Adaptive Network Architectures Are Critical to Government IT Evolution

by Josh Holbrook and Nick Maynard
January 2006

Executive Summary

Shifts in the way government agencies operate and communicate are having a seismic impact on IT systems and network architectures across federal agencies. Unprecedented amounts of bandwidth are required to support new applications, disaster recovery efforts and inter-agency data sharing. Applications and initiatives that leverage service-oriented architecture (SOA) and distributed computing will force government agencies to transform their networks and operational processes. Underpinning this transformation is the need to access applications and services across agencies—giving rise to impromptu and unpredictable information-sharing communities. Strategically, agencies must commit to planning for the unforeseen—whether it be threats of disruption from natural disasters or malicious activity—and take precautions to ensure that networks are self-healing, flexible and adaptable to changing and increasingly more demanding user environments.

Most government networks are not ready for this inevitable transformation. Existing agency networks are built on legacy technologies that are difficult to scale or adapt to the changing needs of today's more sophisticated applications. Perhaps most concerning is that these legacy-related issues are most prominent at centralized locations (i.e., headquarters, data centers) that serve as the heart of IT operational efforts. This shift to SOA and distributed computing casts a different light and a new sense of urgency on driving improved network performance to support agency IT and network upgrade strategies. Government agencies are beginning to recognize the shortcomings of existing network and system architectures and are taking steps to enhance inter/intra-agency information sharing through infrastructure upgrades.

Government agencies are now seeing IT investments as a means to facilitate more effective operational strategies. Projects such as the Quicksilver initiatives—a set of cross-agency IT projects developed by the President's Management Council—are designed to improve productivity and efficiency across the federal government. The importance of these E-Government initiatives is punctuated by the government's funding of priority and aggressive implementation targets. Improved efficiency will be achieved in large part by unifying emerging core applications within a secured environment that will simplify access to IT resources including computing and storage infrastructure and the data that resides on that infrastructure. The foundation for these initiatives must be a unified and flexible WAN architecture that can reliably support the demands of converged, high-bandwidth applications.

As agencies and solution providers reexamine their network architectures, they must first understand the user requirements associated with emerging applications (e.g., web services, remote networked storage) and balance the integration of new technologies with continued use of legacy network services. For locations that require high bandwidth (DS3/50 Mbps and above), this involves assessing the pros and cons of traditional carrier services versus private optical network solutions. When weighing this decision, agencies must consider a wide array of variables, including the cost of equipment, the cost of dark fiber or wavelengths, and how to ensure the network is flexible and adaptable enough to meet future networking needs. The use of a comprehensive financial analysis tool will help enterprises clarify advantages and trade-offs of the alternative approaches.

In this Report, we identify the drivers of network transformation and the requirements of next-generation networks, and provide quantifiable guidance to government agencies weighing carrier versus private optical networking options.

Table of Contents

I. Drivers of IT Infrastructure Transformation

IT transformation is in full swing and continues to gain momentum, represented by $60 billion of IT spending in the federal government in 2005. Renewed IT investments are driven by increasing demands for more efficient communications and information sharing across disparate agency networks. These immediate demands compel CIOs to act quickly and often do not afford them the luxury of a holistic network plan in response to the plethora of emerging applications being introduced. The result is an inflexible architecture that does not adapt easily to changing needs of its users.

A glaring example of this disjointed architecture was brought to light in recent congressional investigations into the lack information sharing within the Department of Justice (DoJ) before the 9/11 attacks. In the white paper titled *Industry Advisory Council DOJ IT in 2005,* Vance Hitch, the DoJ's chief information officer, cites multiple transport technologies managed by a mix of in-house and third parties as contributing to the limited interoperability of networks and applications. Another, more recent example is the government's disjointed response to Hurricane Katrina.

The leading drivers of recent IT investments are increased usage of web services and distributed computing, the consolidation and virtualization of IT resources, the replication of data across geographies, the heightened need for consistent levels of end-to-end security management, and inefficient capital deployment.

Web Services

The increased volume of data required for decision support results in progressively more complex data management environments. Web services, which use distributed software programs and applets that form building blocks for application development, operate across geographically disbursed computing platforms. Enabling rapid development of applications and easy access to information, web services contribute to the complexity of next-generation networks. The need to reference multiple applications physically residing in geographically distributed locations creates additional traffic and service management challenges. The Electronic Freedom of Information Act also drives increasing demand for data by external constituencies.

Enterprises are deploying ubiquitous web services platforms to handle this complicated data management for all of their communities of interest: businesses, citizens, other government agencies and internal users. Controlling large quantities of intersite traffic requires robust and flexible networks that provide high levels of network performance (i.e., low latency and high throughput) to enable a high-quality user experience (see Exhibit 1).

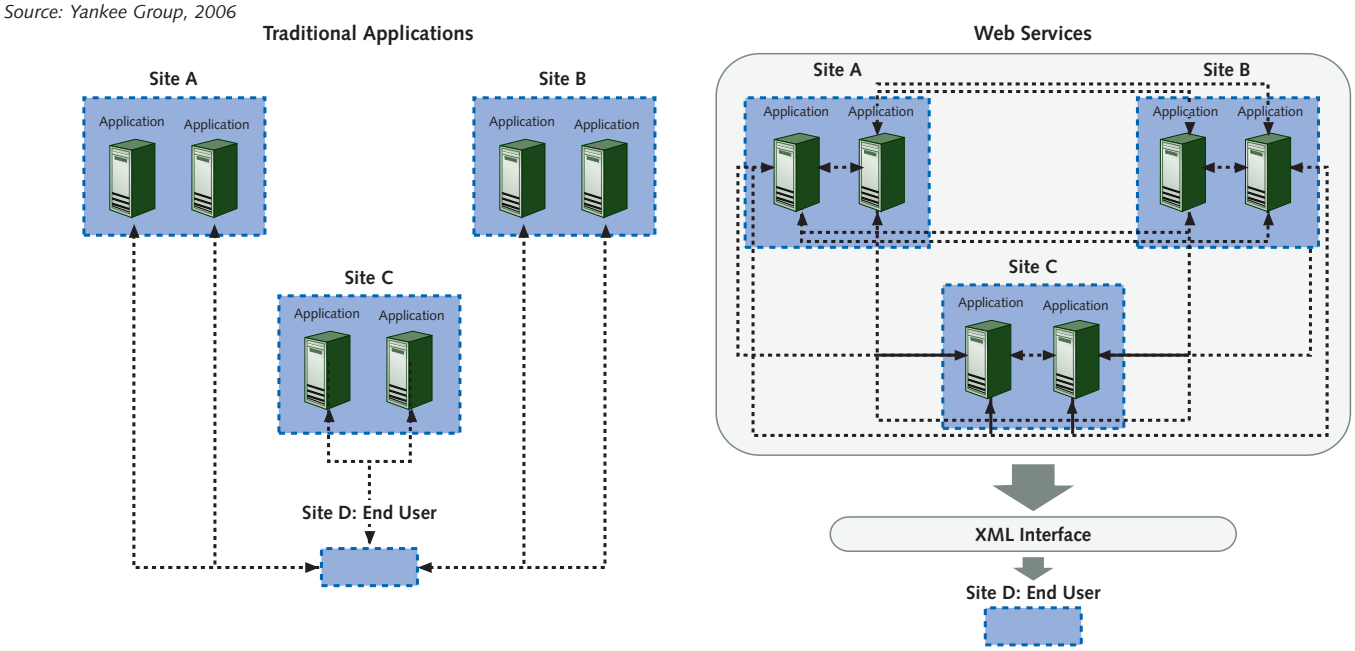
Data Replication

Agencies are increasingly focusing on data availability and protection as they implement solutions for continuity of operations (COOP) and disaster recovery (DR). The transport of data between primary and backup locations often separated by hundreds or thousands of miles is integral to effective COOP and DR strategies. As data backup needs increase, agencies must weigh the risk versus importance of the data and balance this by providing a network solution that is affordable, secure and highly adaptable. Increased user demands on agency networks, coupled with the growth in latency-intolerant and bandwidth-hungry applications, exceed the capabilities of existing network infrastructure. Implementing an effective COOP/DR plan is imperative for government CIOs as they transition to next-generation networks.

Exhibit 1

Increasingly Complex Intersite Traffic Patterns Driven by Web Services

Source: Yankee Group, 2006



Security

Network and application security is important for any organization, but it's especially critical for government agencies that manage highly sensitive and classified information.

Maintaining the integrity of each security zone (high, medium and low) across disparate locations is difficult because of the high number of interconnections between applications and users. Given the unpredictability of information interconnections among agencies, the task of ensuring secure environments is a difficult one for both agency-managed and carrier-managed networks. When we factor in the proliferation of web services, which typically require requests to be executed on several geographically dispersed servers, the complexity of managing next-generation network security significantly increases. The mixture of disparate networks results in inconsistent security protocols that compromise end-to-end security and traffic management. Agencies must focus on perimeter security and approaches to thwart any threats and vulnerabilities. Flexible, adaptable and easily managed networks are crucial.

Cost Efficiency

Budget constrained federal agencies recognize that upgrading network architecture can mitigate operating expenses by enabling the consolidation of IT infrastructure, such as servers and storage networks. Agencies can leverage high-bandwidth networks to centralize IT assets and remove limitations associated of widely distributed IT resources. However, the cost of acquiring the necessary bandwidth to support IT consolidation using legacy transport technology renders the solution impractical. Therefore, to enact their IT centralization strategies government agencies have begun investing in next-generation networks.

The tendency for federal agencies to operate multiple WANs and point-to-point circuits using disparate legacy transport technologies is another driver of cost inefficiencies.

Network management is often an amalgam of in-house and third-party responsibility. In addition, capital and human resources are spread thin across competing technologies. IT executives are beginning to recognize that managing multiple transport technologies within a single agency negatively impacts purchasing power. Agencies are beginning to pursue consolidated network infrastructures, support converged applications, increase IT purchasing power and reduce IT expenditures.

II. Requirements of a Next-Generation Network

The growing cost and complexity of managing multiple applications for numerous constituencies have important implications for network design and operations. Agencies increasingly realize that as networks grow, the rationale for implementing alternative integrated solutions to piecemeal carrier services becomes more compelling. Responding to the proliferation of SOA and emerging applications and services requires unifying applications across multiple locations in a secure and cost-effective manner.

In this section, we discuss the four network requirements that government entities must fulfill to help drive enterprise strategy via IT.

Network Rationalization

Simplifying disjointed network architectures is the primary means to effect cost efficiency. The DoJ's Justice Unified Telecom Network (JUTNet) effort is designed to govern and guide IT investment decisions within the agency and help identify opportunities to collaborate, consolidate and integrate networking efforts. Creating a combination of common solutions, rather than multiple incompatible designs, improves purchasing power and reduces costs. An integrated network also improves productivity by promoting information sharing, improving information integrity and accelerating business change cycles. In light of the numerous applications placing pressures on multiple networks, an effective strategy for any agency is to transition legacy infrastructure to a common next-generation architecture.

High Bandwidth

Bandwidth-intensive applications and the convergence of multiple applications onto a single network drive the need for increased capacity. In addition, the migration of competing networks to a single, interoperable WAN increases the need for bandwidth. The Department of Homeland Security's (DHS's) disaster recovery platform requires real-time scalable bandwidth. This platform is designed to provide emergency managers with better access to disaster-management-related information, planning and response tools.

Additionally, remote storage replication applications rely on a robust network. A high-bandwidth and scalable core network is required to ensure minimal congestion on intersite transport pathways. Some of these mission-critical applications demand that every transaction be mirrored synchronously to a secondary site. However, synchronous mirroring solutions can hurt application performance. A high-bandwidth network is required to ensure mirroring and other network applications run at peak performance levels.

Flexible Architecture

Agencies must design a flexible network that remains easy to manage to ensure operating expenses don't increase in lockstep with complexity. Networks are often designed to address current networking requirements but fail to support converged applications with multiple protocols. E-Government initiatives, such as the ones referenced in this Report, strive to dissolve stovepiped networks in favor of integrated WAN architectures that quickly and cost-effectively incorporate new applications with divergent protocols. Next-generation networks must accommodate multiple traffic types such as ATM, frame relay and Gigabit Ethernet as well as storage and IP traffic. In addition, networks must support application-specific protocols such as those required for NAS (NFS/CIFS) and SAN (SCSI). An architecture that maps multiple protocols to a single network is critical in today's environment, where networks no longer serve the needs of a single community but rather a broad constituency with disparate needs that span internal and external users.

Consistent End-to-End QoS and Performance

Maintaining consistent end-to-end latency, jitter and security levels is exceptionally difficult in an environment characterized by an amalgam of emerging applications operating on legacy technologies. The importance of low latency cannot be overestimated in networks that rely heavily on web services to empower users with information necessary to make accurate and timely decisions. High latency—loosely defined as greater than 10 milliseconds—creates a frustrating end-user experience that hampers adoption of new, productivity-increasing applications.

The Department of Homeland Security's Disaster Management initiative aims to increase the number of current emergency responders using its web-based tool (Disaster Management Interoperability Services [DMIS]) by 10%. In addition, it aims to increase the number of responders with access to the tool by 240%. Time-sensitive web applications and those that have a number and frequency of users such as DMIS rely on a low-latency Layer 1 network to aggregate information from multiple application sites and deliver it to end users. Efficient delivery of web services is predicated upon a robust core network. Application performance is as efficient as its weakest link; and neither web-based applications nor end users can tolerate high latency. Network redesigns must address the need for uniform QoS and security standards throughout the network.

III. Examining Alternative Network Solutions

There are a number of traditional services, such as private line and ATM, that currently carry high-capacity data over enterprise and government networks. However, as the previous section outlines, there is a shift currently under way in agency networking requirements between large agency offices and data centers that is beginning to outstrip the capabilities of legacy solutions. This set of legacy WAN options that support corporate and government networks dominates the majority of networks but may not be able to meet the needs of their end users in the near future.

This section explores the various high-capacity WAN options currently available, including both legacy and optical solutions. A combination of high- and low-capacity services will be required to support the range of agency field offices, headquarters sites and data centers.

Private Lines

Private lines (PLs) offer point-to-point connections for enterprises that require complete control over network design and operations. PLs can be unprotected connections, or they can be protected on multiple levels including diverse paths and redundant CPE. PLs are offered up to 2.5 Gbps and commonly run over SONET/SDH, optical and native Ethernet networks. PL services will remain important to agency networks but they don't represent ideal solutions for reducing complexity, lowering costs and making WANs more flexible in support of critical IT applications. Private line's inability to efficiently scale-up bandwidth and its inherent hub-and-spoke nature make it impractical for environments that demand flexibility.

ATM

Although ATM services will continue to support agency data transport worldwide, these services are not well aligned with the evolution of high-capacity WANs. Results from the Yankee Group *2005 US Enterprise Communications Survey* indicate the continued importance of traditional services such as private line, frame relay and ATM. However, the survey results also show that more than half of the respondents have no plans to purchase any new or additional ATM services. They impose scalability limitations and network topology constraints that impede an enterprise's ability to reduce costs, simplify networks and support emerging IT applications. ATM solutions have proven costly in terms of capital and operations, and provide limited bandwidth efficiency.

Wavelength Services

Wavelengths services are based on wave division multiplexing (WDM), which enables carriers to carry multiple channels across a single fiber. This capability reduces capital costs by lowering the number of equipment platforms and the amount of dark fiber necessary to operate a network. WDM also dramatically increases the available capacity for carriers over their current fiber networks. To take advantage of this lower cost per megabit offered by wavelengths, large agencies have begun utilizing wavelength services themselves, purchasing 2.5-Gbps and 10-Gbps wave services to support their traffic increases.

Wavelength services are protocol-independent and as such are well suited to carry a wide mix of SONET, ATM, Ethernet and SAN traffic—offering high levels of reliability and protection to end users. This protection is offered through fiber route diversity, which protects the connection in case of a fiber cut, and line module redundancy, which enables the WDM platform to restore the interrupted service quickly. Wavelength services have the capability to offer similar performance to a private optical network. But as capacity requirements increase, the cost advantage of wavelength services is diminished compared to private networks.

Private Optical Networks

Many large enterprise, government and academic networks have transitioned from managed carrier services to private networks. Adoption by these organizations began to accelerate as the cost and complexity of private networks decreased.

The economics of deploying and managing a private optical network have changed significantly during the past 3 to 5 years, making it more feasible for enterprises and government agencies to cost-effectively run their own networks:

- **Steep reductions in initial capital costs:** As recently as 3 years ago, the single largest expense for private optical networks was the dark fiber lease. A 20-year contract could cost an agency tens of millions of dollars. Leases are now commonly offered with 3- and 5-year contracts and prices have been reduced by more than 50% in major metropolitan markets. In addition, WDM platform costs have also been reduced while their capacity has significantly increased, allowing a broader set of users beyond carriers to cost-effectively deploy this equipment. Moreover, private optical networks lower overall operational costs by consolidating multiple networks.
- **Advances in network management for simpler operation:** New network planning and management systems make operation easier for end users with more limited, in-house optical expertise than a carrier. The network planning tool enables network managers to quickly assess their capacity demands and networking requirements, and then translate these into a clear deployment plan. Network management systems enable managers to quickly reconfigure their network and address any outages that may occur.
- **Decline in operational expenses due to new features and functionality:** As recently as 1 year ago, sparing costs of WDM line modules were a drain on financial resources. Each line module had a specific channel frequency, requiring numerous types of line modules to be inventoried in case of network outage. With recently introduced software-configurability capabilities, optical network platforms enable agencies to store a single line module type, significantly reducing line module sparing costs. In addition, with dynamic service reconfigurability on a per-port basis, offering any protocol on any port enables agencies to bring up new applications rapidly without waiting for a carrier to deploy new connectivity.
- **Current generation of metro optical solutions offer agencies new levels of network flexibility:** The current generation of WDM platforms can support SONET, Ethernet and SAN protocols, quickly switching from one protocol to another as required by the agency. In addition to being protocol-independent, WDM networks are easily scalable as well. These platforms can quickly scale from current 2.5-Gbps connections to 10-Gbps waves to meet increased capacity demand to meet ongoing and changing requirements.
- **Private metro optical solutions also offer agencies high levels of control over network management and services:** Coupled with the protocol flexibility mentioned above, network control for end users enables them to quickly adapt their network to changing application demands. In contrast, managed solutions typically require days or weeks to complete service changes and even longer to add a new service. This control advantage offered by the private optical networks can be critical for agency operations, especially in national security and defense applications.

Enterprises and government agencies require different levels of capacity based upon location and application usage. But as new applications proliferate, traditional service types may not be suited to meet the bandwidth and latency needs of today's and tomorrow's user communities. A private optical solution may be necessary for networks with the highest requirements for capacity, performance, reliability and security. Large government facilities, data centers and research institutions are some of the types of agency locations that may require a private network. Depending on an agency's network requirements and topology, private optical solutions can be cost-effectively deployed to meet the most stringent networking and application needs.

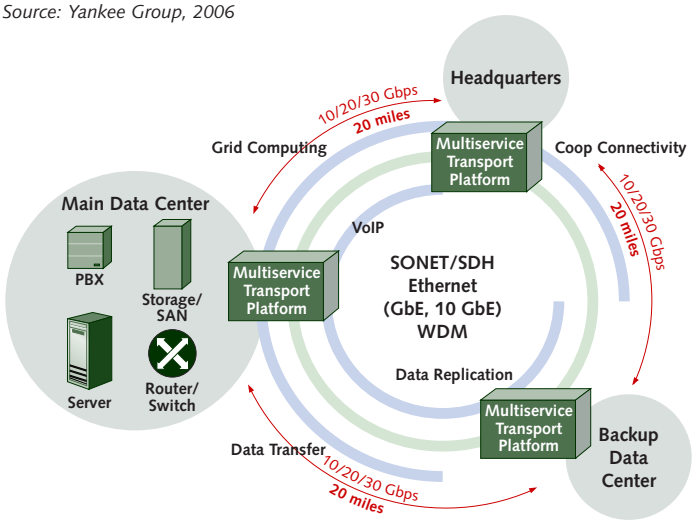
IV. TCO Model for Wavelength and Private Optical Solutions

Yankee Group developed a 5-year total cost of ownership (TCO) model to compare the costs of wavelength services versus a private optical solution (see Exhibit 2). This model is based on a prototypical deployment within several large facilities by an agency that is already familiar with optical network management. The model assumes that fiber availability is not an issue for these large locations within this scenario. It also accounts for the wide number of protocols and high levels of capacity required to support the numerous government applications transported over the network.

Exhibit 2
Summary Metrics for the Private Network and Managed Service TCO Models
Source: Yankee Group, 2006

Factors for Both Wave and Private Networks	Metrics
Network Nodes	3
Term of Contract/IRU	5 years
Capacity	10, 20 and 30 Gbps
Route Protection	Yes
Route Miles (2x for Diversity)	60 miles
Software Upgrades	Yes
Hardware Upgrades	No
Protocols	Ethernet, FC, FICON, OC-n

Exhibit 3
The Agency's Proposed Three-Node Metro Optical Network
Source: Yankee Group, 2006



The model also includes a number of other assumptions about the agency and the network:

- The model assumes a metropolitan area with more than 1 million residents will have adequate fiber availability and competitive pricing.
- The dark fiber is leased for a 5-year period to correspond to the 5-year managed wavelength services contract that would be signed by the agency.
- The network topology for both options includes 60 fiber miles, with two strands of route-diverse fiber connecting three nodes within a metro region.
- For the private build option, we assume the WDM platform and line modules deployed are dedicated to this network rather than shared across several agencies. The platform is also capable of supporting a full range of SONET, Ethernet and SAN protocols. The costs for these service interfaces are included within the model. For the managed service option, the additional costs of the services, such as Ethernet and FICON, are also included in the model.
- For the build scenario, we assume that the operational costs associated with network management will be shared with other networks and connections for that given agency. A fraction of the engineer's time and expenses are devoted to these specific connections.
- The costs for upgrades to the operating system of the platform are included as an annual fee. However, the costs of hardware upgrades are not included.
- Co-location costs, fees and maintenance costs are all included in the model.
- We assume Ethernet, FICON, Fibre Channel and OC-n services are run over the optical transport. The Ethernet and SAN protocols dominated the total traffic of the connections. However, because both the build and buy options have the same services running over them, there is no significant impact on the TCO model results by altering the types of traffic on the network.

The key variable for the TCO model is the capacity of the network. As the capacity requirements increase, the cost-efficiencies of private optical networks become more pronounced. This is due to the capital expenditure for the fiber lease and WDM chassis, which become more cost-effective as the agency deploys more than 10 Gbps of capacity and services. The capacity ranges tested within the TCO model include 10 Gbps, 20 Gbps and 30 Gbps (see Exhibit 3 on previous page). As the capacities increase, the ratio of Ethernet, SONET and SAN protocols remains constant for both scenarios and all other aspects of the model remain the same.

V. TCO Model Results

We used two important metrics to compare the managed services to the private networking solution: initial year costs and total costs.

Initial costs include both the non-recurring capital expenditure and the operating costs for the first year. The total costs include the capital and operational expenses for all 5 years of the model.

Exhibit 4 shows the total and initial-year costs for both the private optical network solution and the managed service solution. The model clearly shows that the managed solution is more cost-effective for agencies with 10 Gbps of capacity or less, while the private network has advantages at 30 Gbps or higher. For 20 Gbps, there is a higher deployment cost for the private network, but the overall costs over the 5-year term are lower. A government agency with this level of capacity would require a custom TCO model that is specifically tailored to its network requirements to determine the best course of action.

The cost advantages for the private optical networking solution over the 5-year study period are demonstrated at the 20 Gbps and 30 Gbps capacities. At these levels, the initial capital cost for the deployment becomes a much smaller percentage of the overall cost of the network. The private network also has a slight 1.1-to-1 cost advantage over the managed service option at 20 Gbps, but a large 1.9-to-1 cost advantage at 30 Gbps of capacity. Exhibit 5 shows that the total cost for the build solution is lower than the buy option once the capacity reaches 20 Gbps.

However, it is important to note that the initial capital expenditure and first-year operational costs are much lower for the managed service until the network capacity reaches 30 Gbps. Even at this very high level, where the costs for the private optical network's initial year are comparable to the costs for the managed service, the private network is still at a slight disadvantage. Agencies with limited annual budgets might not be able to afford this initial outlay for the private network, despite the long-term cost savings the private network could provide, as demonstrated above.

Exhibit 5
Total Costs for Private and Managed Solutions
Source: Yankee Group, 2006

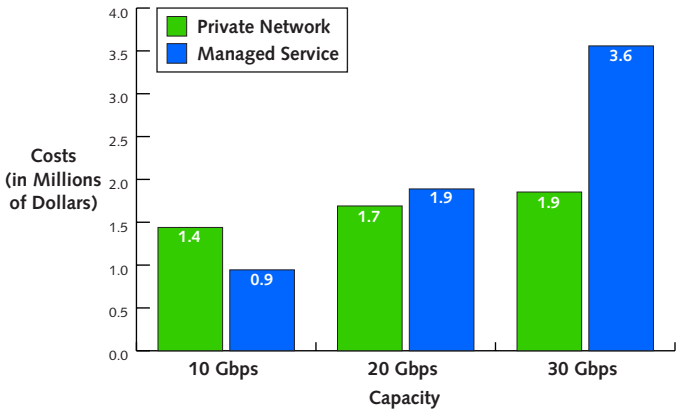


Exhibit 4
Total and Initial Costs for Private and Managed Optical Solutions
Source: Yankee Group, 2006

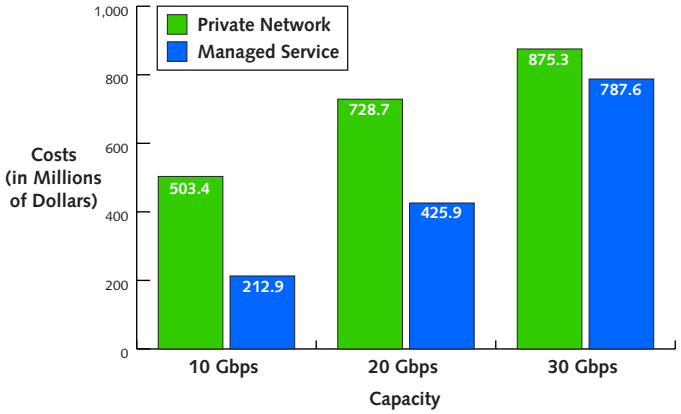
	10-Gbps Capacity		20-Gbps Capacity		30-Gbps Capacity	
	Private Network	Managed Service	Private Network	Managed Service	Private Network	Managed Service
Initial-Year Costs	$503,395	$212,928	$728,740	$425,856	$875,290	$787,584
Total Costs	$1,439,375	$944,448	$1,690,100	$1,888,896	$1,852,850	$3,558,144

Exhibit 6 displays the clear startup cost advantages of the managed solution as determined by the model.

Any changes in the model—such as the term of contract, the number of nodes and deployment in an area with limited fiber competition—will dramatically alter the outcomes for the initial year and total costs. Contract terms for dark fiber and managed services have a large impact on the discount available to the agency. Fiber and service prices would be significantly high for 1-year contracts, while a 20-year lease on dark fiber that is paid upfront would be discounted by up to 40%.

The number of nodes also plays a large role in the build-versus-buy decision for optical networks. The higher number of nodes required by the end user, the more likely the private network option will be the better cost option. For a single point-to-point connection, even with 30 Gbps of total capacity, the operational costs and upfront capex will likely not be worth the potential long-term savings. Prevailing dark fiber costs are such a key factor in the model for the private network that deployment in an area with high rates may offset the cost advantages of the equipment even at higher capacities. These changes, among others, could change the long-term benefits of the private network, making it necessary for agencies considering a private network to carefully weigh the advantages of these two options.

Exhibit 6
Initial-Year Costs for Private and Managed Solutions
Source: Yankee Group, 2006



Optical network connectivity can serve as a key component of infrastructure architecture and strategy. Adaptable solutions—particularly private optical networks and managed wavelength services—are ideal for bandwidth-intensive applications between primary sites in a single region.

Although the TCO model above compares only private networks to a managed service, many variations of optical network solutions are currently available. Agencies can work with solutions providers such as network integrators, VARs and CSPs to build customized optical network solutions created to fit their application network requirements. In addition to private networks run strictly by the agency, there are also numerous private optical networks currently managed by carriers or systems integrators. These management options enable agencies without the in-house optical expertise to operate private networks in tandem with their solution partner.

VI. Conclusions and Recommendations

Optical infrastructure and services have become an important component of agency networks. As bandwidth-intensive applications proliferate—including networked storage, web services and grid computing—agency networks need to support an expanded range of protocols and larger capacities. The complexities associated with these emerging WAN services and applications require enhanced network flexibility, enabling agencies to quickly change network services to support critical applications. Networking requirements for these applications also continue to rise, pushing agencies to demand higher levels of reliability, quality and security. At the same time, networks must become more cost-effective, supporting this broad set of network requirements while lowering both capital and operational costs.

Taken together, these factors are driving network planners to seek out flexible, adaptable and manageable WAN solutions. These WAN solutions include private optical networks and managed wavelength services that are tailored to the networking requirements and cost constraints of government agency networks.

Recommendations for Government Agencies

- **Carefully consider all of the optical alternatives before making a purchasing decision.** The choice between wavelengths, private networks and other options should not be made on price alone. A wavelength service may have higher costs over the long term than dark-fiber solutions, but many factors can still make them the right choice for agencies' needs in terms of cost, control or effectiveness. A private optical network may make economic sense if only the necessary network personnel and support facilities are already in place. Even within the private network solution set, if that is the best option, there is also a wide range of options. Some may fit an agency's needs better depending on protection requirements, contract length, staffing and operational expertise.
- **Understand the applications driving the network transition to forecast future agency requirements.** With so many new applications driving traffic on the network, network managers must carefully track network capacity drivers to understand the agency's future needs. Is the network undergoing slow, steady growth or is a spike in traffic expected? What applications will be key in the near future and what protocols and network performance will be necessary to support them? Will demand occur only along these specific routes or will it expand to include a new group of sites? Network planners need to answer these questions carefully to ensure that they can properly assess their options for the build-versus-buy decision. Optical networking helps agencies meet future needs with only incremental investment, providing investment protection that helps foster development of new applications.
- **Consider the capabilities of network managers.** An agency will need managers capable of deploying or at least managing a private network. Even for wavelength services, there will be high personnel requirements to successfully integrate the service into the agency's network. Agencies should consider the long-term viability of their staffing, monitoring and management costs when choosing a private optical network. A custom TCO study may be required to determine the best option for an agency's network deployment.

VII. Further Reading

Yankee Group DecisionNotes[SM]

- *Infrastructure Management Services Help Enterprises and Service Providers Improve Performance,* January 2006
- *Case Study: Adopting Ethernet WAN Enables Enterprise Application Deployment,* November 2005

Yankee Group Report

- *Standards-Based Communications Servers Show Convincing NPV and IRR for New Product Development Projects,* January 2006

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

31 St. James Avenue
BOSTON, MASSACHUSETTS 02116-4114
T 617.956.5000
F 617.956.5005
info@yankeegroup.com

EMEA

55 Russell Square
LONDON WC1B 4HP
UNITED KINGDOM
T 44.20.7307.1050
F 44.20.7323.3747
euroinfo@yankeegroup.com

North America

200-260 Terence Matthews Crescent
OTTAWA, ONTARIO K2M 2C7
CANADA
T 613.591.0087
F 613.591.0035
canadainfo@yankeegroup.com

Decision Services

Yankee Group Decision Service annual memberships offer clients access to research and one-to-one expert guidance.

Decision Services represent our best value for clients. The services help our members understand industry, regulatory, competitive and market-demand influences, as well as opportunities and risks to their current strategies.

Membership includes an invaluable in-person strategy session with Yankee Group analysts, direct access to a team of analysts, research reports, forecasts, DecisionNotes and regular Online Decision Forums on relevant topics.

We offer Decision Services on almost 30 selected topics in Telecommunications; Wireless/Mobile Communications; Consumers, Media & Entertainment; and Information Technology Hardware, Software & Services.

Decision Instruments

Yankee Group offers a full portfolio of technology and market forecasts, trackers, surveys, and total cost of ownership (TCO), return on investment (ROI), selection and migration tools. Decision instruments provide our clients the data required to compare, evaluate or justify strategic and tactical decisions—a hands-on perspective of yesterday, today and tomorrow—shaped and delivered through original research, in-depth market knowledge and the unparalleled insight of a Yankee Group analyst.

Trackers
Trackers enable accurate, up-to-date tactical comparison and strategic analysis of industry-specific metrics. This detailed and highly segmented tool provides discrete proprietary and performance data, as well as blended metrics interpreted and normalized by Yankee Group analysts.

Surveys
Surveys take the pulse of current attitudes, preferences and practices across the marketplace, including supply, delivery and demand. These powerful tools enable clients to understand their target customers, technology demand and shifting market dynamics.

Forecasts
Forecasts provide a basis for sound business planning. These market indicators are a distillation of continuing Yankee Group research, interpreted by our analysts and delivered from the pragmatic stance our clients have trusted for decades.

Signature Events

Yankee Group's signature events provide a real-time opportunity to connect with the technologies, companies and visionaries that are transforming Telecommunications; Wireless/Mobile Communications; Consumers, Media & Entertainment; and Information Technology Hardware, Software & Services.

Our exclusive interactive forums are the ideal setting for Yankee Group analysts and other industry leaders to discuss and define the future of conversable technologies, business models and strategies.

Consulting Services

Yankee Group's integrated model blends quantitative research, qualitative analysis and consulting. This approach maximizes the value of our solution and the return on our clients' consulting investment.

Each consulting project defines and follows research objectives, methodology, desired deliverables and project schedule. Many Yankee Group clients combine Decision Service memberships with a custom-consulting project, enabling them to augment our ongoing research with proprietary studies.

Thousands of clients across the globe have engaged Yankee Group for consulting services in order to hone their corporate strategies and maximize overall return.

www.yankeegroup.com