WHITE PAPER

CDW PEOPLE WHO GET IT

OPTIMIZING THE NETWORK

Mobility and bandwidth-hungry apps demand faster and more efficient networks.

Executive Summary

Organizations have come to depend on their data networks as a basic necessity to keep the doors open and the lights on. The network has become a utility: It is a basic assumption of staff members that it is something that's always there, all the time.

Although the analogy to power and water utilities may seem appropriate, networks are inherently different. Installing bigger pipes when demand begins to exceed supply is not sufficient. The shift in organizational IT usage from primarily desk-bound data entry personnel to mobile knowledge workers and the growing use of higher-bandwidth applications, such as video conferencing, are driving the need for more efficient and effective enterprise networks.

Table of Contents

TWEET THIS!

At the core of the network, simply building bigger pipes to prepare for 10 gigabit-per-second Ethernet (10 Gig-E) and beyond is one step. But the WAN requires a different set of tools for smart growth, including adding quality of service (QoS) controls, such as bandwidth management and WAN optimization. In the data center, the move toward virtualization and cloud computing calls for different architectures as well as higher levels of reliability and performance than have been achieved before.

Optimizing the network entails identifying both current and future potential bottlenecks and working to remove or avoid them. To do so, network managers must invest in effective monitoring and visibility tools, then use the information these provide to intelligently change the network at the edge, at the core and in the data center.

Optimizing at the Edge of the Network

A difficult truth of networking is that users are all located at the edge of the network. Optimizing the core of the network takes a lot of planning and a lot of hardware, but the edge of the network is where the real action is. Delivering speedy and reliable network service to end users, whether they are at the organization's headquarters, a branch facility or out in the cloud, can be a challenge.

Before network managers can apply tools such as load balancers, WAN optimization and compression hardware, or QoS enforcement systems, they must understand what is running on the network and where the end users are. Thus, the first step toward effective optimization is improving visibility.

Most network managers have reachability monitoring and simple trending — for example, automated testing and alerts for system outages, port problems, high error rates and congestion — well under control. Indeed, the abundance of quality open-source and commercial products in this area can lead to over-reliance on basic reachability and trend information for planning and debugging. Two important steps in monitoring are increasing application layer awareness and better end-to-end testing.

Application-layer awareness: This comes from looking beyond simple in/out statistics to identify the applications that run on the network and the end users who employ them. So many tools targeting application-layer awareness have become available in recent years that network managers may have difficulty picking one. Each has its pros and cons.

End-to-end testing: This is another part of an effective monitoring strategy. In the long run, the network exists to support applications. This means that monitoring the network is useful, but not sufficient. Network managers should integrate end-to-end application layer testing to proactively identify problems and solve them before help desk calls start.

The easiest way to understand end-to-end testing is by considering e-mail. A proper test of e-mail would start a message, send it through the messaging system, receive it in a mailbox and then verify that the end-to-end performance was within acceptable limits. Doing that four times an hour helps to

4 Approaches to Application Layer Visibility

Approach	What It Does	Pros	Cons
NetFlow and similar tools (see sidebar on page 3)	Uses existing network elements, such as switches and routers, to feed a management console with information about flows running across the network at the User Datagram Protocol and Transmission Control Protocol layers	Works with existing network elements; easily combines commercial and open-source data flows	Can overwhelm older devices; unmanaged and older elements may not be able to feed information
Probe-based (also intrusion detection and intrusion prevention systems)	Adds network probes to feed the flow of information back to a dedicated management console (This also can be a side effect of other tools, such as IDSs and IPSs.)	Dedicated probes have better capabilities for application and user analysis; specific network analysis tools offer network managers more information	Can be hard to identify appropriate probe points in highly switched networks; adding probes can be costly
Security information and event management (SIEM)	Uses firewall logs and SIEM capabilities to provide traffic summary information and drill-down	Using existing SIEM is efficient, but only if it has this information and the analysis tools built in	Compliance and security teams may not want to share their SIEM with network teams or be able to handle the added load
Next-generation firewalls (also proxy servers and unified threat management appliances)	All next-gen firewalls generate detailed application usage and user tracking information, and most of these products have management appliances that can collect and summarize data	Next-gen firewalls have better application visibility than any other tools, especially when Secure Sockets Layer decoding is used	Firewalls can show only traffic that passes through them, and internal flows or branch VPN traffic may bypass these devices

ensure that many common problems with the e-mail system can be detected quickly. Yes, products such as Microsoft Exchange have hundreds of internal monitoring elements, many of which are worth looking at. But the end-to-end performance is what really counts, and that's part of end-to-end testing.

The same thing is true of almost any application running on the organizational network. An end-to-end test that validates the operation of simple transactions is part of a holistic approach to network and system management.

When network teams have spent years building effective tools to monitor thousands of network elements and alert administrators of problems, extending those tools to give a full view of application performance across an organization makes a lot of sense. Because the network affects so many parts of every application, continuous end-to-end testing of each application can help to quickly identify the source of a problem.

Not Just NetFlow

NetFlow is a simple protocol that periodically sends sampled information about network flows passing through an interface, such as an Ethernet port, to a management system. Originally designed by Cisco to provide accounting information for Internet service providers, by 2002 NetFlow was widely available in non-Cisco products.

Generally, network vendors made slight changes to the protocol, giving rise to a wide variety of "flow" protocols: Cisco's NetFlow v5 and third-party protocols such as sFlow, jFlow, cflowd and Rflow are all similar.

In an effort to rein in the chaos of "similar but different," and to solve problems with the original NetFlow (such as lack of IPv6 support), Cisco published NetFlow v9. The Internet Engineering Task Force built on Cisco's work with Internet Protocol Flow Information Export (IPFIX), which is sometimes referred to as "NetFlow v10."

Bandwidth Management and WAN Optimization Tools

Once a networking team has a clear idea of what applications are running on the network, who is using them and how much bandwidth each consumes, the next step is to apply bandwidth management and WAN optimization.

QoS and bandwidth management: Bandwidth management is an important part of quality of service controls. It can transform a network that performs inconsistently into a predictable data pathway with reserved bandwidth, controlled congestion, managed jitter and prioritized queuing.

QoS in organizational LANs (where bandwidth is essentially unlimited) can be very useful for keeping time-sensitive traffic, such as voice and video, moving smoothly. A different set of tools is needed when connecting to public networks, though, because QoS enforcement can be difficult outside of an organizational campus. Some enterprises have gone with expensive private solutions (typically based on multiprotocol label switching technologies) that deliver absolute predictability and strong controls. When public networks such as the Internet are thrown into the mix and circuits are oversubscribed, bandwidth management and Class of Service (CoS) are the preferred tools.

In a nutshell, bandwidth management usually includes some type of tagging or coloring (identification of applications or particular traffic flows) followed by control of how the tagged traffic flows across choke points, such as the network connection to a remote office.

There is no universal agreement on the terminology used in this area. If a product vendor speaks of these flows in terms of metals (bronze, silver and gold), then they might refer to CoS, which is largely concerned with prioritizing the traffic once it has been tagged.

If the product is configured to allocate, limit or guarantee a certain bandwidth for each type of flow, then it is bandwidth management. Usually, bandwidth management includes both guarantees (for example, "VoIP calls get a minimum of 96 kilobits per second") and policing (for example, "E-mail cannot use more than 64 kbps"), both based on the bandwidth available going from the LAN to the WAN.

Almost every product mixes the two techniques of prioritization (CoS and bandwidth management) to some extent by applying bandwidth controls to different classes. Therefore, the choice of terminology, whether bandwidth management or CoS, does not provide a significant discriminator when comparing products.

Several techniques for controlling traffic in IP networks are useful when applying bandwidth management. An application layer approach that reserves resources and gives the application information to allow it to perform properly is the most effective strategy. For example, in VoIP and video conferencing, use of "call admission control" ensures that calls are allowed outside of a LAN only when sufficient bandwidth is available for good call quality. Unfortunately, resource reservation is fairly uncommon except in the world of voice and video, so it must be mixed with other techniques.

The transport layer approach, which applies to Transmission Control Protocol (TCP), calls for a bandwidth management device to modify the protocol itself to avoid overusing bandwidth. The device could be a firewall, which is an ideal location for bandwidth management in most networks, or a separate device specific to the task. Generally, firewalls have

fairly primitive bandwidth management features, and only a few actually have transport layer bandwidth management. Network managers who want a good bandwidth management solution should plan for additional hardware in most cases.

The network layer approach, which works for IP (and protocols on top of IP, such as User Datagram Protocol and TCP), has the bandwidth management device simply drop packets when congestion occurs or bandwidth limits are hit. Network layer bandwidth management is the least effective approach and can cause significant network inefficiencies as packets are retransmitted.

Applying Bandwidth Management and Class of Service

Technique	Verdict	Why?
Application layer (such as call admission control, RSVP)	Best	Applications can be blocked or have their usage of the network reduced, preventing congestion and overuse of limited circuits.
Transport layer (such as TCP window size modification, acknowledgment code delays)	Good	TCP behaves well in limited-bandwidth environments, reducing waste and allowing for change even during a connection.
Network layer (such as dropping or delaying IP packets)	Not Preferred	Simply dropping packets during a time of congestion gives users a poor experience and makes inefficient use of the network.

WAN optimization: A close cousin to bandwidth management and CoS is WAN optimization. Many products overlap each other, so network managers will find that WAN optimization devices may also include bandwidth management and application control features.

The goal of WAN optimization is to make more efficient use of limited WAN bandwidth, which can be accomplished using a variety of techniques. The most important techniques are caching and compression.

Caching reduces WAN usage by storing copies of recently transmitted data locally. For example, if one user in a branch office downloads a Word document from a file share, the WAN optimization device in the branch may save the document. When the next user in that office clicks on the same document, it doesn't have to be retransmitted because there's already a copy stored in the WAN optimization device. Not transmitting the file requires some cooperation on the other end, so optimization devices are generally deployed at both ends of the WAN link.

Compression also reduces WAN traffic. Not all data compresses properly, and if the traffic flow is largely precompressed data (such as zip files) or images, compression won't do much good. But for many typical network applications, even those that are web based, compression can make a big difference.

Although compression generally requires a device at each end of the link, some vendors have become very clever about accomplishing this with a single device. For example, many poorly written applications, such as big enterprise resource planning (ERP) packages, retransmit the same JavaScript repeatedly in every web page. Web browsers also have the ability to decompress data automatically, without any operating system or user intervention. Some WAN optimization devices dig deep into the transmitted pages to make the user's client web browser perform some on-device caching and compression without having a second device at the other end of the WAN.

Encrypted Streams: Uncompressible and Uncachable

Encrypted data cannot be compressed or cached, which means that — in theory — a WAN that is transmitting encrypted data won't benefit from WAN optimization.

WAN optimization vendors are well aware of this issue. Most have added Secure Sockets Layer decryption to their products, turning them into SSL proxies. By digging into encrypted content, they can add both compression and caching, resulting in big benefits.

Both network management and security management can work together in this case. Rather than fight the desire of security teams to encrypt absolutely everything everywhere, network managers can support very secure networks and offer performance enhancements by selecting and sizing WAN optimization devices to perform SSL decryption.

Retrofitting the Core Network

For network managers who still run 100 megabits-per-second switches at the edge of the network, talk of 10 Gig-E, 40 Gig-E and even 100 Gig-E at the core sounds unimaginably fast and even a bit of overkill. It's not. Factors throughout the network are pushing a demand for bandwidth from end to end, and building a speedy core is crucial to meeting that demand and supporting future requirements.

Several technologies are pushing demand for ever-higher bandwidth and more reliable networks. These include mobility, video and unified communications, backup and deployments, and business continuity.

Mobile devices, including notebooks, tablets and smartphones, now commonly connect at speeds of 300Mbps and will reach more than 450Mbps over the next few years. The density of mobile devices during group meetings and other collaborative events can generate a huge need for speed from a single wiring closet.

Training videos were just the start. Video conferencing is the next step many organizations are taking, moving to network-based video streams. Video conferencing planners advise allowing for 15Mbps per conference.

When every client system is connected to the network, it's not just user applications that burn bandwidth. Installing, patching, upgrading and backing up hard drives can also put a lot of stress on the network.

As organizations become more dependent on their data networks, business continuity plans depend on the ability to constantly move data between data centers. Enterprise applications such as Microsoft Exchange have amazing business continuity features that also require continuous synchronization of databases.

Network managers should prepare for higher core speeds by looking at architecture, interconnects and equipment bottlenecks.

Core architectures for 10Gbps and faster: Campus network designs swing back and forth over time based on the relative costs of switching, bandwidth and routing. Currently, network trends are pushing toward switching and switch-like technologies rather than routing to handle very high speeds.

Network managers who are thinking of adding 10 Gig-E technology must consider whether virtual LANs (VLANs) and switching should be used in place of some routers and firewalls — and assess the implications of such a decision for control, management and security. At the same time, they should also keep in mind how they will reintegrate routing (if needed) when the relative costs change or as switches gain faster routing capabilities.

Even in switching, network trends will change over time depending on densities, product capabilities and bandwidth requirements. Pushing switched devices up to 10 Gig-E offers an opportunity to re-evaluate network architectures and incorporate new thinking, where appropriate. For example, some networking vendors are pushing hard to move from three-tier network architectures (core, distribution, edge) to two-tier architectures (core, distribution plus edge).

Network managers should take a long view, beyond what the network will look like tomorrow, and think about what it will need to look like in five, 10 or even 20 years — especially as cabling choices and topologies are selected. There's no single right answer to building a network, because every organization has a different set of requirements.

Comparing Two- and Three-Tier Network Architectures

Characteristic	Three-Tier	Two-Tier
Simplicity	More devices, more management	Fewer devices, less management
Latency	More hops, higher latency	Fewer hops, lower latency
Bandwidth and oversubscription ratio	Lower-cost links can be used, but Inter-Switch Links (ISLs) can be a bottleneck because of oversubscription	Oversubscription is less of a concern because fewer devices and links between them are needed, but higher-speed links drive up cost
Power and space	More devices, more power consumed, more space required (Cabling is simplified across multiple devices.)	Fewer devices, less power consumed, less space required (Cabling requires careful planning to achieve densities without a bird's nest.)
Scalability	Very scalable; just add more edge switches as growth is required or devices are added	Not scalable; when the distribution is full, adding another device is a major redesign chore

Interconnects for 10 Gig-E: Many forward-thinking network managers put in piles of multimode fiber (MMF) in the late 1980s to cover their organizations for the next 30 years. But those 30 years are over, and new fiber standards mean that most old fiber can't be driven at 10Gbps speeds. For the short term, fiber will generally be required for 10 Gig-E, because copper 10 Gig-E is not widely available — although a standard has been defined for 10GBASE-T over twisted-pair cable at distances up to 100 meters (Category 6a is commonly used to define this type of cable).

Although many vendors are searching for solutions to extend the life of 62.5µm fiber (usually called OM1), which is currently limited to about 30 meters in 10 Gig-E applications, in-building fiber should be upgraded to OM3, a type of 50µm fiber that has been optimized for 10 Gig-E transmission at up to 300 meters. OM3 fiber (and its associated patch cables) can be easily recognized by the aqua blue color of its jacket. OM4 fiber, sometimes sold as OM3+, takes the maximum distance for 10 Gig-E out to 550 meters and should be used instead of OM3 in cable plant replacements. This is overkill in data centers and for patch cables — at least until the price difference disappears in a few years.

Bringing 10 Gig-E to the desktop via twisted-pair copper (10GBASE-T) doesn't fit into most network managers' plans, and it is not economical to install the kind of infrastructure

that could deliver that bandwidth to every network connector in the organization. In addition to the higher cable cost, every component would need to be qualified for 10 Gig-E, driving up the total price and creating a maintenance nightmare requiring specialized equipment, spare parts and trained installers. For these reasons, it's best to focus on getting 10 Gig-E to the wiring closet and in the data center, and sticking with Category 5e or Category 6 cabling for 1 Gig-E.

When installing cable plant for the next 30 years, neither OM3 nor OM4 cable will help with the 100Gbps jump, as 100 Gig-E is limited to 125 meters over MMF. Instead, single-mode fiber (SMF) will be needed for very large buildings and for inter-building links.

Equipment bottlenecks: For years, most network managers have gotten away from looking for switches and routers with extremely high throughput specifications. With the exception of firewalls, switches and routers are usually capable of very high throughput with multigigabit backplanes, and the exact specifications aren't very important since everything is heavily over-engineered, particularly at the distribution and edge layers. Unfortunately, as speeds edge up and 48 ports of 1 Gig-E fit into a 1U edge switch, oversubscription of Inter-Switch Links has cropped up.

Network managers who never expected to need more throughput from their core switches suddenly run out of gas when speeds approach 10Gbps. The solution is fairly simple: Start paying attention again. In addition to rereading those long-ignored published specifications, network managers should check with vendors about low-cost upgrades. For example, Cisco's Catalyst 6500 Series Switches, which dominate core networks in every type of organization around the world, have been upgraded multiple times with additional capabilities to work around the initial 32Gbps backplane limits.

Optimizing the Data Center Network

For data center managers, the question is not whether they will use virtualization, but rather, "How much will I be virtualizing today?" From the network point of view, server, storage and application virtualization present some challenges. Among them are the following:

- **Physical "mobility" of applications:** An application server may move from one virtualization host to another at any time, and those hosts could be in different cabinets, different data centers or even different time zones.
- **Concentration of bandwidth:** Traditional utilization metrics for LAN and storage networks are inappropriate when a physical host has 10 virtual guest servers on it. If the physical host is actually a blade chassis, the problem becomes 10 times worse.
- **Eggs all in one basket:** Because each physical server has many more virtual systems on it and each storage area network has many virtual servers using it, reliability of the entire system — including the data and storage networks — is more important than ever.

As network managers face the challenges of increasingly powerful servers, the installation of blade servers and the interconnection of SANs, they must accommodate these changes in the data center. Here are some strategies to keep pace with the tsunami of virtualization:

1. Figure out how to handle mobile IP, even across the country.

When an application server migrates from one virtual host to another, it expects to take its network configuration with it. If the server is moving from one side of the building to another, it may be easy enough to keep its subnet alive between racks and rooms. But when the server moves between data centers on a campus, or even across the country, things get more complicated.

Many techniques can solve this problem, starting from the easy option of bridging through very small, special subnets and moving all the way to automatically changing routing and network address translation policies as applications migrate. Network managers must research these techniques and work with application deployment teams to make sure that the network supports — and does not hinder — highly reliable operations.

2. Recalculate bandwidth ratios.

Every network has some level of oversubscription, usually in the uplinks between switches and sites. Bandwidth usage at the edge may be growing a little bit, but inside the data center, the numbers can be much larger. If 10 servers, each of which uses 100Mbps of bandwidth on a single 1Gbps network connection, are all virtualized onto a single host, that 1Gbps connection is probably insufficient. At the same time, the uplink from that cabinet's top-of-rack switch (or end-of-row switch) may also be heavily oversubscribed because of the number of servers in such a small space.

Many network managers are investigating collapsed networks to help resolve some of these issues, but there is no silver bullet. The important first step is to realize that old assumptions about how much bandwidth a cabinet of equipment will generate have all gone out the window, and that every device must be looked at as a potentially heavy source of data traffic.

3. Insist on IEEE standard link aggregation and multi-VLAN rapid spanning tree.

As servers have increased the number of on-board Ethernet ports, many server managers have casually used dual links as a reliability mechanism. A naïve implementation of just

plugging those links into a commodity switch works pretty well — as long as there's not a system failure or the link doesn't get congested.

In the world of blade servers and virtualization, load balancing and a robust high-availability strategy are important. Network managers must understand how IEEE standard link aggregation works across two, four or even more interfaces. Network managers also must work on knowledge sharing and training, and team up with server operating system managers to be sure that they know how to properly configure and use multilink network connections.

4. Add load balancers.

Load-balancing technology was originally designed to handle heavy loads on web applications. Now, however, load balancers are valuable tools in building highly reliable systems. They have even undergone a name change; vendors are calling them "application delivery controllers." With the rise of virtualization and the requirement to quickly identify a system that is paused during migration or maintenance, load balancers have taken on new importance.

Load balancers can also enable highly reliable applications. Many apps have built-in high-availability features, but a dedicated hardware load balancer (or virtual machine in some cases) offers more-sophisticated load-balancing features and is a preferred solution. Tools such as Microsoft's Network Load Balancing are only appropriate for small-office environments and test deployments. This means that network managers should make load balancing available to all applications as a basic part of the network service. Just as application managers assume that the network exists, they should also be able to assume that a reliable load-balancing solution is available.

Especially in their role of application delivery controllers, these devices do much more than load balancing. Features such as SSL acceleration, compression, protocol optimization, caching and connection multiplexing work together to make applications seem faster and more reliable, providing a better user experience.

5. Pay attention to the SAN.

Network managers must get involved with storage area network management because SANs depend heavily on reliable high-speed networks. Organizations that have implemented iSCSI storage already have started to integrate networks, but many that are still using Fibre Channel have built a parallel infrastructure just for storage.

Data network managers need to keep this parallel infrastructure in mind, especially as they move to 10 Gig-E, because the costly Fibre Channel SAN infrastructure can be a drag on the rest of the network. Finding solutions to speed SAN networks and increase their reliability is a good exercise in forward thinking.

Fibre Channel over Ethernet

Fibre Channel over Ethernet (FCoE) sounds, to a network manager, like a great idea: Just stop putting in those separate, funky Fibre Channel switches and use the fantastic Ethernet network to handle all of the storage networking needs. Unfortunately, it's not that simple.

Fibre Channel switches are active devices, providing some security enforcement, keeping data paths separate and isolated, and tightly managed Inter-Switch Links. Moving that processing to a multitier Ethernet LAN is not an easy matter and requires very careful engineering — and possibly a feature set that doesn't exist in current equipment.

Some vendors, such as Cisco, have gone for intermediate solutions, allowing a server or blade server to multiplex Ethernet and Fibre Channel over a single link but peeling out the Fibre Channel at the edge switch, dropping it as quickly as possible into a real Fibre Channel infrastructure. This type of Fibre Channel at the edge doesn't buy much, except for fewer patch cables.

The next steps would be to go for full multihop FCoE, but there isn't widespread agreement on the minimum requirements or how to make this work. And with 10 Gig-E, iSCSI and even Network File System gaining momentum, the case for investing more hardware and network infrastructure in Fibre Channel is getting weaker.

Before leaping into trying to integrate Fibre Channel and Ethernet, network managers should step back and get a realistic evaluation of whether Fibre Channel has a future in the enterprise infrastructure.

Reworking Networks for the Cloud

As organizations have begun to move applications to the cloud, network managers are relieved that they no longer have to worry about them. Moving apps to the cloud, however, requires rethinking some things at the network layer.

- **Bandwidth management:** One usual side effect of cloud computing is an increased requirement for Internet bandwidth and reliability. Network managers should keep service-level agreement (SLA) metrics, such as bandwidth, latency and availability, in mind when they upgrade Internet connections. Adding those metrics to a contract may be difficult for most ISPs.

  No matter whether the SLA is part of the contract, the networking team should be evaluating these metrics and self-reporting how well the Internet connections are holding up as applications move outside the building.

- **Encryption increase:** Many network and security managers have been able to apply security controls, such as data loss prevention, intrusion prevention, URL filtering and application layer controls, because traffic in the LAN may not have been encrypted. When applications move to the cloud, though, encryption is a clear requirement. Security managers will have to figure out how to do their job, typically using tools such as next-generation firewalls (which can handle SSL decryption), as encryption usage skyrockets.
- **Access controls and authentication:** When all of an organization's network traffic resided on a LAN, network and security managers could be sloppy about access control policies by depending on known IP addresses to define permissions within the network. When applications move to the cloud, these controls must be reconsidered, because IP addresses should not be used across the Internet to define security permissions.

Network and security teams should look at network access control to re-establish access control policies based on a user's identity and group affiliations. Cloud-based applications also must be online and integrated with the organization's authentication and authorization system, such as Windows Active Directory.