

# Designing a Successful DNS Strategy



by Jennifer Pigg | May 2010

## I. DNS: The Internet Linchpin

In the early days of the Internet, users trying to reach another host on the network were required to type in lengthy IP number strings (e.g., 216.27.61.137). To simplify this process, a flat file was devised that paired each IP address with a comparatively easy-to-remember common language address (e.g., SRI-NIC.ARPA). By the late 1980s, this flat file had evolved to the hierarchical Domain Name System (DNS) we use today—a system that is open, distributed, and expands as users, enterprises and domains appear on the network.

DNS works very well—so well, in fact, that most users are never aware of it. Users expect that when they type in a URL or e-mail address, they will be connected to the correct Web site or e-mail box. Security may top the list of enterprise concerns, but too often the link between security vulnerability and DNS is not understood. Enterprises must acknowledge the importance of DNS to the operation of the Internet and, consequently, to any company that uses the Internet for sales, service, marketing or logistics.

As the Internet expands in terms of users, devices and traffic, so does the opportunity for DNS mayhem—whether malicious (hacking), aggravating (spam) or illegal (accessing sites containing content that violates national law and/or regulatory mandates). Enterprises and ISPs must protect their users and networks—sometimes from the hacker in the basement, but increasingly from organized crime and entire governments.

## II. DNS: Vulnerable to Attack

Recent headlines underscore DNS' vulnerability:

- **Twitter's DNS hijacking:** On Dec. 17, 2009, from 9:45-11:00 p.m. PST, 80 percent of Twitter traffic was redirected via a DNS spoof to a page showing a picture of a green flag followed by the words: "This site has been hacked by the Iranian Cyber Army." Twitter was the highest profile site to suffer the DNS attack, but it is estimated that six to 10 other sites were also hit.
- **The great firewall of China:** On March 24, 2010, China extended its network censorship overseas when at least one ISP began returning faulty high-level queries from a Beijing DNS root server operated by Swedish Internet Exchange operator Netnod. That server returned information intended for Chinese users, blocking access to sites such as Facebook, Twitter and YouTube and redirecting users to bogus addresses. Netnod claimed its server did not publish the faulty data that redirected the queries. Security experts posited that it must have been altered by the Chinese government.
- **Pakistan blocks YouTube:** In February 2008, Pakistan's state-owned telecommunications company managed to bring down YouTube for over an hour after receiving orders from the Pakistani government to block access to the site. In what was essentially a cache poisoning attack, the telco broadcast the false claim that the telco itself was the correct route for 256 addresses in YouTube's domain. Unfortunately this reroute did not only affect YouTube traffic from Pakistan—it sent all traffic destined for the domain to the new set of bogus IP addresses.
- **Brazil's Bandesco under fire:** In April 2009, one of the largest banks in Brazil fell victim to a cache poisoning attack launched against Brazilian ISP NET Virtua. Users accessing the bank via NET Virtua found themselves redirected to fake Web sites. The attack aimed to both obtain personal data from bank users and install malicious software on users' computers.

This custom publication has been sponsored by Neustar.

These examples are particularly disturbing because some of them are politically backed attempts to control the Internet for the purpose of censorship. However, they are just the tip of the iceberg in terms of the volume and severity of DNS attacks. Yankee Group enterprise surveys paint a sobering picture of the security challenges users and enterprises face (see Exhibit I).

The survey results illustrate the continued pervasiveness of security attacks. Many of these threats, such as spam, denial of service (DoS) and phishing, rely on DNS to execute their attacks. However, even DDoS attacks that do not target DNS can be reduced in scope and impact with robust, intelligent DNS infrastructure.

### III. Not Your Father’s DNS

The opening up of the enterprise to business partners and customers, the relentless expansion of consumer activity on the Web and the security concerns associated with these trends are raising user and service provider awareness about the role of DNS. However, there are more changes coming that are raising the profile of DNS—notably the move to cloud computing and the migration to IPv6.

### Cloud Computing

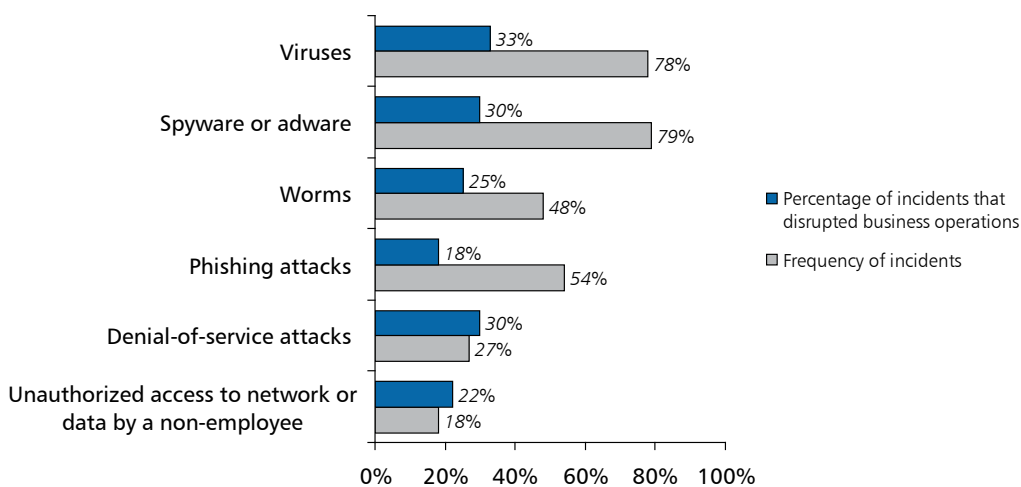
Robust DNS services are critical as large online retailers, media companies, gamers and entertainment providers, and service organizations move to cloud computing and resource virtualization. In the cloud, the end-user application has no way of knowing where in the network a unit of work resides at a given time, so it cannot point to the specific IP address. DNS enables users or applications to address the domain name, which in turn points to the appropriate IP address or set of addresses.

Therefore, a cloud computing application is only as robust as its DNS information. The DNS IP address look-up and routing information must be *accurate* in terms of the frequency of update, it must be *secure* in terms of its vulnerability to attack and *fault-tolerant* in terms of geographic distribution in highly recoverable, secure data centers. Ideally, DNS servers should not be collocated with user applications or data. Enterprises leveraging software- and infrastructure-as-a-service (SaaS/IaaS) applications have found themselves in trouble recently when their service provider network or site, which also housed their DNS data, went down, taking with it all access to the DNS as well.

#### Exhibit I: Enterprises Are Harried by Security Breaches, Data Loss

Source: Yankee Group Anywhere Enterprise—Large: 2009 Mid-Year Analysis, Wave 1-6

Which of the following incidents have been experienced by your organization over the past 12 months, and what was the impact to your business?



When the DNS service is managed separately from other applications, users can be redirected to a redundant site when a network or data center goes down. If there is no redundant data center, a DNS redirect can take customers to a site that informs them of the outage and provides an estimate of when service will be restored. The same scenario can occur when an enterprise outsources its Web hosting, e-mail or disaster recovery services but keeps its DNS servers in-house. If the enterprise site goes down, so do the DNS servers; the enterprise's disaster recovery protocols cannot kick in because the DNS servers are not available to perform the reroutes.

## IPv6

Ericsson, the network solution supplier, had skeptics shaking their heads when it projected that 50 billion devices would be connected to the Internet by 2020. Cisco CTO Padmasree Warrior made this prediction seem meek, however, when she stated during a March 2010 CTIA keynote address that we would have 1 trillion devices connecting to the Internet by 2013. In this emerging "Internet of things," every PC, laptop, notebook, TV, e-reader, smartphone, mobile phone, gaming console and handheld gaming device will be Internet-enabled. Added to the impact of these user devices is the connectivity demand from burgeoning machine-to-machine applications. Each of these billions (or trillions) of devices requires a unique identifier and information about where the device is located.

Until now, we have relied almost exclusively on IPv4 addresses to provide a unique identifier for each device connecting to the Internet. However, the number of IPv4 addresses is limited to  $2^{32}$ , or slightly under 4.3 billion. Various schemes have been deployed to conserve IPv4 addresses, including Classless Inter-Domain Routing (CIDR), network address translation (NAT), Dynamic Host Configuration Protocol (DHCP) and private networks. However, we are still running out of IPv4 addresses rapidly. There is industry consensus that we will exhaust the number of available IPv4 addresses by 2014. More aggressive forecasts, many coming out of the five Regional Internet Registries and the Internet Assigned Numbers Authority (IANA), warn that we will run out of IPv4 addresses by the latter half of 2011. The solution, IPv6 addressing, is accelerating in deployment, but today accounts for less than 1 percent of all connected devices. The next three years will see service providers and enterprises scrambling to deploy IPv6-compatible infrastructure and addressing, which will in turn impact

the way they manage DNS. IPv4 is not going away, however. IPv4 and IPv6 addresses will coexist on the network for the next 10 years, at minimum.

Manually managing and editing DNS files today is cumbersome, and it is easy to make mistakes. And while 32-bit IPv4 addresses may seem lengthy and esoteric, they are simplicity itself when compared to IPv6, which uses a 128-bit address scheme (supporting  $2^{128}$  addresses, or about 340 followed by 36 zeros). Managing networks comprising of both addressing schemes will ensure the demand for automated DNS services and tools that match IPv6 addresses with their associated domain name and provide NAT between IPv4 and IPv6 domains.

## IV. What Is Your DNS Channel Today?

Enterprises have three choices when deciding how to manage their DNS requirements:

- Do everything in-house
- Rely on their ISP
- Turn to a managed DNS service provider

In addition, enterprises must determine if they will differentiate between how they manage their internal and external DNS requirements.

### External DNS

External DNS is focused on the customer experience—improving performance, security and reliability of the customer's Internet access to the enterprise's Web presence. Yankee Group forecasts that global e-commerce revenue will increase at a 20.2 percent CAGR between 2008 and 2013. In the U.S., e-commerce accounts for 35 percent of manufacturing revenue, according to the U.S. Census Bureau. Due to this increasing importance of e-commerce, external DNS architecture must be highly redundant and recoverable, meaning that most enterprises will implement and maintain multiple secondary DNS servers.

In addition, because they face the Internet, external DNS servers are exposed to security threats and must be able to identify and repel attacks. As part of this, the DNS administrator must ensure that external DNS servers in the majority of cases are set to disable recursion in order to avoid Kaminsky-style cache poisoning attacks.

However, the DNS architecture is also likely to be much more distributed. To improve performance, it is necessary to keep address resolution close to the client, meaning that the external DNS servers are increasingly geographically distributed. Remotely located servers also provide redundancy and recoverability in the case of regional outages. So while the enterprise is deriving an increasing percentage of revenue from e-commerce applications, the infrastructure that identifies each e-commerce infrastructure asset is increasing in size, complexity, geographical reach and vulnerability.

## Internal DNS

Internal DNS management is focused on managing the DHCP/DNS environment inside the corporate firewall. Its primary goals are to provide address resolution for network-attached IP devices and to protect corporate assets. The internal DNS administrator must deal with all the issues that are part of the external DNS architecture, including security, recoverability, redundancy and geographical distribution. However, the number of IP devices that fall within the logical confines of the corporate VPN is growing geometrically due to the increase in laptops, notebook computers and smartphones, as well as the transition of the enterprise to VoIP.

In addition, as we discuss later in this report, due to the proliferation of virtualization and cloud computing, it is becoming increasingly complex to identify, locate and manage compute resources. In the case of cloud computing, maintaining low latency for DNS queries can be very difficult as virtual compute resources move throughout the virtual network or VPN.

The majority of enterprises manage DNS requirements in-house or via their ISP. Many use both—they keep DNS management for their internal network in-house and use their ISP for their external Internet-based ecosystem of customers, business partners, Web sites, company portals and e-commerce sites. However, an increasing number of enterprises of every size—from neighborhood pizzerias to global retailers—are turning to managed DNS services. In this section we examine the pros and cons of each solution and the reasons behind the growing reliance on managed DNS solutions.

## Do It Yourself (DIY) for Internal DNS Control

As with any outsourcing debate, the arguments in favor of keeping DNS in-house are cost and control. Most OSs, including Windows, Unix and Linux, come with a DNS server. For smaller enterprises focused on internal DNS control such OS-resident DNS services are likely to be enough. Enterprises that are looking for more flexible and robust control of their IP addressing and DNS management can also turn, for a price, to IP Address Management (IPAM) solutions from either their IP infrastructure vendors (e.g., Cisco, Alcatel-Lucent) or from IPAM-focused vendors such as Infoblox. These IPAM solutions carry with them an implementation cost of between \$15,000 and \$30,000 for a large enterprise. However, the majority of the cost, as with any DIY project, is operational.

Consumers and small enterprises are also likely to leverage some of the free DNS management services that have emerged from companies such as OpenDNS or Google for enhanced control of internal DNS queries. These services are recursive only, so they merely direct end-users back to the Internet; they do not resolve DNS address queries. They offer straightforward GUIs that enable the consumer or enterprise to filter content based on social criteria (e.g., no sexually explicit sites), traffic management (no access to YouTube) or security criteria (filtering out potential phishing sites). The downside of these services is that most make their money on NXqueries, or redirects. If a user types in a non-existent URL, he or she is redirected to an error page that contains paid advertising. While Google does not currently use redirects, Yankee Group believes it would be naïve to assume that the company is not going to leverage the rich, user-specific data on Internet usage that is available as a result of its DNS service. We do not recommend these recursive services for enterprises with more than 50 employees.

Enterprises taking the DIY route must also manage DNS for the external network, servicing the company's e-commerce, e-mail or external Web site. The upside of DIY is control. Nobody is going to care more about the network and customers than the enterprise itself. However, the potential downside also relates to control.

## DIY for External, Authoritative DNS Services

The argument against managing DNS in-house is: Can you exert enough control?

Yankee Group estimates that over 85 percent of enterprises that manage DNS in-house do not have dedicated DNS staff. All of the enterprises' Internet communications, including e-mail, rely on DNS, but it is often managed on an ad-hoc basis with limited expertise and few defined operational processes. Enterprises considering in-house DNS management for their external customer-facing Internet presence must be prepared to address:

- **Availability:** Are there geographically dispersed, redundant servers?
- **Bandwidth:** Is there sufficient capacity to handle spikes in demand? Is external traffic traversing the internal network? If so, performance of the internal network is likely to be both unpredictable and slower.
- **Latency:** Are there sufficient geographically distributed servers, each with enough cache memory? If not, latency injected by the DNS queries (as they are resolved on remote, distant servers) will be noticeable.
- **Performance:** Even if there are sufficient geographically distributed servers, the enterprise will not be able to guarantee that address resolution will be handled locally. Some authoritative DNS services resolve this issue with the use of IP Anycast (which we describe later in this report).
- **Administration:** Editing DNS records is crude and unforgiving. For example, on Oct. 12, 2009, the entire Swedish Internet (the .se zone) stopped working for an hour due to a simple typo introduced during DNS maintenance.
- **Personnel:** DNS management for an enterprise with multiple offices and an internal and external network is complex. DNS skills are specialized and difficult to find. Enterprises will have multiple DNS servers at multiple sites that must be maintained separately. However, personnel with DNS expertise are likely to be centralized, making changes to the DNS infrastructure lengthy and burdensome.

- **Security:** The DNS infrastructure is vulnerable to amplification and spoofing attacks and requires constant monitoring and updates to identify and mitigate such attacks.
- **Outage costs:** This is, in Yankee Group's opinion, the greatest vulnerability to managing DNS in-house. If your customers cannot get to your Web site due to a DNS outage, the money you have saved by managing DNS in-house is likely to evaporate in the first hour of the outage.

Many of these vulnerabilities can be avoided with a managed DNS service. But who should host it—the ISP or a managed DNS service provider?

## Using Your ISP for DNS Management

The upside to using an ISP for DNS management is that it has the potential to resolve almost all of the vulnerabilities of in-house managed DNS. The downside is that it rarely does. DNS management is not the main function of an ISP. As a result, DNS performance is likely to suffer in terms of:

- **Bandwidth:** DNS must be able to resolve queries quickly. ISP network congestion, inadequate peering arrangements and poor DNS architecture will all impact DNS performance.
- **Latency:** Three or four years ago, a user request to connect to a Web site may have resulted in one DNS query. Today, however, many Web sites have multiple real-time feeds from advertisers and other third parties. Each of these feeds can result in five to 30 DNS queries. To avoid injecting an unacceptable amount of latency into the session, the DNS name servers should be geographically close to the user, which cannot be guaranteed by a geographically restricted ISP.
- **Support:** Enterprise users have reported difficulty in getting their ISP to focus on DNS configuration or performance issues. If you or your customers are experiencing poor DNS query resolution, resulting in a sluggish online experience, the ISP is likely to examine the performance of the link and clear the trouble ticket if no problem with the connection is found.

- **Coverage:** The geographical reach of the ISP is, almost by definition, smaller than the geographical dispersion of the customer base. Because of this, the enterprise will see a wide variation in latency for DNS queries.
- **Updates:** ISPs handle DNS management for many customers, and they do not like to update the database regularly. Most ISPs have a policy to update changes between once an hour and once every six hours.

The bottom line is that performance becomes unpredictable. It may be great one minute and slow the next, or fast at one location and dragging at another.

An even more pressing issue with ISP-managed DNS, however, is availability—and that's the issue likely to prompt users to look beyond their ISP for a DNS solution.

As we explain in Section III of this report, DNS name servers should not be collocated with the customer application or data. Enterprises that rely on hosted or cloud (IaaS, SaaS) services have found themselves in trouble recently when the service provider's network or site went down, taking with it all access to the DNS as well.

More and more organizations rely on e-commerce as a main or primary revenue stream and are dependent on their external network for mission-critical corporate functions such as customer service, sales and support. They realize they cannot afford to see DNS go down or suffer a security breach. This is why they are investigating managed DNS services.

## Using a Managed DNS Service Provider

Until 2008, companies with one or two domains and little reliance on the external network or Internet were inclined to manage (using the word broadly) their own DNS. Similarly, large enterprises with 200 or more domains, a business model that relied on a robust external network, and enough DNS work to justify one or more dedicated resources maintained control of their DNS infrastructure themselves. Midsize corporations, characterized by three to 200 domains and up to 4 million DNS queries per month, were most likely to recognize the need for well-managed DNS and to lack the internal resources to devote to it. These corporations were most likely to turn to a managed DNS service.

Two years later, Yankee Group sees business and government organizations of all sizes using managed DNS. This migration is driven by:

- Heightened awareness of the vulnerability of DNS to DDoS attacks due to the well-publicized "Kaminsky attack."
- Heightened awareness of the importance of DNS due to recent well-publicized attacks on the DNS infrastructure of large social Web sites and corporations.
- Increased reliance on the external network in order to conduct business, service customers and generate revenue.
- The understanding that loss of control is a ruse. Through comprehensive portals and reporting, managed DNS services provide better visibility and control of network operations than can be provided internally or via an ISP.
- The understanding that a managed DNS service provider has tools and capabilities that help secure the network, improve availability and enhance performance, which in most cases the enterprise cannot afford to duplicate.

Enterprises are turning to managed DNS because it provides the security, performance and response time they need at a cost that is trivial compared with the major financial losses (in both e-commerce revenue and business interruption) that could result from a Web site that is down.

Managed DNS service pricing is typically scaled to the size of the network. The monthly fee increases with the number of domains and DNS queries. An enterprise must have at least 10-25 domains and over 200,000 queries per month before the monthly price exceeds \$100 for any of the DNS service providers. Managed DNS service providers charge the largest domains, with 20-30 million queries per month (about 0.003 percent of domains), about \$4,000 per month—or about half the cost of a fully loaded DNS management head count and a fraction of the cost of technology and management systems.

## V. What To Look for in a Managed DNS Service

Managed DNS service providers vary widely in terms of the type, size and location of the enterprises they serve; the breadth of their service and security capabilities; and the size and stability of their network. For enterprises looking to secure the customer experience with a managed DNS service, Yankee Group urges them to compare service offerings based on the following criteria—our Managed DNS Service Bill of Rights:

- **Security:** Through the use of network heuristics, the service provider should be able to identify and defend against DDoS attacks and spoofing or cache poisoning attacks. Those attacks that it does not prevent altogether, it must be able to contain and quickly recover from.
- **Performance:** The service should offer consistently high performance from any location under any traffic load conditions. Users should ask the DNS service provider if it has implemented IP Anycast. Some authoritative DNS services use IP Anycast to improve query resolution response time and to load-balance query traffic. The IP Anycast protocol enables the DNS provider to deploy multiple geographically distributed iterations of the root servers. This allows DNS to resolve the query at the closest (or alternatively, least congested) name server, improving response time and customer quality of experience. Note that there are a number of easy-to-use tools available on the Internet that can assist the enterprise in evaluating the performance, in terms of speed of query look-ups, between different service options. Users should keep in mind, however, that performance is likely to vary between geographies, depending on the provider presence in those locations.
- **Change management:** DNS changes should be propagated in real time. Some providers execute DNS changes according to a schedule (every hour or more). Even enterprises that believe they can tolerate this will eventually hit a situation where they need a change executed immediately due to a security breach or network outage.
- **Scalability and latency:** Network nodes should be located in the right geographies for the enterprise. Insufficient numbers of nodes or nodes that are continents away will add seconds to the query response times and degrade user experience.
- **Recoverability:** There should be no single point of failure. The managed DNS service provider should use multiple carriers to avoid being impacted by a network outage. Before committing to a service contract, enterprises should make sure they understand the fail-over and recoverability strategy of the service provider in the case of a node, network or major power failure or natural disaster.
- **Service and support:** The enterprise should have access to 24-7-365 support and a Web portal with visibility into historical and real-time data, and it should be able to manipulate the time-to-live characteristics of cache elements if needed.
- **SLA:** The service provider should offer service level agreements of 99.999 percent DNS uptime guarantees—for the entire network, not just one site—with defined penalties for non-compliance.
- **Internal and external DNS management:** Some enterprises want internal DNS management in addition to an externally facing managed DNS service. In addition to all of the features and functionality of an external service, an internal service should provide role-based access control. It should allow the administrator not only to prevent access to potentially malicious or known phishing sites, but to block according to content (pornography) and performance (YouTube) criteria. It should include audit logs, continuous “blacklist” updates and an easy-to-use GUI for the enterprise network administrator.
- **ROI:** The enterprise should be able to realize a positive ROI due to the reduction in operational costs, improved user experience and performance on the Web site, uptime and business continuity.
- **Proven track record:** The service should be a proven solution, and the provider should be able to point to real-world implementations of the service globally. Only with such references in hand will enterprises be confident that they are getting a robust, scalable solution.

## VI. Conclusions and Recommendations

Think of DNS as “The Force.” It unifies all people and devices connected via the Internet, and its pervasiveness can be used for good or evil.

Companies must be able to leverage DNS while protecting their Web assets from security breaches. Although enterprises may want control over this infrastructure, such total control is not possible. The dissolving of corporate and network boundaries, the growth of and increasing reliance on e-commerce, the proliferation of cloud computing solutions and the gradual penetration of IPv6 all mean that the enterprise no longer knows where its users, its data or its customers are physically located on the network at any given time. Enterprises must still, however, be able to secure and guarantee the performance of their DNS infrastructure over the patchwork of networks, technologies and access devices that characterize the Internet.

A secure, robust, flexible and continuously updated DNS infrastructure is critical to any enterprise—regardless of size—that uses the Internet, whether it is for e-mail or e-commerce. Yankee Group recommends the following to enterprises:

- **Take a hard look at the way you currently manage DNS.** How much does it cost you per year; how rapidly are changes implemented; how frequently is it down; how vulnerable is it to a security breach, particularly an amplification or cache poisoning attack?
- **Examine how your customer, partners and employees connect to your company.** How geographically distributed are they, and in how many countries?
- **Examine the importance of the Internet to your enterprise now and its potential importance in three years.** Do you use it only for e-mail, or do you use it for service, for support, as a critical communication tool or as a revenue stream?
- **Investigate a managed DNS service.** Enterprises that are not satisfied with the way their DNS is managed today or that view the Internet and their Web presence as critical to their company’s survival should definitely consider a managed DNS solution. Similarly, enterprises that have a highly distributed employee base connecting to corporate resources from many different networks and non-company owned devices should investigate how a managed DNS service can help them provide better security, performance and availability.
- **Use the Managed DNS Service Bill of Rights.** Use the guidelines detailed in Section V of this report to evaluate services and determine which service meets the needs of your enterprise.
- **Respect DNS**—and may the force be with you.

# Yankee Group—the global connectivity experts

The people of Yankee Group are the global connectivity experts—the leading source of insight and counsel trusted by builders, operators and users of connectivity solutions for 40 years.

We are uniquely focused on the evolution of Anywhere, and chart the pace of technology change and its effect on networks, consumers and enterprises.

For more information, visit <http://www.yankeegroup.com>



## Research

Leverage qualitative research to make informed business decisions today and plan for the future.

## Data

Gain quantitative insight into current markets and new opportunities via monitors, surveys and forecasts.

## Interaction

Connect with analysts to gain deeper insight into research and trends.

## Consulting

Get in-depth analysis and actionable recommendations tailored to your needs.

## Events

Access world-class events live and online with industry leaders and Yankee Group experts.

Yankee Group's Link products and services provide clients the insight, analysis and tools to navigate the global connectivity revolution.



## Jennifer Pigg, Vice President

Jennifer Pigg is a vice president in Yankee Group's Anywhere Network research group. Her area of expertise is Anywhere Network Infrastructure, technology and management, including carrier convergence infrastructure, carrier Ethernet services and transport, mobile backhaul, packet optical transport, active and passive optical networking, core and edge routers, and multi-service aggregation devices. She also examines the technology challenges facing service providers as they address shifts in the Anywhere Network, such as peer-to-peer content delivery, the approach of IPv6 and cloud computing. On the infrastructure management side, she writes on network OSs, Domain Name System (DNS) and policy management.

Headquarters