



White Paper

metagroup.com



800-945-META [6382]

September 2004

Building the Adaptive Network: *The Role of Managed Services*

A META Group White Paper
Prepared by META Group for Cisco Systems

“IT organizations face a new mandate to align capabilities, costs, and goals directly with those of the business — that is, to become adaptive. Key to maximizing precious IT resources are the development of an adaptive infrastructure and the out-tasking of functions that are not core to the business.”



Contents

Networks: Pivotal to IT	2
A New Mandate for Progressive IT Organizations	3
<i>Critical Issue #1: One Network, Many Stakeholders.....</i>	<i>4</i>
<i>Critical Issue #2: Controlling (and Hiding) Complexity.....</i>	<i>5</i>
<i>Critical Issue #3: Improving Operational Efficiency.....</i>	<i>5</i>
<i>Critical Issue #4: Virtualizing Network Services.....</i>	<i>6</i>
<i>Critical Issue #5: Protecting the Business.....</i>	<i>7</i>
Key Technologies	7
<i>Voice Over IP and IP Telephony.....</i>	<i>8</i>
<i>VPNs Are Changing the Economics of the IP-Based WAN.....</i>	<i>9</i>
<i>Ethernet: The Ultimate in On-Demand Network Service</i>	<i>9</i>
<i>New Bandwidth Alternatives: QoS, Caching, and Compression</i>	<i>9</i>
<i>Mobility and Remote Access.....</i>	<i>10</i>
<i>Wireless Local-Area Networks.....</i>	<i>10</i>
<i>Getting Help With Security.....</i>	<i>11</i>
<i>Storage-Area Networking.....</i>	<i>12</i>
<i>Disaster Recovery and Business Continuity.....</i>	<i>12</i>
Getting the Job Done With Managed Services.....	13
<i>Types of Outsourcers.....</i>	<i>15</i>
<i>Case Study #1: Outsourcing to a Strategic Partner.....</i>	<i>16</i>
<i>Case Study #1: Outsourcing to a Strategic Partner (cont.).....</i>	<i>17</i>
<i>Case Study #2: Reducing the Cost of Remote Network Monitoring.....</i>	<i>18</i>
<i>Case Study #3: Supporting Sudden Changes in the Business.....</i>	<i>18</i>
Planning for New Technology Adoption.....	18
<i>Leveraging a Vendor's Refined Processes.....</i>	<i>18</i>
<i>Proven Areas of Success for Network Out-Tasking.....</i>	<i>19</i>
Bottom Line.....	20

Networks: Pivotal to IT

The role of networking has grown with each major wave of computing — from departmental computing, to client/server, and on to Web computing. The new computing paradigms emerging in the coming years will be no different: networks are the foundation of service-oriented architecture and Web services, multimedia convergence, and utility computing. Entire industries will be restructured by the power of networks — from the use of RFID in retail, to the use of sensor networks in manufacturing, environmental monitoring, and logistics. Leading organizations recognize that an effective communications infrastructure is truly transformational to the business for improving worker productivity, tightening business relationships, and improving service to the customer.

Much is at stake. Networking consumes a large part of the IT budget, typically 13%-25% of enterprise IT costs. But networkers do not get a blank check. IT organizations (ITOs) are more likely to evaluate network spending in the context of total cost of ownership and return on investment, requiring a solid business case before opening the wallet. Best-practice organizations are able to reduce cost *and* improve productivity simultaneously. For example, consolidated data centers and centralized applications enable significant lowering of IT support costs.

However, even though IT centers may be concentrated, users do not have to be. Leading organizations allow users to work from wherever they are able to be the most productive. A strong communications infrastructure is what “glues” it all together.

To succeed, network services must become more reliable, more ubiquitous, and (paradoxically) more invisible to the user in the process. They must be secure. Issues of compliance, cost reduction, business performance management, and cross-business function process improvements are top priorities for business leaders. The future of business depends on networking.

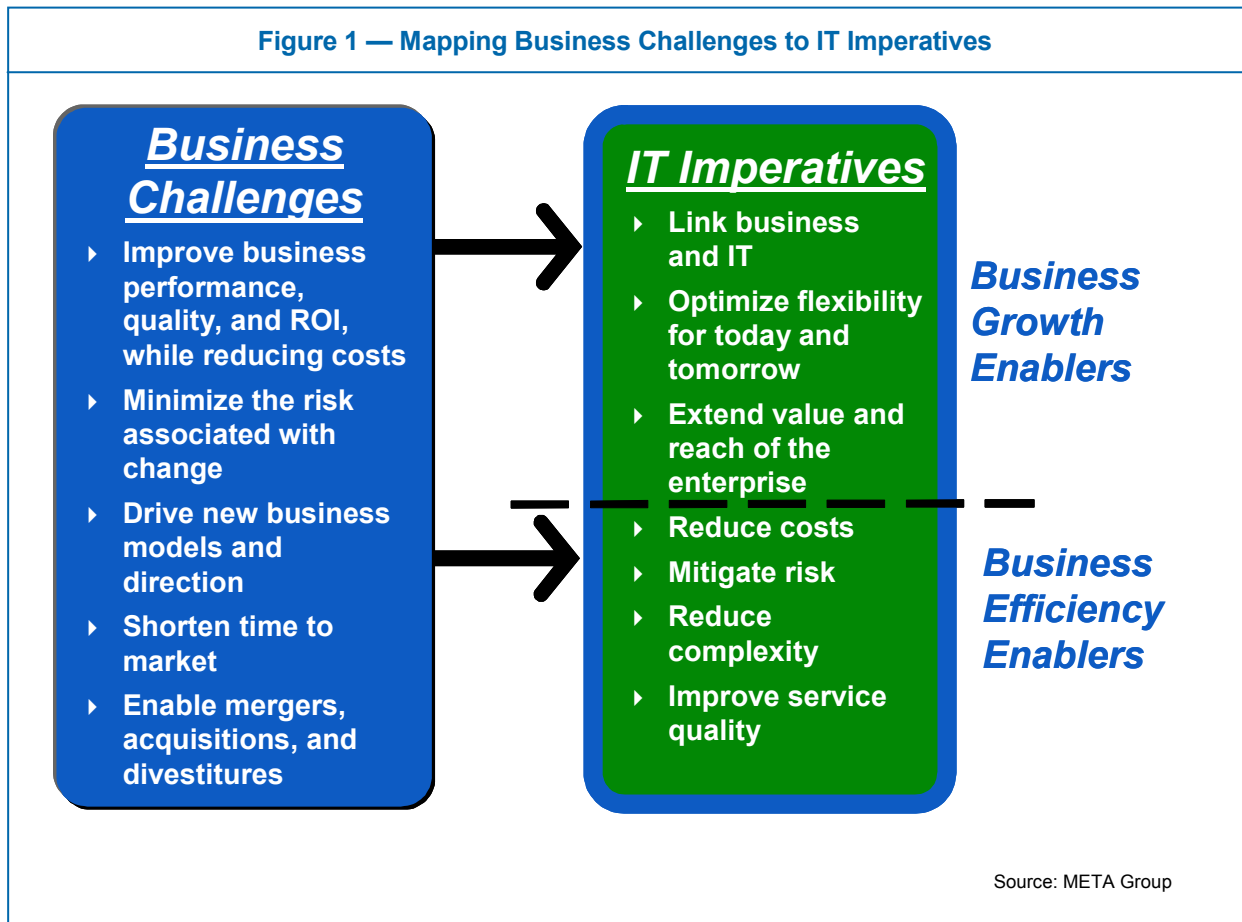
This paper examines the state of the enterprise network, highlighting the key critical issues that will be driving network growth in most large companies for the next two years. It provides insight into the major technologies slated to make a measurable difference to ITOs. It also looks at how the intelligent application of managed network services can help an IT organization meet its business challenges and maximize its investments in infrastructure.

A New Mandate for Progressive IT Organizations

IT organizations face a new mandate to align capabilities, costs, and goals directly with those of the business — that is, to become adaptive. Key to maximizing precious IT resources are the development of an adaptive infrastructure and the out-tasking of functions that are not core to the business.

Adaptive efforts go by many names — from “utility,” to “grid,” to “on demand” — but they all have the same key emphasis: to align IT capabilities, costs, and goals directly with those of the business (see Figure 1). These initiatives have great potential to drive efficiency and reduce cost, starting with the network. In a 2004 META Group survey of 308 users and decision makers, network infrastructure was cited as the number-one area of investment required to become adaptive.

Figure 1 — Mapping Business Challenges to IT Imperatives



Source: META Group

Forward-thinking networking organizations have an overarching vision of a unified, multiservice infrastructure — based on Internet Protocol (IP) — that furnishes support for the full range of networking needs in the data center, at the corporate campus, in the branch office, or wherever mobile workers find themselves. It must be extensible to meet the needs of many constituents — not only corporate users, but also customers, business partners, and suppliers. The goal is to furnish “anywhere, anytime” access to any application. Although the infrastructure needs to be open and transparent to users, it must also be secure. And the real trick is making it highly cost-effective.

With the massive variety of available networking solutions — some of which are new, some current, and some legacy — the operational complexity of the network is still very high. There is no single technology that fits all situations, and even the best ITOs maintain a portfolio of dozens of network technologies and carrier services. Capacity is consumed at a frenetic pace, and network managers are often playing catch-up with the applications that are running. One multinational drug company has identified more than 8,000 applications running on its network (with the list growing every month).

Throwing more staff at the problem is not the answer to the complexity problem. Compensation continues to be one of the most expensive items in the IT budget, running at 20%-50% of total cost. Skills such as networking and security are in high demand and carry premium salaries. The mandate to do more with the same or fewer resources will only continue, further stretching IT personnel. Planners must find another strategy besides hiring more people.

The paradox is that although infrastructure is critical to running the business, the discipline of managing the network infrastructure is rarely a necessary competency for business success.

Critical Issue #1: One Network, Many Stakeholders

Many teams have a stake in the successful operation of the new, converged corporate network. Although data network managers tend to take on the daily operational tasks of running it all, they must also satisfy the needs of various constituencies, from data center and voice managers to security teams and application groups. New techniques such as RACI modeling (i.e., defining who within the ITO is “responsible, accountable, consulted, or informed”) are emerging to clarify the roles of key constituents. With so many people involved, organizations are looking for help to improve their change-management and reporting processes and provide each stakeholder with a unique view of the infrastructure.

The IT organization is far from immune to corporate infighting and politics, and as a result, it can be slow to react to changes in the business. A third party often can be the right catalyst for getting the job done. One global company uses an external outsourcer to enforce its IT standardization efforts, allowing the vendor to charge a premium for proprietary implementations, thus reducing complexity and improving costs over the full life cycle.

Critical Issue #2: Controlling (and Hiding) Complexity

With so many moving parts, it is imperative to take a system-level view. Companies are looking for ways to tie their disparate network domains into a cohesive whole. At the operational level, companies are also seeking to deliver an integrated view across the many disparate devices that make up the system.

IT shops have an abundance of tools that support individual elements and functions, but lack an overall systems view supported by an integrated workbench. Automation provides more rapid deployment, better efficiency, and improved visibility into operations. The level of sophistication found in managed service provider tools often exceeds that available to typical customers on their own.

Managed network service vendors can provide tools to interconnect network segments and create interworking systems for deskbound users, roaming workers, and telecommuters, while shielding individuals from the complexities of connectivity. Advanced toolsets allow administrators to have a system-level view of the services rather than a view of the underlying components. Service-level reporting portals display results based on total service characteristics, expressed in a format that is not IT-centric but is understandable by any business manager.

Critical Issue #3: Improving Operational Efficiency

Due to the typical difficulty of hiring the right people, lack of investment in tools, and the struggle to improve processes, mature internal IT organizations will become the exception, not the norm (as defined by META Group's Process Maturity Model and other methodologies, such as the IT Infrastructure Library [ITIL] and COBIT). META Group estimates that only 30% of ITOs will ever achieve maturity.

Administrators have hit the wall with their current tools and processes, and a much higher degree of automation is needed to push support team productivity to the next level. Although companies generally do a fair job of monitoring network faults, there are substantial gains to be made in configuration, accounting, performance, and security management.

Better cost management is a key aspect of attaining efficiency. The ITO historically has required a high fixed-cost investment, forcing planners to “bet” on the future direction of the company regarding issues such as:

- Will the company’s business units, employee base, and locations grow, or will they shrink?
- Should the IT organization hire new staff and build a large operations center?

Aligning cost with consumption is a key tenet of on-demand or utility computing strategies. By using managed services, the company can grow or expand to meet changes in the business, shifting risk to a managed service provider while allowing expenses to accrue in a linear fashion.

Operational efficiency is also essential for new technology adoption. Administrators are cautious about introducing yet another complex box and driving up operational costs, unless it can be easily integrated as a “plug and forget” appliance, or better yet, as a service “in the cloud” (i.e., supplied by the network itself).

Critical Issue #4: Virtualizing Network Services

Connectivity is just a start. The real goal is to supply a rich set of communications and collaboration services that relies on, but stands apart from, the network infrastructure itself. Services such as voice mail, audio/videoconferencing, instant messaging, whiteboarding, e-learning, and content management are network services that can either exist integrated within the infrastructure or ride separately. Separating communications and collaboration from infrastructure allows for more consistent services across the enterprise, enables rapid change, and controls cost.

Voice applications are prime candidates for virtualization. No longer will voice service be dictated by where a customer is connected to the network. What will matter instead is who they are, how they are connected, and what they want to do. Security services such as firewalling, denial of service, and messaging hygiene also fit naturally into the network.

Another important area of virtualization for large corporate networks and service providers is the partitioning of a consolidated network into multiple logical networks, each of which may be viewed as a private network for its own user base. One chemical company has 23 independent business units, and it is building a common pool of capacity via Multiprotocol Label Switching (MPLS). That pool can be shared by all units, but each will see that capacity as entirely its own.

Critical Issue #5: Protecting the Business

There is a great deal at stake in the consolidated network. One hour of systemwide downtime can cost a company \$330,000 to \$2.8 million. Networks play an active part in ensuring business continuity in the face of disaster.

Keeping ahead of the security threat is key for protecting the business. The number of security vulnerabilities has exploded, with more than 4,000 new exploits discovered each year. Simply keeping up with the reported problems poses a predicament for chief security officers and systems/network administrators. After a vendor releases a security patch, it can take many months for system administrators to identify and fix the vulnerable computer systems. As late as 2003, many enterprises reported outbreaks of the Melissa virus, which exploited vulnerabilities fixed in patches in 2000. Clearly, companies must do more to keep ahead of these threats.

Pressure to improve security is not coming from within the enterprise only, but from regulatory bodies as well. The dramatic increase in compliance mandates (such as Sarbanes-Oxley, HIPAA, GLBA, and Basel II) has complicated matters for both business and IT. The risks are real: A regulatory infraction will send people to jail and stock prices tumbling.

But the need for better business protection is due not only to the hacker threat, but also to threats such as:

- Continued fears of terrorist attacks on systems, particularly in financial, government, and energy organizations
- The growing potential for failures in the aging power grid, as demonstrated by outages in the US and Europe during 2003/04
- Natural disasters, such as earthquakes, floods, or hurricanes

Key Technologies

Organizations are focusing on a few key areas for their network investments (see Figure 2). The critical growth areas are in:

- Convergence
- IP over the wide-area network (WAN)
- Infrastructure optimization
- Mobility and wireless technology
- Security

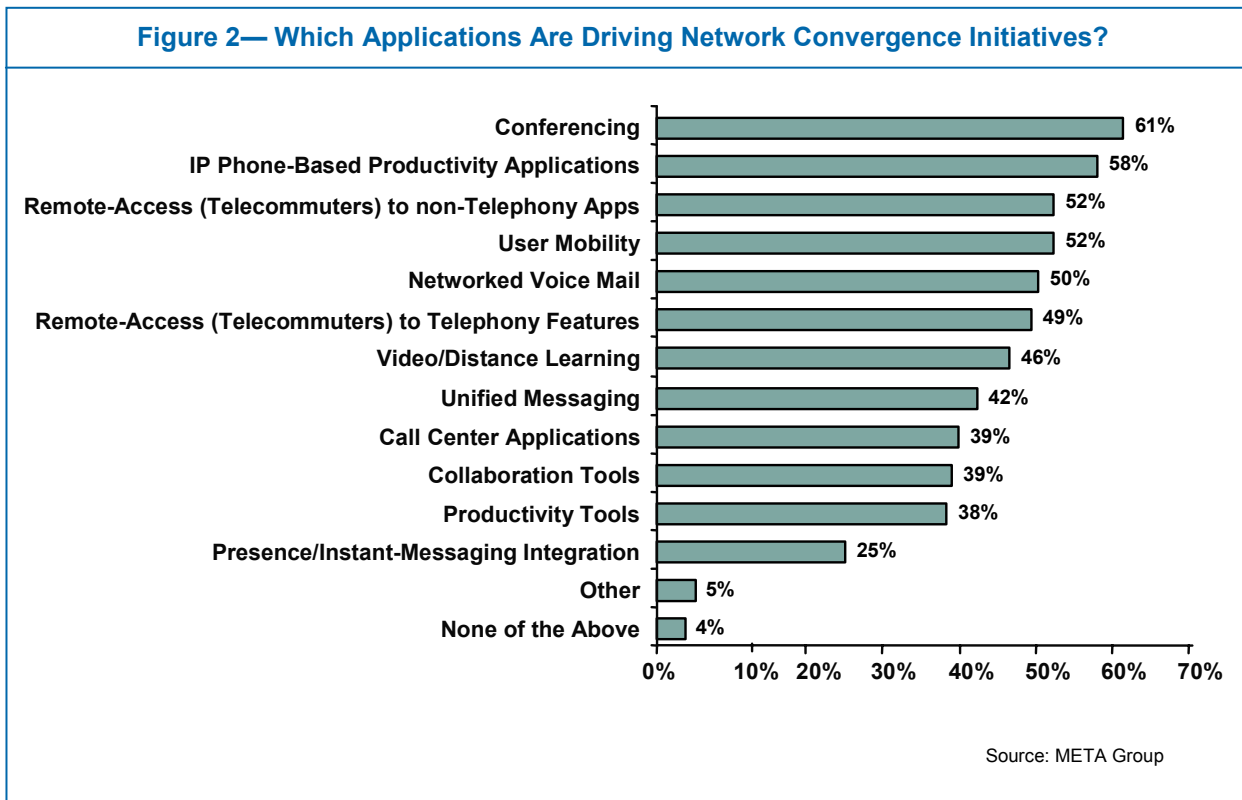
- Storage
- Disaster recovery and business continuity

Following is an examination of the most critical of these technologies.

Voice Over IP and IP Telephony

Voice over IP (VoIP) is foremost in the minds of both network planners and service providers. No longer confined to demonstrations and test beds, the VoIP market has clearly shifted toward a full, end-to-end implementation of VoIP known as IP telephony (IPT), where IP-based phones and devices are placed directly in the users' hands. Enterprises now see opportunities in IPT to consolidate cost, management, and infrastructure — and to boost flexibility, usability, and productivity.

There is no single universal business case for IPT, though cost reduction remains the key driver. Planners look for cost reduction in two key areas: carrier services and operational savings. Productivity is the next consideration (see Figure 2).



As vendors add XML display screens, IP telephones are morphing into a new type of integrated voice and data access device. With the ability to deliver simple applications to a display phone, companies can extend applications into areas where they would not think of adding PCs (e.g., retail floors, manufacturing lines, warehouses).

VPNs Are Changing the Economics of the IP-Based WAN

There are two major spheres of the IP-based WAN: public and private. In the public sphere, the growth of public broadband services provides a lower-cost approach to “always on” service, especially for small offices, teleworkers, and remote users. Compared to traditional services such as frame relay, DSL access-based virtual private networks (VPNs) — using technologies such as IPSec or SSL — reduce the total cost of wide-area networking by 17%-65%, according to a recent META Group study.

Private WANs are also a very strong component. Historically, WANs have been rigid and inflexible, requiring massive reconfiguration when, for example, data centers move or when new applications are introduced. This is changing with new VPN technologies such as MPLS, which is becoming the architecture of choice for network-based VPNs by carriers and enterprise customers alike.

Although native MPLS technology is found only within the largest enterprise networks, carrier MPLS services offer benefits to all types of businesses. They furnish a unified, adaptive, reliable, and cost-effective wide-area solution for interconnecting major offices and automatically rerouting traffic to the optimal destination without administrative intervention. MPLS will displace other carrier services, such as frame relay, before 2008.

Ethernet: The Ultimate in On-Demand Network Service

Network services have historically been static, with a high fixed cost. The old model requires companies to build much more infrastructure than they need, so that optimizing cost involves skimping on headroom for applications. Ethernet changes the economics of networks — by provisioning capacity on an as-needed basis, delivering bandwidth matched to application needs that can be adjusted rapidly over time — often in a matter of hours rather than weeks. In the markets where these services are available, the applications for metropolitan Ethernet and Ethernet-based Internet data centers continue to grow in demand.

New Bandwidth Alternatives: QoS, Caching, and Compression

Throwing bandwidth at every application problem is not practical. Fortunately, there are other techniques for transparently improving application performance.

Quality of service (QoS) can give priority to mission-critical applications and ensure the fair use of available capacity. Caching, or temporarily storing repetitive HTML content, can help Web applications, and compression can reduce the total volume of traffic.

Bandwidth compression and optimization (BCO) incorporates all of these to increase overall network capacity and traffic control. BCO can reduce network traffic by 60%-80%, freeing up bandwidth for new applications and accelerating the performance of existing ones.

Mobility and Remote Access

Work is an activity, not a location, and users should be able to work where they want to work and where they work best. Work habits, physical workspace, and supporting technologies are evolving to create a more flexible, unbounded work environment. Companies also find that a mobile worker strategy enhances its disaster recovery/business resumption plans by providing alternative working environments in the event of a catastrophe.

The challenges of supporting such a fluid, mobile workforce are significant. The enterprise ITO must balance multiple and often conflicting concerns:

- The remote-access program must enable efficiency of the remote worker while keeping corporate resources safe from loss and misuse.
- Users want convenience and solid performance.
- Costs must be controlled.
- The complexity of network access must become invisible to the user.
- Devices themselves must recognize the context in which they reside and configure themselves accordingly.

Wireless Local-Area Networks

More than 30% of enterprises will be moving their wireless local-area network (WLAN), or Wi-Fi, trials into full production deployment in late 2004. Where the security of wireless LANs was once an emphasis, the market will shift toward management and integration during 2004/05. WLAN vendors are being judged on how well they integrate into the overall campus network.

Mobility creates a particular challenge for access security. It is essential to validate the identity of the people or applications gaining access and permit just the right level of access. A directory-based identity infrastructure has now become a best practice. For companies that have an identity infrastructure in place, developing that infrastructure to deliver reliable, high-quality authentication services for more applications and more users is a compelling priority.

A key application for WLANs is in guest networking, or furnishing “in-the-building” access for consultants, contractors, or other guests. Yet doing so in a manner that complies with internal security requirements is a challenge. Use of emerging standards such as IEEE 802.1x and 802.11i security, the adoption of network admission control for wireless technology, management systems that provide better device awareness, and endpoint policy management software are rapidly improving the situation.

In this new wireless world, enterprises will know more about who is connected, where they are connecting from, what device they are using, and what they do once they are connected. The irony of the emphasis on wireless security is that these users may actually have more security than wired users.

Getting Help With Security

Simply running the infrastructure is not enough to ensure success — information and applications must be protected. Security is fraught with complexity, since private application traffic must be isolated from the outside world. The ever-rising list of system threats and vulnerabilities forces a perpetual emphasis on security patches and fixes, along with the introduction of new technologies such as intrusion detection and intrusion prevention systems. But prevention only goes so far, and organizations must prepare for the inevitable. When a security event does occur, the ITO must have an incident response mechanism in place that will get the organization running again and help prevent future attacks.

With security personnel costs rising 31% per year, many firms out-task their security expertise to service providers to ease this burden. In addition, many firms choose to augment their in-house security staff by turning over tasks such as off-hours 24x7 management and threat alert correlation services to a service provider. Another route to achieving lower total cost of ownership for security is to buy security services that are integrated into other managed network services they use, such as a secure multiservice MPLS VPN service.

Staying on top of security threats is a tremendous resource drain. This is why many organizations are considering security services that can help keep them up-

to-date on patches and information on the latest attacks, in much the same way that anti-spam services are gaining hold in the enterprise.

Reacting to a network attack is necessary, but preventing one is much better. Perimeter intrusion detection devices are shifting their emphasis toward prevention, which is a subtle but important change. Intrusion protection places more emphasis on automated response (e.g., closing network ports, banning suspicious IP addresses, shutting down interfaces). Adoption of these systems will increase as they become more reliable, trustworthy, and scalable, and as they adopt the appliance integration model.

Storage-Area Networking

If the network has become the first layer of utility computing, then storage is the next. The idea of having a common pool of storage not assigned specifically to any one device is a powerful one. Storage-area networks (SANs) furnish better asset utilization, simplify management, and reduce labor costs. META Group estimates that only 30% of server-connected data is currently hosted on a SAN or as network-attached storage (NAS), though nearly 60% of Global 2000 organizations have deployed some type of SAN or NAS.

Currently, storage networks are distinctly separate from other networking infrastructure (e.g., LAN, WAN), because the purchase decision makers, management tools, and protocols are all different. However, by 2008/09, integrated networks will mature to enable storage as a service available to applications.

The storage networking market is also undergoing a dramatic technology shift. A new protocol known as iSCSI is competing against Fibre Channel, currently the most widely deployed option. As interoperability improves at the switch layer, individual vendors are innovating at the storage management software layer.

Disaster Recovery and Business Continuity

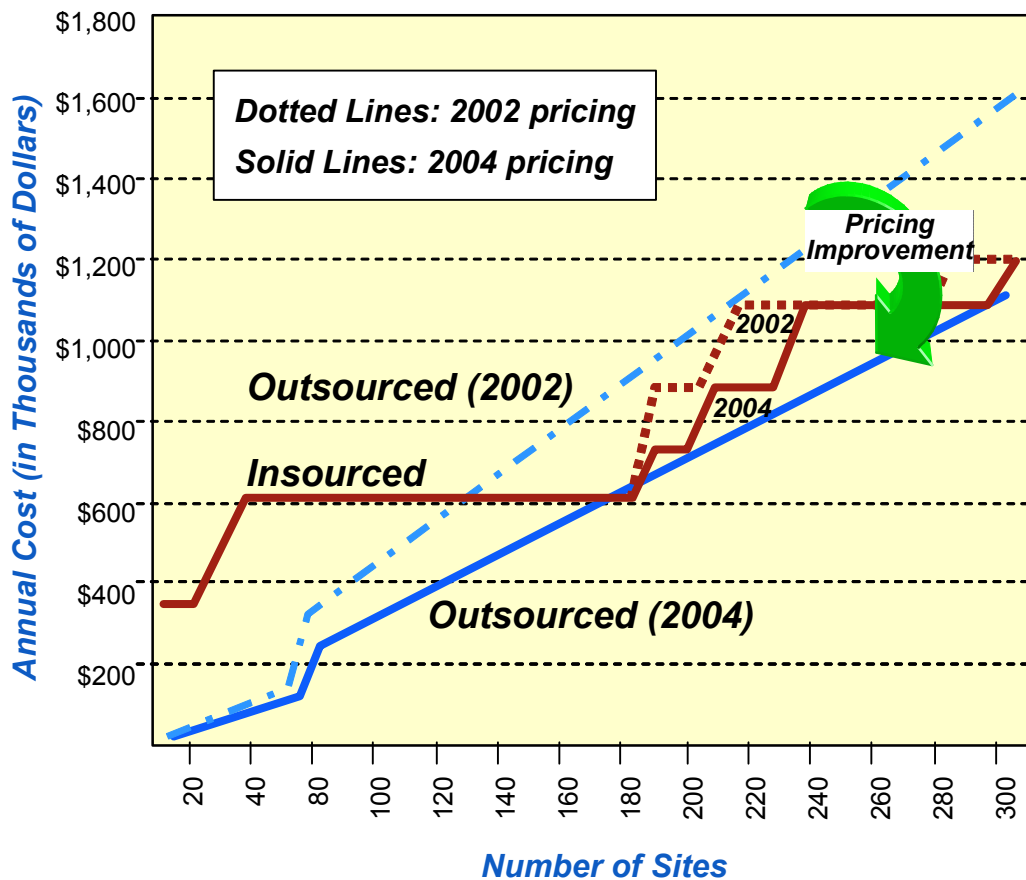
Data center consolidation is a key industry trend, allowing enterprises to centralize resources to one or two data centers and improve service levels to the business while decreasing cost. This shifts risk into the network. META Group projects that by 2007, 40% of Global 2000 users will support two data centers for high-availability requirements (and workload balancing), deploying capacity-on-demand capability for less-critical recovery services.

Getting the Job Done With Managed Services

As we have already established, a company working to leverage the network to its maximum benefit has a full agenda. The challenge is how to do take on all these activities in the face of flat (or even declining) resource levels. Using outside expertise allows a buyer to rapidly add IT capabilities, such as new technology expertise, as well as augment the manpower available to the company, such as with a large network expansion, potentially accelerating the time to market.

The economic payback for out-tasking network services is improving (see Figure 3). But the benefit is not entirely about cost. Many ITOs are starting to view out-tasking as a prescription for change that provides control over business outcomes in various critical areas and not simply as a cost-cutting measure.

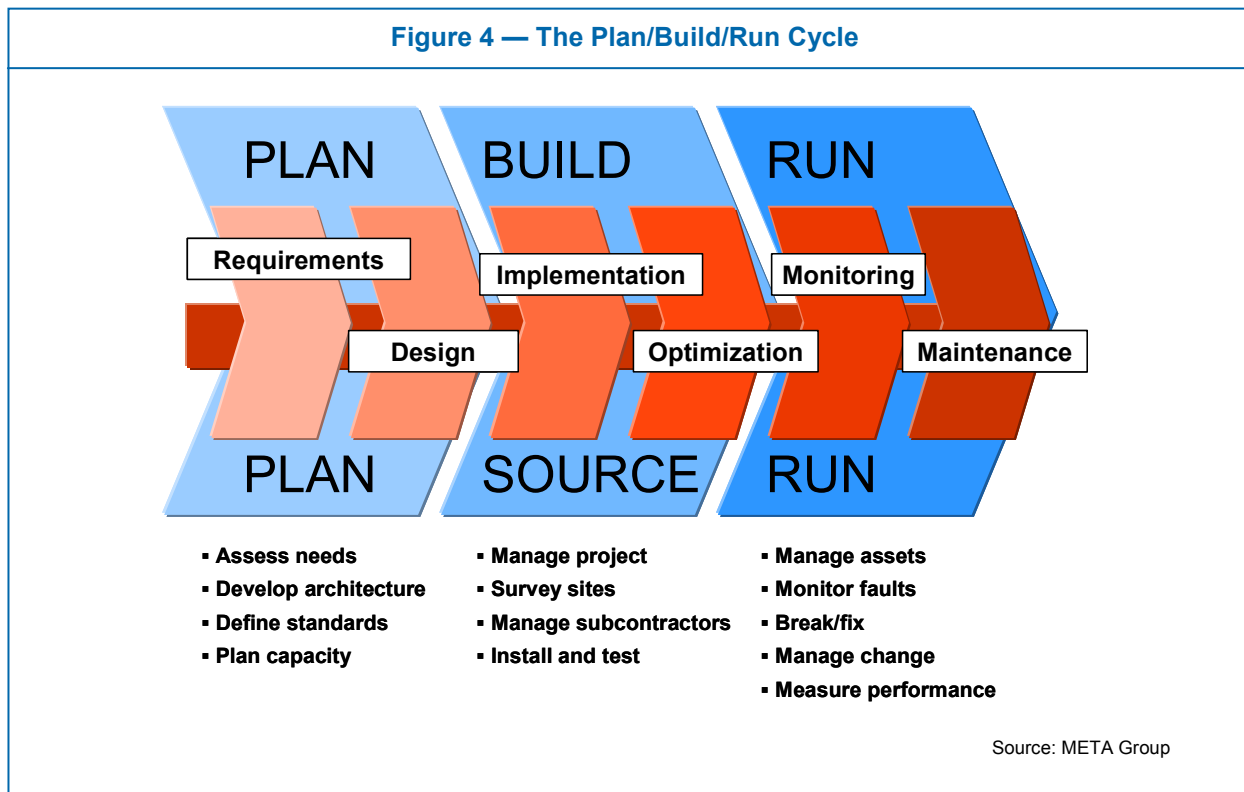
Figure 3— Who's Going to Manage the Network?



Source: META Group

Managed services range from short-term, task- or project-specific initiatives to the outsourcing of the full technology management life cycle. Looking at managed wide-area network services as an example, there are many stages in the plan/build/run cycle (see Figure 4).

By outsourcing managed network services to a service provider, the service provider manages the entire process, from planning through implementation and ongoing operations, handing over this hard work while still maintaining control of the organization's destiny.



Types of Outsourcers

Managed service providers fit various classifications, including:

- **Telecommunications carriers:** These providers have expertise in networking and can provide a “one-stop shop” for all communications functions — providing not only basic transport services but also equipment, deployment, management, and ongoing monitoring. Increasingly, carrier networks feature services such as security, quality of service, and content controls, though application recognition and optimization still remain a challenge.
- **Full-service outsourcers:** These service providers have a broad base of talent in many disciplines from which they can draw. Contracts with these outsourcers often span multiple domains, such as the data center, application hosting, desktops, the help desk, and managed networks, and perform services such as design, systems integration, and ongoing management.
- **System integrators:** Systems integrators provide various services such as consulting, design, integration, and ongoing management, including the management of subcontractors, often with specialization in a specific vertical market (e.g., government, retail, telecom).
- **Value-added resellers:** Value-added resellers (VARs) may specialize in network-based solutions. In fact, networking solutions continue to be among the top three most popular offerings from VARs, along with applications such as messaging or office automation.
- **Equipment vendors:** These vendors often provide planning and integration services as part of the sales process, offering deep expertise in their particular solution.
- **Specialized management service providers:** These specialized providers can provide unique expertise in a specific area, such as systems monitoring, Web hosting, or security.

Case Study #1: Outsourcing to a Strategic Partner

A leading scientific company with more than \$25B in revenues relies on a service provider in the role of a strategic partner to provide architecture, technology selection, and deployment services for all aspects of IT. The service provider's staff works daily with company employees, in the same locations as the customer. Users are largely unaware as to whether staff is employed by the contractor or by the company itself.

As an alternative to full network outsourcing, specific functions such as monitoring, maintenance, and break/fix work are frequently out-tasked to a third-party service:

- Talent may be brought in for specific activities such as audits, compliance reviews, and assessments.
- Specific projects requiring deep, specialized expertise in areas such as VoIP planning, site surveys, wireless LAN radio frequency engineering, or metropolitan-area network planning are often contracted out on a per-project basis.
- Monitoring, management, and maintenance functions can often be included in network services contracts to enable the ITO to focus its efforts on adapting to business process improvements instead of focusing on the mundane daily chores.

One of the most important capabilities that an outsourcer can bring is *scale*. Many service providers can execute a large number of activities simultaneously, such as a large network rollout. As a result, even many organizations that are network “do-it-yourselfers” use third parties to get specific jobs done more quickly and cost effectively. Selective out-tasking of network installation and management can eliminate the requirement to increase staff during a network deployment.

Managed network services also allow the ITO to realign its resources, freeing up personnel to work on other aspects of service delivery and constituent needs. During 2002-04, IT staffing has shifted away from areas such as data networking and help desk, while additional resources have moved into application development, data center/desktop operations, and finance/administration roles. Selective use of out-tasked services has helped drive this change and will have an important role in future growth of the IT organization.

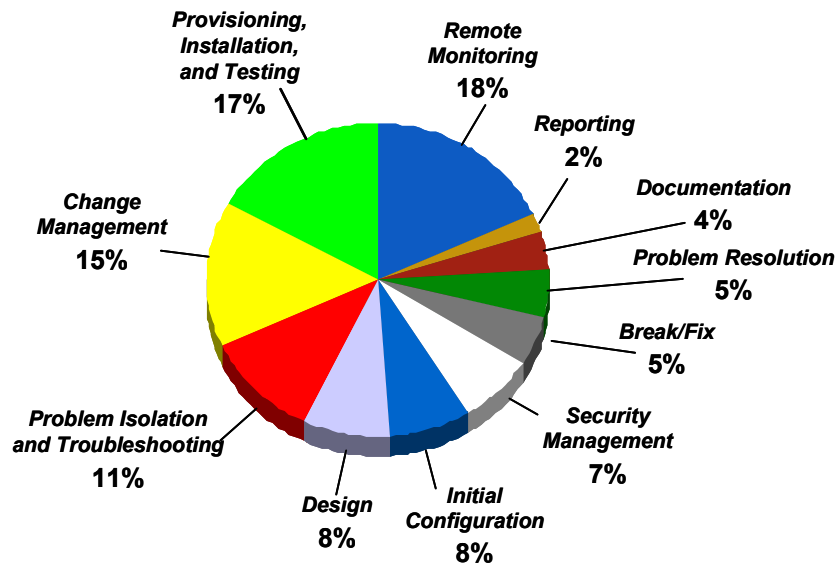
(cont.)

Case Study #1: Outsourcing to a Strategic Partner (cont.)

The network deployment functions that are the most time-consuming and labor-intensive are those most likely to provide rapid payback for the customer, leveraging the strong processes, expertise, and economy of scale of the provider. Fully half of a wide-area network technician's support effort goes to installation, remote monitoring, and change management (see Figure 5).

To assist the IT organization in the network rollout process, labor-intensive tasks such as site surveys and installation services are frequently out-tasked. Ongoing monitoring, maintenance, and break-fix work are also easily handed over to an external provider.

Figure 5 — WAN Support Time Distribution



Source: META Group

Case Study #2: Reducing the Cost of Remote Network Monitoring

One case study example is from a large medical products company that provides equipment to clinics and hospitals, including the monitoring of critical life-support devices. The company's competency is in life-support systems, not in networks. Under the agreement with its customers, this company dispatches technicians for remote maintenance of these devices, and a dispatch can cost several hundred dollars per incident. Because of the variety of network devices in the remote customer sites, the company sought an outside company with broad expertise, to ensure that medical device technicians were not sent to the customer site unless a true medical need arose. This dramatically reduced the number of incorrect dispatches.

Case Study #3: Supporting Sudden Changes in the Business

A large multinational pharmaceutical company saw the need to spin out a smaller equipment and services company. Unlike the highly methodical and controlled environment required by a drug company under regulatory scrutiny, the new entity required rapid integration of entirely new companies within a matter of weeks. The spinout company also has a radically different business model than its highly regulated parent company, and plans to buy and sell businesses every few months. The volume of new locations, infrastructure, and end-user devices meant that service requests were going to go through the roof. The parent organization was simply unequipped to handle this new activity. For the new company, use of a managed service provider proved to be the best way to get the job done.

Planning for New Technology Adoption

By using outsourcers to take care of daily operational tasks, the ITO can realign its resources to focus on transforming the business. Third parties can also play a role in new technology adoption, especially for specialized expertise that is often difficult or costly to hire. These areas include VoIP planning and architecture, content security, service-oriented architecture, business continuity/disaster recovery, wireless technology, and mobile applications.

Leveraging a Vendor's Refined Processes

Technology is often the easy part of IT. Building sophisticated processes to support the technology is more difficult. Third-party vendors frequently bring proven IT services management frameworks such as ITIL into an organization through outsourcing or managed service offerings, improving the overall quality and stability of IT services.

Proven Areas of Success for Network Out-Tasking

There are literally hundreds of components and processes within the IT portfolio. Within the network domain, out-tasking is becoming more widespread, with some services standing out. For example, full network management outsourcing is common among multinational organizations faced with the complexity of many countries, languages, cultures, time zones, and suppliers. Companies of all sizes in Europe and Asia tend to use outsourcers first before they build internal capabilities. Worldwide, small and medium businesses need to augment their IT capabilities. Other companies choose to outsource only a subtask through managed network service contracts.

META Group customers cite the most success with out-tasking of the following services:

Security	<ul style="list-style-type: none"> • Auditing • Planning • Monitoring • Remediation
Network	<ul style="list-style-type: none"> • Design and architecture consulting • Planning and project management • Network monitoring • Deployment and installation • Maintenance and break/fix
Remote-Access VPNs	<ul style="list-style-type: none"> • Dial-up • Managed broadband
Remote PBX and IP-PBX Monitoring	<ul style="list-style-type: none"> • Videoconferencing and Webcasting services • Remote desktop/laptop storage and archival • Audio/video/Web conferencing services (especially for large-scale deployments)
Remote-Office Support	<p>Including:</p> <ul style="list-style-type: none"> • Broadband VPN services • Implementation • Monitoring • Management
Telecom Life-Cycle Management	<p>Spanning the full range of:</p> <ul style="list-style-type: none"> • Telecom planning • Procurement • Benchmarking • Auditing • Ongoing service-level monitoring

Bottom Line

Networking and communications infrastructure must tightly align with and adapt to changes in the business. The ITO must manage complexity, boost employee productivity and efficiency, and produce value for the business. Just as Global 2000 and public-sector organizations have sought cost-efficiency within their own IT operations, they are now seeking to augment their own capabilities with external network services that can bring technology expertise, process maturity, and scale into their organizations.

Infrastructure does not exist for its own purposes. It is merely a means to deliver business applications and functions. Providers that can link the value of infrastructure to the value of applications are best positioned to succeed. A telecommunications manager for a Global 200 manufacturing organization stated, "We're looking for additional visibility into how well our applications are performing. We need services that can not only give us capacity, but also help us support the business as well."

So what's next for the corporate network? It is clear that networks will take a more active role in delivering applications and enhancing business productivity. They will become self-optimizing and self-securing, with better application awareness, adjusting to fit the varying needs of users, administrators, and the business at large.

Connectivity is just the beginning. Using outside resources to augment in-house expertise allows the IT organization to focus on building a more effective business.

David Willis is a vice president with Infrastructure Strategies, a META Group advisory service. For additional information on this topic or other META Group offerings, contact info@metagroup.com.



About META Group

Return On IntelligenceSM

META Group is a leading provider of information technology research, advisory services, and strategic consulting. Delivering objective and actionable guidance, META Group's experienced analysts and consultants are trusted advisors to IT and business executives around the world. Our unique collaborative models and dedicated customer service help clients be more efficient, effective, and timely in their use of IT to achieve their business goals. Visit metagroup.com for more details on our high-value approach.

