reliable, since the frame relay service provider can reroute traffic in response to network outages.

Although frame relay is cheaper than private line, it can still become very expensive as an enterprise scales. In a meshed environment, adding new sites can be very difficult since each site requires its own permanent virtual circuit (PVC). The entire process requires a lot of coordination between the enterprise and the frame relay service provider, creating a management burden and adding significantly to the cost.

ATM uses the same virtual circuit concept as frame relay but provides a higher level of service quality. It's a better choice for high-bandwidth applications. However, it's more expensive than frame relay and has similar management and architectural issues.

## Dialup

Retail organizations in particular use dialup services to connect each retail location with the corporate headquarters. Each time a consumer's credit card is swiped at the point of sale (PoS), the terminal uses a dialup or satellite service to check the consumer's credit and post the transaction. The retail location uses the same dialup for other tasks, such as uploading the day's transactions and updating inventory. This access method has considerable disadvantages.

Dialup is very low bandwidth and limits the applications that a retail location can deploy. Even if headquarters uses a service provider for a centralized dial plan, it may not reach every location. This increases the number of vendors needed to provide coverage, increasing the costs and administrative burden. Lastly, dialup service is not an always-on connection. This also limits applications.

## The Broadband Explosion

The explosive growth of broadband services has transformed how organizations connect their branch locations. Today, each branch location can subscribe to a local broadband service provider. Retail stores, bank branches and small offices can subscribe to cable, wireless, satellite or business DSL services. This has tremendous benefits for the branches and the entire organization. Broadband delivers high-speed, always-on access, something dialup users did not have. This enables organizations to deliver more content and deploy more sophisticated applications. In addition, sites can order broadband service and have it provisioned quickly. This enables the

company to add new sites much faster than they could with frame relay. These benefits and increasing reach and availability of services is driving rapid adoption of broadband. It has the potential to transform how organizations and their branch offices communicate and share information.

Broadband is a compelling alternative for branch office connectivity, but it also creates a unique challenge for network managers at the corporate headquarters. Using frame relay or ATM had its drawbacks, but network managers had centralized control. Now, each branch location can choose its own broadband service provider. In some instances, a network manager could be responsible for hundreds of branch locations and dozens of different providers. Trying to maintain a consistent and secure corporate network can become costly and very complex.

## Broadband Aggregators

As attractive as broadband is from a cost perspective, the complexity of managing dozens of broadband provider relationships diminishes the value of any cost savings and may lead to a higher total cost of ownership (TCO) after all the operational costs are factored in. A service provider that could act as an overlay or aggregator on behalf of the customer and manage the installation and implementation from end to end would allow the enterprise to gain the cost benefits of a broadband-based VPN service without enduring the escalating operational expenses.

When corporate WANs didn't have to service a distributed, dynamic organization, older WAN technologies were sufficient, if not ideal. Private line and frame relay promised network and communications managers dedicated bandwidth and predictable performance. Network managers perceived it to be secure and reliable. However, as enterprises continue to expand their geographic footprint, and the number of locations for which they need to provide access, the weaknesses of these legacy WAN technologies become more apparent. Broadband access provides a more flexible solution, enabling organizations to quickly add new sites and provide high-speed access to more locations. The challenge for enterprises is to secure their rapidly growing environment and maintain consistency and manageability. VPN technology delivers a platform for secure access to corporate information; enterprises need to deploy a flexible, adaptive and cost-effective VPN service to meet their changing needs.

### III. Defining VPNs

In its simplest definition, a VPN provides access to the information or network resources of a private network from a shared or public medium. IP VPNs are virtual connections between dedicated sites over the public internet or private network infrastructures. With IP networking now mainstream, IP VPNs have become a primary networking technology. In fact, IP VPNs are the preferred networking technology for many companies.

IP VPNs address the many concerns of older networking technologies. They provide ubiquitous reach, secure connectivity via encryption and tunneling technology, connectivity flexibility and, generally, lower costs. The value of IP VPNs is apparent. The remaining challenge for organizations is to determine the right deployment strategy and whether they should manage internally or seek help from an IP VPN service provider.

There are two categories of IP VPNs:

- **Site-to-site solutions** include customer premises equipment (CPE)-based solutions and network-based solutions. An enterprise can manage a CPE-based solution internally or enlist a service provider. A network-based solution requires a managed service.
- **Remote access solutions** provide secure access for remote users, typically by client software on a users PC or laptop.

With the increase in the number of remote locations and their exploding adoption of broadband services as their primary access medium, it's critical that enterprise make the right choices. Each IP VPN category fits a particular enterprise need. However, for organizations trying to provide connectivity to remote locations, a site-to-site solution is the logical choice—they simply need to decide how to manage and deploy it.

#### CPE-Based DIY IP VPN

An internally managed, CPE-based IP VPN is one of the earliest deployment models. Network managers deploy a dedicated VPN device at each location and manage the service themselves. The VPN device could be a VPN appliance, firewall or a router with VPN capabilities. Enterprises choose the hardware, install the system and manage every function. For a time, this was the only

option for network managers. Today, enterprises choose this model when they demand complete control of the environment. Additional benefits include service provider independence and perceived end-to-end security. For most organizations, however, the challenges with this approach quickly outweigh the benefits

The most significant challenge for network managers is the management complexity. It's very complicated to manage an IP VPN from cradle to grave. It's expensive to deploy and configure all the devices, and the network manager is responsible for a long task list of operational requirements, including:

- Design
- Sourcing
- Ordering equipment and services
- Configuration management
- Implementation/installation
- Network and device monitoring and management
- Technical support
- Reporting
- Billing/metering
- Dispute resolution
- Cabling

Operational costs make up the largest area of spending when calculating the TCO of an IP VPN. According to Yankee Group research, IT organizations can expect to spend more than 8 hours per managed device per month on operational tasks, including support requirements of network, systems and security administrators and help desk staff (see Exhibit 3).

**Exhibit 3**  
CPE-Based DIY IP VPN Operational Requirements

Source: Yankee Group, 2007

Operational Requirement	Hours per Month per Device
Network/Systems Administrator Support Requirements	6.40
Security Administration Support Requirements	2.00
Help Desk/Billing Support Requirements	0.64

In addition, network managers need to worry about their equipment vendor possibly discontinuing support or investment for their equipment, spending additional money on network and security management software, as well as maintaining the necessary skills of their staff.

In addition to the management headache associated with the equipment and service, the IT organization must manage its ISPs. In all likelihood, the branch offices may use dozens of broadband service providers. Prices and service levels can vary considerably. According to the Yankee Group *2006 Enterprise Managed Services Survey*, two-thirds of organizations require either a single provider or seek to consolidate as many IT services as possible with a single provider. Only one-third of organizations seek a best-of-breed provider for all services. This dynamic exists because nearly 40% of the respondents indicated that managing multiple vendors for their IT needs is the leading challenge they face. Managing a myriad of providers also means billing issues and the inability to negotiate lower rates. For many organizations, the operational burden of the equipment and access services make an internally managed solution the least attractive option for secure, reliable branch access.

### Network-Based IP VPN Service

With a network-based managed service, a VPN service provider enables all the VPN functionality in the service provider's network. The service provider doesn't require specialized VPN equipment on the customer premises. With IPsec and MPLS, the service provider delivers a managed service that emulates frame relay or ATM. The biggest advantage is that there is no additional CPE to purchase, manage and account for beyond the broadband access modem/router, which the service provider delivers with its service. This reduces management overhead and capital expenses. The service provider may also include internet access and security services via its network. Some service providers also offer quality of service (QoS) to reserve bandwidth for and prioritize different types of traffic across their networks.

Network convergence has a profound impact on which network services CIOs choose to deploy. Requirements to prioritize voice and video traffic have given rise to the emergence of MPLS VPNs because they are capable of providing QoS, whereby these

performance-sensitive applications are assigned to a higher class of service (CoS) than other types of traffic. Companies make significant capital investments to enable video conferencing and VoIP so it's critical these expensive projects launch successfully. Prioritizing the most sensitive traffic is critical to optimizing application performance and maximizing return on investment.

Despite the advantages of converged networks, CIOs often lament over complexity and security issues associated with running disparate applications over a single network. However, MPLS VPNs with private access circuits allow the use of private IP addresses, which can simplify network design and makes the network less susceptible to hackers and denial-of-service attacks.

For organizations that are less sensitive to security issues, managed network-based MPLS VPNs enable organizations to opt out of IPsec encryption for sites that are connected to the network via private access circuits. Companies that require stringent security policies must ensure their MPLS VPN service provider uses CPE that supports IPsec at all sites, and that it has the necessary equipment in its network to encrypt/decrypt the traffic. For example, many financial services firms that are transmitting transaction information will require IPsec encryption to protect privileged information and remain in compliance with industry regulations. In these regulated environments, not having IPsec encrypted links is not an option for organizations. In addition, if the MPLS VPN service provider does not offer to support IPsec encryption over any broadband access (i.e., not just its own), this will limit the number of branch offices that can be served. This eliminates the benefits of affordable, ubiquitous broadband access. For many organizations, end-to-end security and the ability to support broadband access are requirements. They need a solution that delivers the best of each.

### CPE-Based Managed Broadband IP VPN

Organizations seeking the best attributes of the previously discussed approaches, and a solution for addressing the challenges, can choose a hybrid MPLS/IPsec VPN service. For smaller sites using broadband-based services, the service provider deploys a broadband modem/router that supports IPsec at each branch office and manages everything from installation to ongoing monitoring and support. This enables the enterprise to turn on branch

sites quickly and easily. In addition, the service provider can order and provision the broadband access. Larger sites would connect directly to the provider's IP VPN service and benefit from QoS and traffic engineering features of the MPLS-based service. With the provider terminating both IPsec and MPLS VPN connections, customers experience a single logical network with seamless any-to-any connectivity among branch sites and main offices.

The hybrid offering also provides a centralized management point for configuring network security and traffic control policies, which can be applied to the enterprise as a whole. Also, customers benefit from receiving one bill for the hybrid services. By using a hybrid managed service model, the cost is much lower, and the organization can focus on business issues rather than focusing on many of the management headaches that come with managing multiple carrier networks and the day-to-day management of equipment. The IT department can focus on more valuable contributions and strategic initiatives rather than operating as a cost center. The major benefits include:

- **Centralized policy control and management:** Network managers receive the benefit of a distributed, flexible solution but can centrally manage security and access policies for their entire organization.
- **Operational cost savings:** Network management is much simpler, and there are no hardware purchase or support costs.
- **Capital cost savings:** In many cases, the service provider owns and manages the equipment. There are no lease- or asset-related expenses.
- **Scalability:** Network managers can quickly provision new sites. Since it is a managed offering, it can scale quickly, leveraging ubiquitous broadband access and the expertise of the service provider.
- **Better value:** Services cost less and deliver high-speed, secure connectivity to every branch location.

Distributed organizations with many branch offices can capture the benefits of both the internally managed CPE-based approach and the network-based approach with this solution. It also addresses the major challenges of each. In particular, it centralizes the purchase and support of the VPN equipment and the broadband services. It delivers reliable, secure branch location access at a much lower cost (see Exhibit 4).

## IV. Conclusion

The importance of secure access to corporate information from branch locations cannot be overemphasized. Today's networked organizations rely on their branches to reach customers, enhance service levels and generate revenue. Network managers are responsible for delivering new, productivity-enhancing applications to every user in the organization's value chain. How well enterprises accomplish these goals can be the difference between success and failure, being a market leader, or falling behind competitively. A broadband-based managed IP VPN service can meet many of the network challenges that distributed organizations face and reduce costs at the same time. It can help companies transform how they communicate and share information, while simultaneously reducing IT operational costs. It's a network service that truly delivers value for each dollar spent.

### Exhibit 4 CPE-Based DIY IP VPN vs. Broadband-Based Managed IP VPN

Source: Yankee Group, 2007

Operational Support Category	DIY CPE-Based Approach	Broadband-Based Managed IP VPN
Network/Systems Administrator Monthly Support Requirements per Device (in Hours)	6.0	0.0
System Administration Monthly Support Requirements per Device (in Hours)	2.0	0.0
Help Desk/Billing Monthly Support Requirements per Device (in Hours)	0.5	0.0
<b>Total Support Hours per Month</b>	<b>8.5</b>	<b>0</b>
<b>Number of Sites</b>	<b>100</b>	<b>100</b>
<b>Total Required Support Hours</b>	<b>850</b>	<b>0</b>
<b>Average Hourly Salary per Support Person</b>	<b>\$40</b>	<b>\$40</b>
<b>Managed Device Monthly Service Fee</b>	<b>-</b>	<b>\$100</b>
<b>Monthly Support Costs</b>	<b>\$34,000</b>	<b>\$10,000</b>

## Yankee Group

Yankee Group has research and sales staff located in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific. For more information, please contact one of the sales offices listed below.

### Corporate Headquarters

Prudential Tower  
800 Boylston Street  
27th Floor  
**BOSTON, MASSACHUSETTS 02199**  
617-598-7200 phone  
617-598-7400 fax  
info@yankeegroup.com

### Europe

55 Russell Square  
**LONDON WC1B 4HP**  
**UNITED KINGDOM**  
44-20-7307-1050 phone  
44-20-7323-3747 fax  
euroinfo@yankeegroup.com

### Yankee Group | the global connectivity experts™

A global connectivity revolution is under way, transforming the way that businesses and consumers interact beyond anything we have experienced to date. The stakes are high, and there are new needs to be met while power shifts among traditional and new market entrants. Advice about technology change is everywhere—in the clamor of the media, the boardroom approaches of management consultants and the technology research community. Among these sources, Yankee Group stands out as the original and most respected source of deep insight and counsel for the builders, operators and users of connectivity solutions.

For 37 years, we have conducted primary research on the fundamental questions that chart the pace and nature of technology changes on networks, consumers and enterprises. Coupling professional expertise in communications development and deployment with hundreds of interviews and tens of thousands of data points each year, we provide qualitative and quantitative information to our clients in an insightful, timely, flexible and economic offering.

### Yankee Group Link

As technology connects more people, places and things, players must confront challenging questions to benefit from the changes: which technologies, what economic models, which partners and what offerings? Yankee Group Link™ is the research membership uniquely positioned to bring you the focus, the depth, the history and the flexibility you need to answer these questions.

Yankee Group Link membership connects you to our qualitative analysis of the technologies, services and industries we assess in our research agenda charting global connectivity change. It also connects you to unique quantitative data from the dozens of annual surveys we conduct with thousands of enterprises and consumers, along with market adoption data, comprehensive forecasts and global regulatory dashboards.

### Yankee Group Link Research

As a Link member, you have access to more than 500 research reports and notes that Yankee Group publishes each year. Link Research examines current business issues with a unique combination of knowledge and services. We explore topics in an easy-to-read, solutions-oriented format. With the combination of market-driven research and built-in direct access to Yankee Group analysts, you benefit from the interpretation and application of our research to your individual business requirements.

### Yankee Group Link Interaction

Our analysts are at your further disposal with data, information or advice on a particular topic at the core of a Link membership. We encourage you to have direct interaction with analysts through ongoing conversations, conference calls and briefings.

### Yankee Group Link Data

Yankee Group Link Data modules provide a comprehensive, quantitative perspective of global connectivity markets, technologies and the competitive landscape. Together with Link Research, data modules connect you to the information you need to make the most informed strategic and tactical business decisions.

### Yankee Group Consulting

Who better than Yankee Group to help you define key global connectivity strategies, scope major technology initiatives and determine your organization's readiness to undertake them, differentiate yourself competitively or guide initiatives around connectivity change? Our analysts apply Yankee Group research, methodologies, critical thinking and survey results to your specific needs to produce expert, timely, custom results.

### Yankee Group Live!

The global connectivity revolution won't wait. Join our live debates to discuss the impact ubiquitous connectivity will have on your future. Yankee Group's signature events—conferences, webinars and speaking engagements—offer our clients new insight, knowledge and expertise to better understand and overcome the obstacles to succeed in this connectivity revolution.

### [www.yankeegroup.com](http://www.yankeegroup.com)

The people of Yankee Group are the global connectivity experts™—the leading source of insight and counsel for builders, operators and users of connectivity solutions. For more than 35 years, Yankee Group has conducted primary research that charts the pace of technology change and its effect on networks, consumers and enterprises. Headquartered in Boston, Yankee Group has a global presence including operations in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific.