IDC
Analyze the Future

WHITE PAPER

The Next-Generation Enterprise WAN Aggregation Router

Sponsored by: Cisco

Abner Germanow Lucinda Borovick

March 2008

EXECUTIVE SUMMARY

Businesses are increasingly reliant on their wide area networks (WANs). The quality, security, and reliability of communications between headquarters locations and branch offices, customers and suppliers, as well as the wider Internet are increasingly tied to overall business performance. With the growth of advanced services such as voice and video over IP, mobile data connectivity, remote application access, and unification of wireline and wireless networks, the headend router is being asked to perform a wider variety of functions than ever before.

To support these requirements, headend routers must provide highly available and high-performance data connectivity services. In addition, routers must perform a number of additional functions, including the following:

- Branch services aggregation, to provide the flexibility to handle different types of traffic from multiple locations, often at different speeds, and provide the appropriate level of service required for each
- Bandwidth and traffic management, to provide high performance, flexibility, and application intelligence for advanced data services such as voice and video
- WAN and Internet gateway security, to supplement security devices at the headend by incorporating security functionality such as access control lists (ACLs), VPNs, and deep packet inspection
- Converged communications aggregation, to provide an interface to service providers and enable high-performance, high-availability voice, video, and data communications across the WAN
- Business portal to the outside world, to serve as the primary conduit for Internet-based interactions between the enterprise and employees, partners, customers, and suppliers

In a survey of 200 managers responsible for headend routers and in detailed interviews with WAN managers working for companies with 500 or more employees, IDC identified a number of requirements for next-generation headend routers. They include the following:

- Service capabilities and performance, giving users the ability to incorporate enhanced network services without sacrificing routing performance

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

- Network resiliency and security, providing the ability to withstand failures and infrastructure attacks and maintain consistent service levels under pressure
- Reduced maintenance costs and complexity, providing the capability to easily deploy, maintain, and upgrade the router and associated integrated services
- Support for emerging WAN technologies, with a flexible, modular architecture and clear road map to not only meet new business and IT requirements but also take advantage of technology advancements

This white paper takes a deeper look at these requirements and describes some of the capabilities that will need to be incorporated into next-generation routers designed to meet the changing needs of this market.

Growing Demands on the Wide Area Network

The network is evolving as the primary conduit of business interactions and services. As business functions migrate online, the focus on the WAN increases. No longer viewed as just the plumbing, the network — along with the connection it provides between the business and other networks — has evolved into the lifeblood of the organization. The relationship between business success and IT requires an understanding of and preparation for change while driving service-level improvements across the organization. The WAN is a critical focal point for business performance, IT change, and optimization.

The major CIO challenges that are placing demands on the network include the following:

- Improved service levels to increase customer satisfaction and grow revenue
- Increased flexibility to adapt to new traffic flows and demands generated by new applications, and new business models
- Interconnected infrastructures encompassing an important global network of customers, partners, and suppliers
- Ability to deliver business critical data, voice, and video traffic with consistency, reliability, and security
- Ability to optimize the WAN telecommunications services budget, which is often one of the largest line items in the IT budget
- Evaluation of performance-to-price ratios

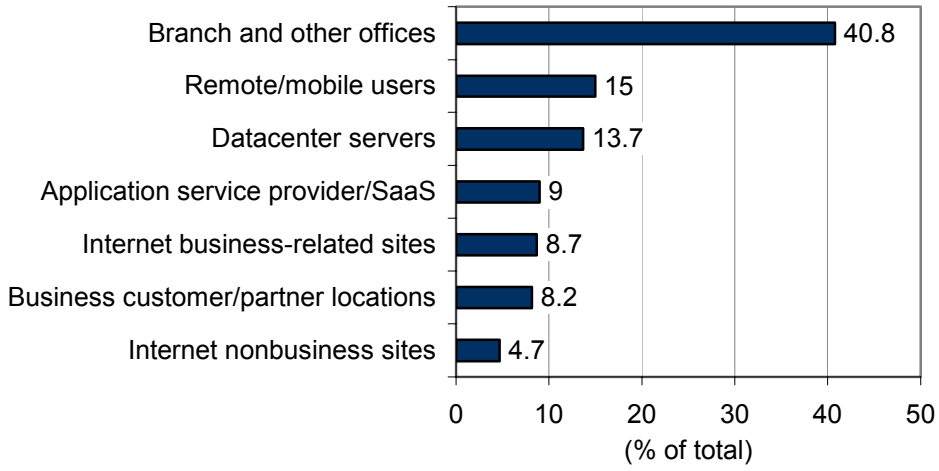
At the heart of the WAN is a headend router that must simultaneously handle today's mission-critical traffic and emerging applications ranging from videos to the new business models. In this white paper, IDC examines the role of the headend router through the lens of the traffic and business issues that the platform is being asked to support. To supplement current knowledge, IDC conducted a Web survey of 200 respondents from U.S. companies with 500 or more employees with responsibility for headend routers. This survey was conducted in November 2007. In addition, IDC conducted telephone interviews with WAN managers. The candidates for the interviews were jointly identified by IDC and Cisco.

The Complex Role of the Headend Router

The headend router serves as the primary connectivity interface between the campus or datacenter and the outside world. Historically, the primary role of the headend router was to aggregate branch and regional office communications, while other external or specialized destinations played a much smaller role. Today, internal branch and regional traffic continues to represent the largest portion of traffic for a headend router, with survey respondents indicating that over 40% of the WAN headend routers are attached to branch and other offices (see Figure 1).

FIGURE 1

Percentage of Traffic Handled by Headend Routers by Source/Destination



Source: IDC, 2008

New Business Trends Create New Traffic Types

Viewed from the perspective of today's business reality, the very nature of the network infrastructure has undergone a profound change. While branch and regional traffic is likely to continue to be the most mission-critical traffic flowing into the headend router, Figure 1 demonstrates how other destinations such as remote and mobile workers along with application hosting and software as a service (SaaS) are becoming increasingly important. As each traffic destination and application set rises and falls in relative importance, it introduces a new set of performance demands, security risks, service requirements, and management needs.

One of the largest new destinations is remote/mobile workers; it eclipses even traffic flow to datacenter servers and is second in amount of traffic only to branch offices. It wasn't that long ago that most employees sat at headquarters in close proximity to the systems running back-office applications. Today, end users are increasingly remote, often working from home offices or on the road visiting customers. At the end of 2007, the number of mobile workers reached 750 million worldwide.

Further, network traffic extends to the realm of nonemployees. Application service provider/SaaS commands 9% of network traffic, with business partners representing 8.2%. This new extended enterprise brings new security and service-level requirements to the WAN infrastructure.

New Types of Traffic Introduce New Complexity

Successfully managing a WAN requires balancing a number of different variables that define success. One of the key challenges is how to deal with the unpredictable nature of today's traffic. WAN managers must be prepared to accommodate change quickly to deal with large surges of bandwidth demand while reducing latency. A vice president of network infrastructure at a large financial institution described this challenge:

> [Business managers ask me …] Exactly how many microseconds of latency am I picking up? Are you sure you're not dropping any packets whatsoever from point A to point B? And by the way … those feeds tend to have these unpredictable loads. What if the financial market goes crazy, then the data feed from the market goes crazy as well, and so traffic can suddenly go up by a factor of 2 to 3 times overnight and then just as suddenly drop back down again? It's very hard to predict when it will happen and exactly how high it will go.

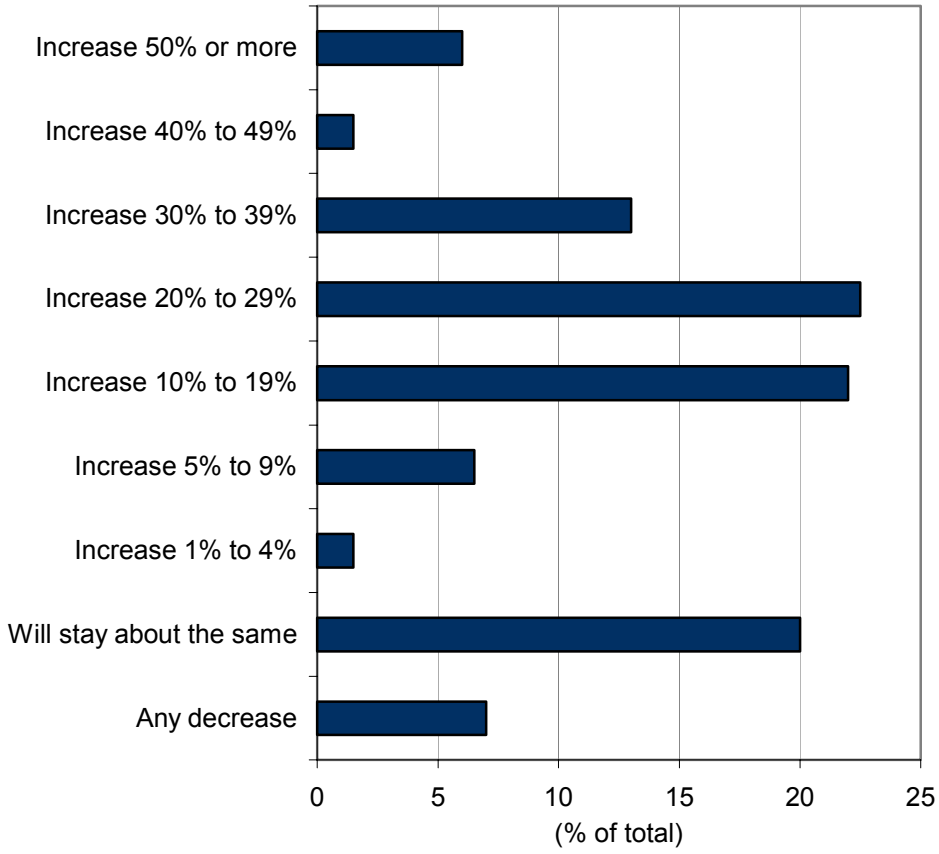
Financial institutions are at the forefront of this curve due to the correlation between trading system performance (of which network performance is a key component) and profit. Elsewhere, the migration of voice and video onto the network is pushing down latency tolerances while overall traffic demand continues to rise. Security is also an important consideration. Network managers must ensure network security without introducing performance bottlenecks. Users don't want to have to trade off security for network performance.

One of the approaches many organizations are taking is to introduce additional bandwidth into their networks (see Figure 2). Fully 73% of respondents indicated they expect to increase their bandwidth at the headend over the next 24 months.

FIGURE 2

Percentage of Traffic Handled by Headend Routers

Q. By what approximate percentage will your bandwidth use change over the next 24 months?



Note: Respondents were asked about the extent of both increase and decrease, but "decrease" respondents were consolidated due to the small percentage of responses.

Source: IDC, 2008

Implementing bandwidth increases of these levels is an expensive option. Addressing new applications such as voice and video by simply increasing bandwidth capacity is not a cost-effective method to dealing with growing demands on the network.

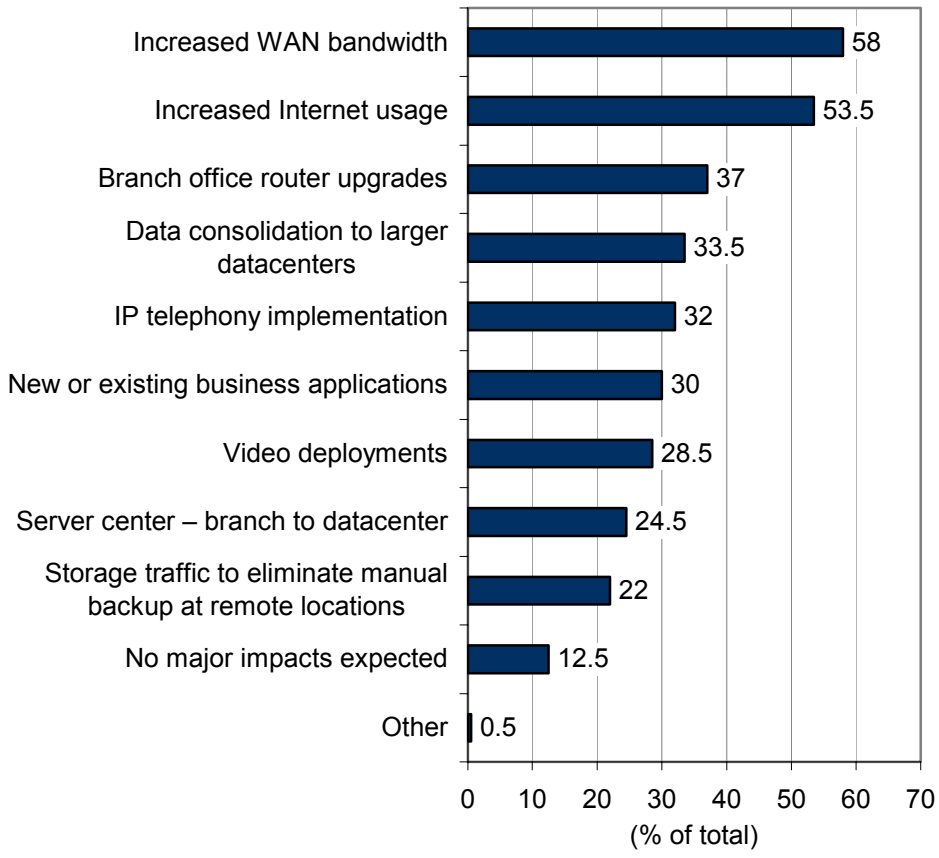
WAN managers should tie expected increases in network traffic growth with ways to intelligently manage that traffic. A next-generation headend router needs to not only support higher capacities but also enable WAN managers to optimize connections, manage the mix of WAN services, and assess and adopt emerging WAN technologies such as MPLS. Other options such as using quality of service (QoS) functions can shield mission-critical applications from the demands of other traffic, but it needs to be easy for WAN managers to enable QoS without sacrificing other attributes of performance and control.

What Functions Must the Headend Router Deliver?

The headend router performs a number of functions both on the platform itself and in concert with security, monitoring, and bandwidth-shaping functions that are often deployed in appliances next to the headend router. Some of the many changes in the network infrastructure that survey respondents expect will impact their headend routers over the next 12 months include increased WAN bandwidth and increased Internet usage, branch office router upgrades, data consolidation, voice and video deployments, and business application support (see Figure 3).

FIGURE 3

Infrastructure Drivers Impacting Headend Routers Over the Next 12 Months



Source: IDC, 2008

To respond to these challenges, the headend router must perform well in the following key WAN roles:

- Branch services aggregation
- Bandwidth and traffic management
- Secure WAN and Internet gateway
- Converged communications aggregation
- Business portal to the outside world

Branch Services Aggregation

The role of the branch is changing. Historically, the branch has been the forgotten, isolated outpost with rudimentary functionality that suffered in form, feature, and presentation compared with the rich data experience in the home office. The advent of new services such as telepresence makes it possible to offer the same business services at the branch as enjoyed at the corporate headquarters or to offer a richer customer experience than competitors. Consequently, companies must rethink their branch office architecture.

To deliver these new WAN services in the branch, companies must upgrade the branch to support rich media for training, collaborative voice and video, radio frequency identification (RFID), surveillance cameras, and even digital signage. This means rethinking how much bandwidth is needed, understanding how security requirements change, and determining how to effectively manage and deliver these new services.

The headend router plays a key role in aggregating this new business application traffic from the branch. It needs the flexibility to handle different types of traffic from multiple locations, often at different speeds, and provide the appropriate level of service required for each, without compromising corporate security standards. Technologies such as QoS, encryption, and WAN optimization all play a role here.

Bandwidth and Traffic Management

WAN services are one of the largest IT budget items for many companies. Consequently, companies would like to avoid the need to expand WAN link capacities whenever possible. When a business application that was designed to run over a bandwidth-rich local area network (LAN) is deployed over the WAN and displays poor performance, it is a problem. Further problems are created when adding more and more applications to the WAN mix. Upgrading the size of the pipe is expensive and does not guarantee long-term performance gains. Rewriting these business applications for WAN deployment is often not an option. IT departments need a way to balance the utilization of expensive WAN links while ensuring that critical business applications meet acceptable performance requirements.

Bandwidth monitoring and management are key elements in meeting those performance requirements. One way to ensure healthy application performance over the WAN is to monitor the headend router jointly with traffic shaper appliances. The problem is this solution does not always scale in concert with the router. The importance of scalability is illustrated by the following quote from a network administrator of a large college:

> When we upgraded from the 25MB [Internet] connection to the 125MB connection, we had plenty of bandwidth for everything. We used to use a traffic shaper on the old connection, but it can't support the higher-speed link, and the high-end traffic shaper is too expensive.

IT departments are in a continual state of balancing WAN costs, end-user performance, and network infrastructure purchases. Traffic patterns shift with business and application changes. The ability to manage this balancing is a challenge for any network manager.

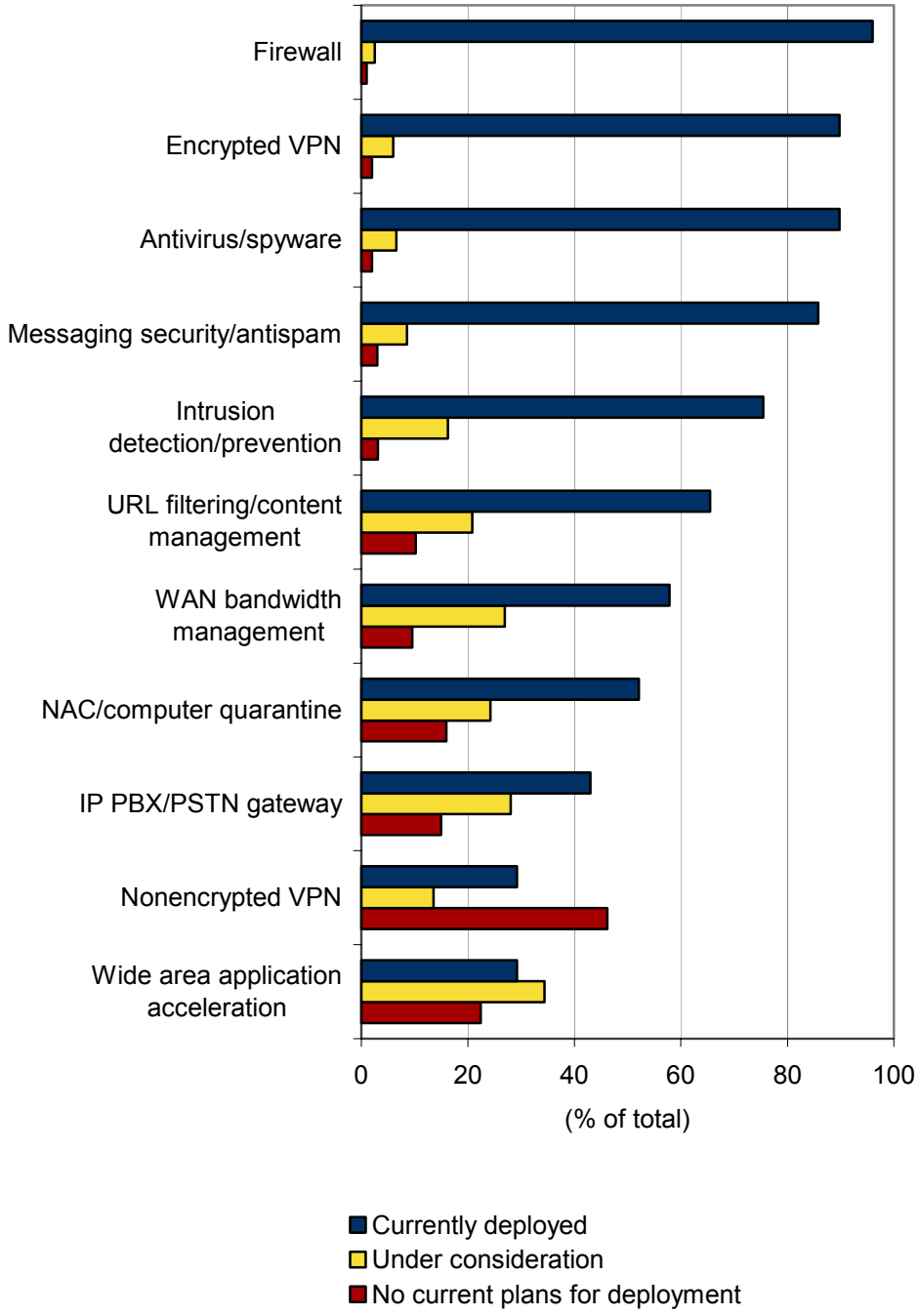
Secure WAN and Internet Gateway

Since the headend router sits as the access point to the WAN and often the broader Internet, it is quite common to find a number of other advanced devices deployed alongside the router, the majority of which are focused on some sort of security or threat detection. The types of security appliances that sit next to the headend router have evolved significantly over the past five years. Beginning with simple firewalls, they have evolved to firewalls with VPN, URL filtering, antispam, intrusion prevention, and unified threat management appliances that consolidate multiple security functions into a single box. Lately, some large companies have also been deploying session border controllers (SBCs) in support of voice over IP deployments and other applications that use SIP.

This point is exemplified in survey results, in which nearly 100% of respondents have a firewall deployed at the headend, with the vast majority also deploying encrypted VPN, antivirus/spyware, antispam, and intrusion detection/prevention devices (see Figure 4).

FIGURE 4

Diverse Advanced Services Are Deployed Next to the Headend Router



Source: IDC, 2008

While many devices may form a complete WAN/Internet security solution, the router itself is often the first line of defense. Security in the router is implemented across the four major planes of router architecture — data, control, management, and services — with much of the security conversation around routers involving the services plane. (Sometimes control, management, and services are lumped into simply the "control plane.") The key to any function running in the services plane is that the processing requirements of that function not be allowed to impede the performance of the data plane functions.

One of the key security features in the router is the use of ACLs in the management plane that stop attacks that do not use standard application protocols. Attempts to use ACLs to provide a secure gateway are useful when a router is first deployed but can deteriorate over time as the lists are either adjusted to make exceptions for new applications or are not adjusted and thus squelch adoption of productivity-enhancing tools. In addition, the use of ACLs can have a negative impact on performance if the router is not optimized for security services.

As traffic processing engines and operating system architectures improve, the headend router will be able to play a larger security role than it has in the past due to the ability to segregate control, management, and services plane functions from the data plane. IDC believes security appliances will continue to play a role in identifying leading-edge threats, while the responsibility for stopping more mature network-level attacks is likely to migrate to the headend router over time.

The WAN managers that we interviewed prefer to continue the separation of security from the headend router, but they also see the value in integrating additional security features into the headend router. One vice president of network infrastructure at a hosting company described his thoughts as follows:

> I think it makes sense to integrate those functions in remote offices and customer sites. In our environment, however, I'm a bit old school, and I think they need to stay separate. Integrating some functions into the router like bandwidth management makes sense, but security threats change much faster than we change our routers.

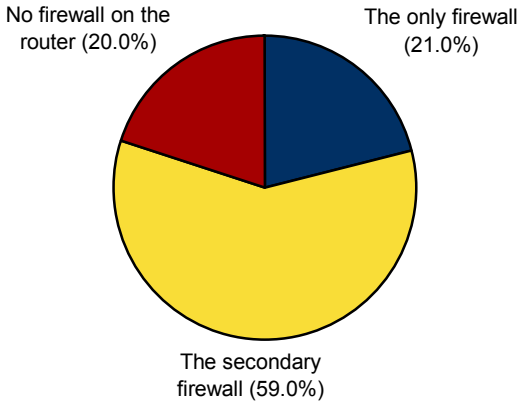
This calls for the need to integrate security on each of the planes in the headend router. The data plane can be secured using techniques such as ACLs, unicast RFP, flexible packet matching, QoS, and IP source tracking. The control plane can be secured using receive ACLs, control plane policing, MD5 authentication, and ICMP techniques. The management plane can be secured using techniques such as CPU and memory thresholding, password and SNMP security, and remote terminal access control, while securing the services plane will depend on the IP services deployed.

In the online survey, we asked users what role firewall functionality would play if they did enable the functionality in the headend router. Fully 59% of respondents said they saw it as the secondary firewall, while 20% stated they would not enable the firewall. The remaining 21% said they could see it as the only firewall (see Figure 5). So there is clearly room for the headend router to play a bigger role on the security front.

FIGURE 5

Role of Firewall Functionality in the Headend Router

Q. If your organization decided to enable firewall functionality in the headend router(s), which of the following would that firewall serve as?



n = 200

Source: IDC, 2008

Note that the few places without firewalls are often very high-performance datacenters with a singular purpose such as videostreaming.

Converged Communications Aggregation

The headend router has two significant responsibilities in enabling converged communications: interfacing with service providers and enabling high-availability and high-performance voice and video communications across the WAN.

As the service provider interface, the headend router sits between the enterprise and a growing number of communications services ranging from SIP trunking, to PSTN gateways, to intercompany telepresence dialing services. Larger companies are beginning to mirror service provider communications deployments by deploying SBCs at the headend to control SIP signaling and monitor the setup and teardown of media streams. Today, SBC functionality is deployed in an appliance deployed next to the headend router, but next-generation routers will have either embedded SBCs or increasingly tight integration with SBC appliances.

In support of voice and interactive video traffic, the headend router must be able to provide for consistent service levels — regardless of the network load — to maintain exemplary voice and video session performance. Here, low latency is an absolute requirement. Additionally, rapid recovery and traffic control mechanisms must be in place to ensure voice and video session stability at all times. On-demand and live streaming video, while not requiring the low latency and session stability of a videoconferencing session, still demand lots of bandwidth — bandwidth that must be shared with other business-critical applications.

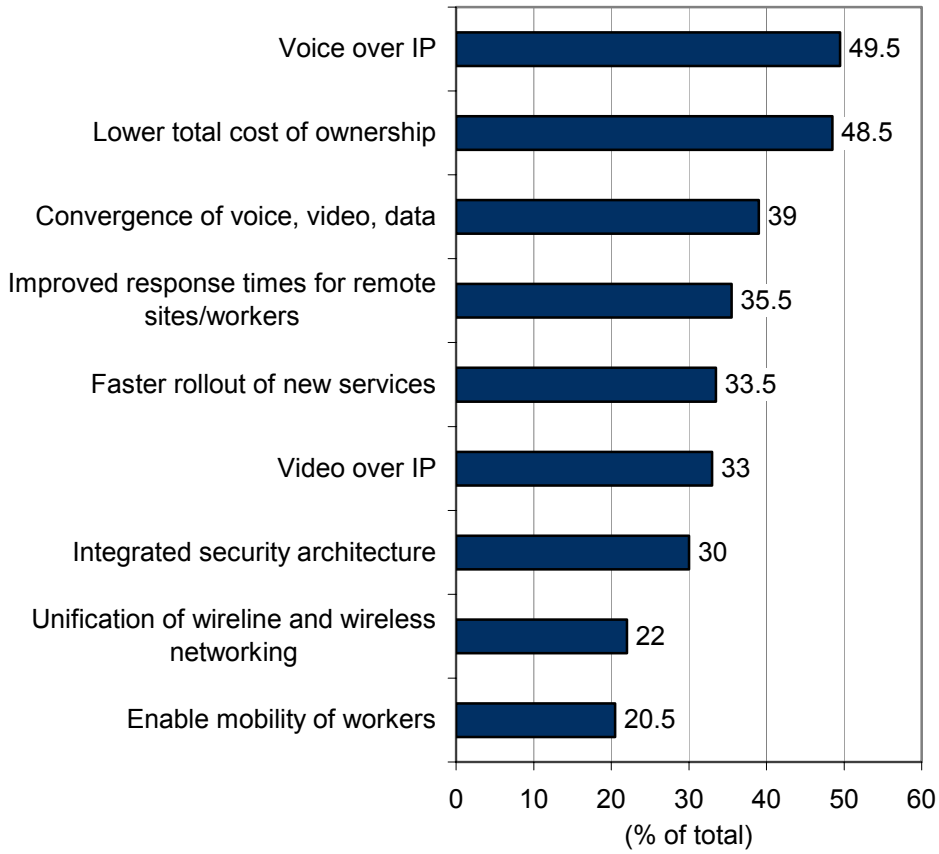
IDC interviewed one manager of a global ring (mostly OC-3) WAN who had enabled eight QoS classes on the WAN to deal with the combination of voice and semiconductor design files flowing over the same network:

> We have a situation where we have a number of applications that tend to be transactional where response time matters as well as voice on one side of the spectrum, and on the other side of the spectrum, we have a handful of applications that we want to limit what they can do. We had to develop a scheme to help manage all of that.

The survey also pointed to the importance of headend routers being able to support converged traffic, with 49.5% of respondents saying their WAN needs to support voice over IP, 33% requiring it to support video over IP, 22% needing it to provide unified wireline and wireless networking, and 39% specifically calling out the need to support converged voice, video, and data (see Figure 6).

FIGURE 6

Key Services and Attributes Users Intend to Support on Their WAN



Source: IDC, 2008

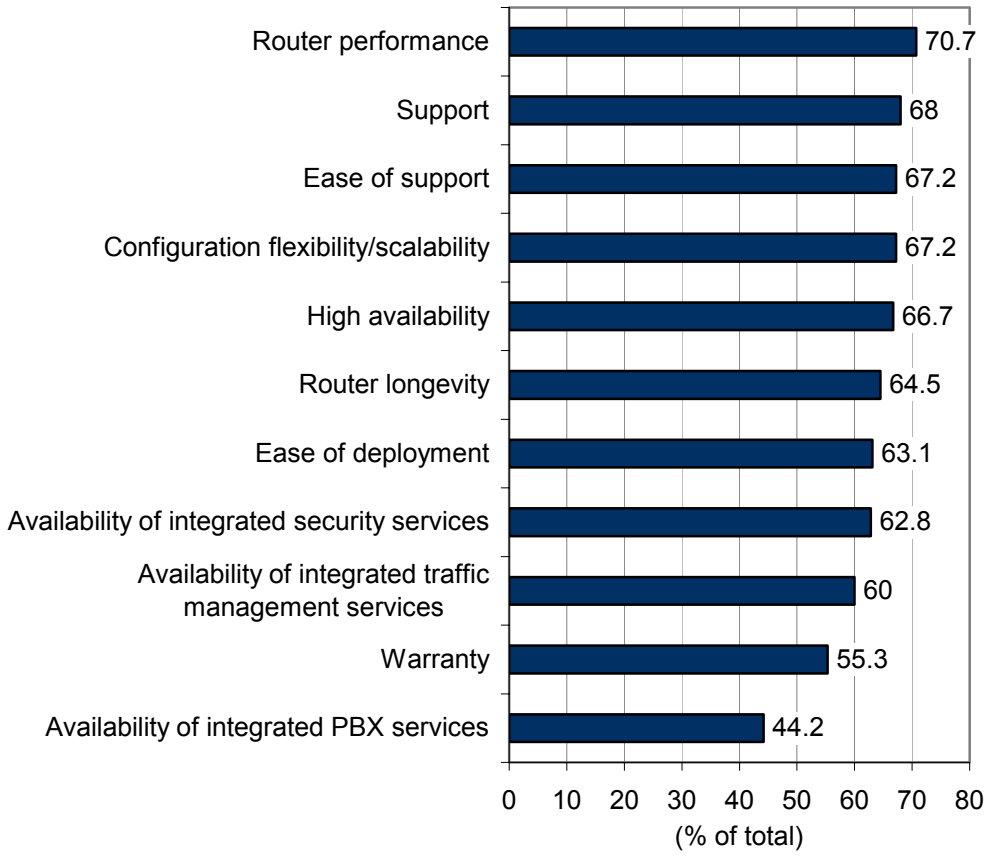
Business Portal to the Outside World

The headend router plays a quiet role in the quality of a growing number of interactions between the enterprise and employees, partners, customers, and suppliers. Every external or remote user accessing a company Web site or service will flow through the headend router. As more and more of the business services for both the enterprise and the service provider are built on IT technology, the link to the outside world becomes ever more mission critical. The headend router needs to be able to provide secure, highly available, and high-performance access for the available business applications. Failure to provide such critical access can have a negative impact on customer satisfaction, partner relationships, supply/distribution operations, and business reputation and performance.

The importance of router performance is borne out by the survey data, in which the largest percentage of users (70.7%) rated it very or somewhat important when evaluating a new headend router platform. In addition, fully 66.7% of users rated high availability as very or somewhat important (see Figure 7).

FIGURE 7

Users Rating Criteria Very/Somewhat Important When Selecting New Headend Router



Source: IDC, 2008

CHANGE IS CONSTANT — CHANGE IS RISKY

The location of the headend router puts it in the critical path for delivering WAN-related services. Consequently, it is one device that IT departments would rather not touch. Any kind of configuration change or update could result in failure, and that would mean cutting off everyone on the other side of the link from the business. To shift and adapt to connectivity, traffic, and service changes, headend routers need to be reconfigured; however, making these changes introduces risk.

The ability to quickly add new services, more connections and bandwidth, and increased traffic loads at the headend is critical to nurturing new business opportunities on the network. Despite this situation, network managers are reluctant to make changes to the headend router unless something is broken or a major WAN redesign is under way. On the one hand, this reluctance to make changes is understandable given the business impact of losing any traffic running over the headend router and the increasingly narrow maintenance windows available to bring down any portion of the network.

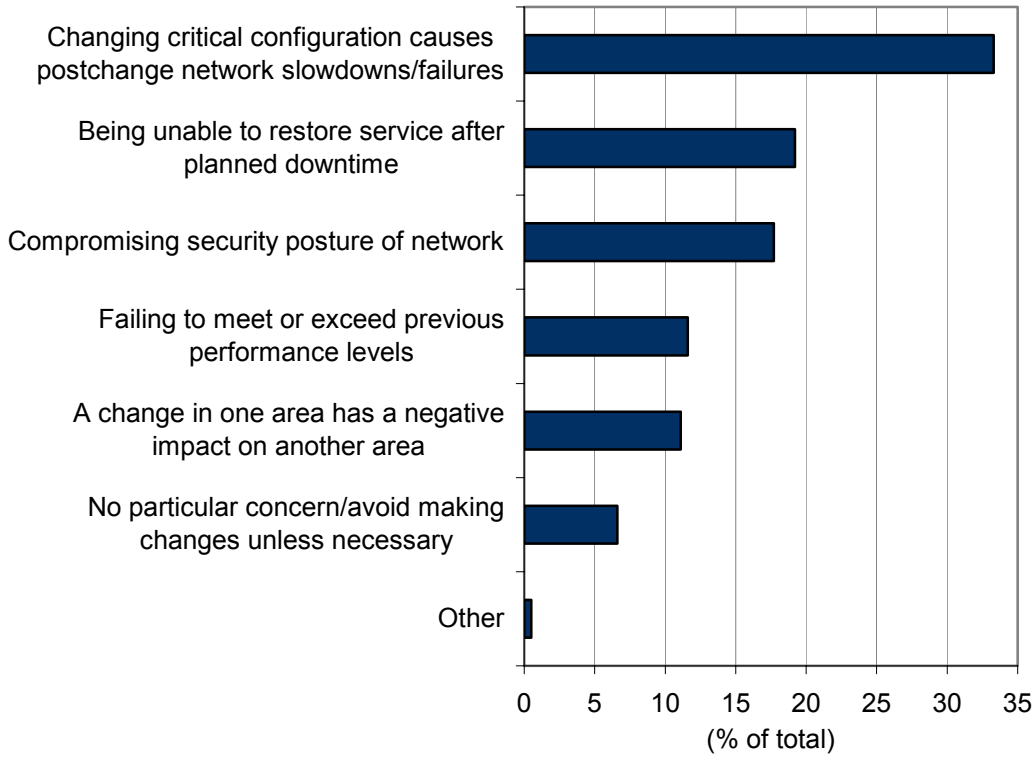
On the other hand, this practice of making changes only when absolutely necessary can bring bad results — results such as higher WAN services costs, security vulnerabilities, or service shortcomings. If the WAN headend is not properly managed, it could result in network instability or disappointing WAN service levels — characteristics that may be more costly and risky than proactively making changes to the WAN that optimize WAN service options and security functions.

The challenge facing administrators can be seen in the user survey results, in which 34% of respondents said that their single biggest concern when performing configuration changes to the headend router would be potential network failures or slowdowns (see Figure 8).

FIGURE 8

Challenges When Making Configuration Changes to the Headend Router

Q. Which of the following concerns you most when making changes to the headend router?



Note: Multiple responses were not allowed.

Source: IDC, 2008

The Key Requirements for the Next Generation of Headend Routers

Companies currently looking to upgrade their headend routers must make their selection based on the router that not only can best handle today's needs but also can grow and evolve to handle emerging network requirements.

The role of the headend router will continue to gain importance and sophistication as more of the critical business applications migrate from the LAN to the WAN. The requirements for the next generation of headend routers must take this into consideration while providing the capability to ramp up for new types of traffic and traffic patterns to ensure consistent and reliable performance across the WAN links as new business services are added.

Specific requirements for the next generation of headend routers include the following:

- Service capabilities and performance
- Network resiliency and security
- Reduced maintenance costs and complexity
- Support for emerging WAN technologies

Service Capabilities and Performance

For buyers to be receptive to adding additional capabilities onto the router, they will need to be convinced that these technologies will have zero impact on router throughput. Given the growing number of security and traffic management devices that reside in the same neighborhood as the headend router, companies may want to consolidate a number of services into the router. Advantages of such consolidation include reducing the datacenter footprint, reducing power and cooling requirements, and reducing management complexity.

For companies to ensure high QoS, it will become increasingly necessary to properly govern the use of the WAN by an increasingly diverse and demanding set of business applications. While use of such governing features as QoS on the WAN is still rare today, as traffic volumes grow on the WAN, the headend router will play a crucial role in making sure the WAN can protect, prioritize, and deliver all needed application flows. IDC believes the number of companies that enable a limited number of classes of service on the WAN will increase significantly over the next several years. The migration of voice to the network is in progress in mainstream IT infrastructures, and the use of video is moving from light entertainment to business useful and even business critical in some environments.

Additional buyer requirements for next-generation headend routers with regard to service capabilities and performance include the following:

- Support for a diverse set of services and the ability to easily add and support new services as they become available, including security, voice, and video
- Easy deployment of and support for services with support for streamlined certification and change management processes
- Ability to provide a complete and clear understanding of any performance constraints that might come into play when enabling new services
- Ability to easily and painlessly add or subtract new services without impacting the network
- Clear articulation of what licensing fees are associated with these services

Network Resiliency and Security

Network resiliency and security are critical to delivering service levels to the business. A resilient network not only offers the appropriate service levels under ordinary circumstances but also can maintain service levels under extraordinary circumstances. Here, the ability to reroute around a link failure, fail over away from a faulty component, and prevent security breaches is critical in avoiding service disruptions. Peace of mind for WAN administrators is knowing that sufficient redundancy and recovery capabilities are built into the system in the event of a failure or a problem. Or in the case of configuration errors, systems can be easily rolled back to previous or original configurations. And in an age of viruses, Trojan horses, and denial of service attacks, providing a high degree of network security is more important than ever.

Specific requirements for next-generation routers with regard to network resiliency and security include the following:

- Hardware component redundancy such as dual processors, so when one component fails another is ready to immediately take its place
- Software redundancy and recovery features, such as multiple software images providing similar failover and rollback functionality to that found in most router hardware components today
- High-availability capabilities that ensure that failure of individual service features has no impact on network connectivity and routing performance
- Router architecture that ideally separates control plane functions from packet-forwarding functions
- Integration of enhanced security features on each of the planes in the router: data, control, management, and services
- Network infrastructure protection at critical WAN/Internet gateway
- Automated management features such as automatic notification, diagnostics, and troubleshooting tools in case of device or component failure
- Flexibility to support multiple different types of network design configurations
- Scalability to provide the router with enough head room to expand as the need arises

Reduced Maintenance Costs and Complexity

There is no arguing that business is moving faster and faster in today's networked world. Given the central role of the headend router in today's IT and business environments, the time required to deploy new services or accommodate new traffic types or connect to more cost-effective telecom services must be minimized if the router is to properly serve the organization. Time saved on testing, configuration, installation, and service deployment is of great benefit to not only the network staff but also the business itself.

Headend routers must also be maintained and updated on a regular basis if they are to keep pace with changes in the network. Unfortunately, many headend routers today do not receive sufficient maintenance and updates. Fear of disrupting a stable environment, lack of time to perform necessary tests and upgrades, unwillingness to suffer user downtime, and costs all play a role.

Organizations running routers with out-of-date firmware and software risk reduced operational efficiency of the devices and put the WAN links at greater risk of latency or even failure. The next generation of devices must step up to the plate and provide a maintenance solution that alleviates these concerns while reducing the cost and hassle of maintaining these devices.

Additionally, as next-generation routers provide for more and more networking services traditionally associated with standalone appliances or server software, there is an opportunity to further simplify the headend WAN infrastructure. Integrated services enable the next-generation router to reduce the number of devices controlling the headend WAN. This device reduction not only eases the network support burden but also provides relief for power, cooling, and space requirements associated with the network.

Buyers will be looking for the following improvements in maintainability of next-generation headend routers:

- Reduction in time to test and deploy
- Remediation capabilities to quickly and easily roll back configuration changes
- Regular and low-impact upgrades (in terms of risk, costs, and time) of components such as processors, individual modules, and software/firmware to save money, boost performance, improve service, and extend the life of the router
- Simplified device management to reduce the cost and time for staff maintenance work and training and enable more time for WAN administrators to focus on incorporating new innovations

Support for Emerging WAN Technologies

IT departments want the flexibility of adding new WAN infrastructure technologies and services (such as security, application acceleration, voice and video delivery, and QoS) as less expensive and more effective WAN offerings become available. They do not want to be locked into a limited set of telecom services or even broader WAN design by their headend router. Nor do they want to miss an opportunity to further strengthen their security posture or offer heightened application service levels. WAN services cost dearly, but new technologies are constantly appearing that provide lower cost, increased capacity, improved security, and greater availability. Next-generation headend routers need to give IT managers the flexibility to swap their WAN services contracts to achieve the proper balance of cost, capacity, and reliability that meets their ongoing needs. Items that buyers would like to see include the following:

- Clear network design and product road map that points to rapid adoption of new WAN connectivity options
- Scalable performance characteristics that support not only more and higher-speed connections but also a greater mix of networking services across these connections
- Hardware and software structure that readily accommodates new connectivity, capacity, and service demands, allowing graceful WAN headend migrations in the near term and lengthening router service life over the long haul

CONCLUSION

As an increasing number of business services and interactions move online, the network is evolving and incorporating a wide variety of new technology and functionality to keep pace. This evolution places a greater burden on headend routers to integrate additional functionality such as support of converged communications, consolidated network management, and integrated security, all while maintaining consistent performance levels and a low total cost of ownership profile.

In a survey with 200 managers with responsibility for headend routers, supplemented by telephone interviews with WAN managers, IDC probed the requirements for next-generation headend routers. IDC found that in addition to providing high-performance support for data services, the next generation of headend routers will need to provide robust network resiliency features, converged communications support, reduced maintenance costs and complexity, as well as a flexible architecture to support tomorrow's generation of emerging WAN technologies.