A Two-Tier Architecture for Converged Networks

Abstract

This paper discusses the key requirements that IT organizations should consider when building a network. In brief, the network should provide high availability, voice-quality network connections, comprehensive security and ease of management and operations. We will introduce the concept of the two-tier architecture as a way to effectively achieve these four stated requirements and the benefits of migrating from a three-tier network architecture to a more streamlined two-tier architecture. Individual network components become the building blocks in delivering a streamlined and effective network capable of meeting the demands of current and future business convergence initiatives.
Introduction

Ethernet and IP are the basic ingredients of the modern enterprise network. The ubiquity of these protocols has simplified the choice of networking products and design. While the days of protocol wars are long gone, the IT organization should not be fooled into a false sense of security by the standardization of the IP/Ethernet network. While it is true that the advent of a single, standardized protocol increases simplicity, the network must assume a larger role in supporting emerging applications. The rapid pace of technology innovation is forcing businesses to evaluate the opportunities that applications like IP Telephony offer. At the same time, the business must be more effective in detecting and responding to the security threats of a highly inter-networked world.

IP Telephony is reaching critical mass within large enterprises causing many IT organizations to reevaluate their assumptions about network design and availability. Voice over Wi-Fi has emerged as an application that could drive widespread wireless adoption within the enterprise—forever shifting traditional network boundaries. Advances in Power over Ethernet (PoE) have given birth to new applications like network-based security surveillance and promise to reduce the cost of provisioning IP telephones and wireless Access Points (APs). However, each of these new initiatives comes with its own intrinsic complexity that—given the multipurpose nature of the network—must be closely managed.

A pressing item on every IT organization’s agenda is how to cope and respond to internal and external security threats. It is no longer sufficient for the network to simply resist these threats; rather, the network must play an active role in the identification, quarantine and resolution of threats as they occur.

The modern network not only provides connectivity between users and resources, but also the services required to guarantee the integrity, responsiveness and quality of this connection. To respond to this added complexity, enterprises are forced to reevaluate staffing plans and training programs—at the same time while being pressured to decrease overall staffing levels!

Just as application demands, security threats and staffing requirements have evolved, so too must the network. This paper discusses the key requirements that IT organizations should consider when building a network. In brief, the network should provide high availability, voice-quality network connections, comprehensive security and ease of management and operations (see Figure 1). We will deconstruct the historical view of how to architect a network and ability to dynamically stop/restart and load/unload software modules without impact to network and introduce the concept of the two-tier architecture as a way to effectively achieve these four stated requirements.

Individual network components become the building blocks in delivering a streamlined and effective network capable of meeting the demands of current and future business convergence initiatives.

Figure 1. Requirements for Convergence

A Historical View of Network Architecture

The arrival of the Internet forced network architects to reevaluate the way in which they designed networks. Traffic patterns were turned upside-down as the business became increasingly dependent on the Internet to deal with suppliers, partners and customers. Scalability became the buzzword of the day. Vendors delivered products capable of gigabit and subsequently 10 Gigabit Ethernet speeds. These capacity advancements allowed enterprises to alleviate bottlenecks and create a network for the Internet age.

However, enterprise demands have not kept pace with these capacity offerings. Rather, other criteria have surfaced as being more important than pure speeds and feeds. Many vendors have succeeded in supplying customers with sufficient capacity, yet few have met demands needed to support a converged communications infrastructure. The age of voice, video and data convergence has superseded the Internet age. IT organizations now require a network capable of supporting a plethora of emerging convergence applications. The network must deliver a consistently high quality of connectivity and be secure and simple to manage. This new paradigm of converged communications requires a fresh approach to network architecture, and simplicity is key. Incumbent network design principles are complex and are proving a hindrance as enterprises seek the benefits of a converged infrastructure.
Several leading vendors have long advocated the segmentation of the network into three tiers—core, distribution and access. The stated purpose of the three-tier design was scalability. Traffic was groomed as it passed from access to distribution to core so as to limit network contention. It was believed that a three-tier network improved network availability by segmenting operational domains. Routing and policy enforcement were often available only as a function of the core, while high-speed switching and aggregation capacity were relegated to the distribution layer. The access layer lacked intelligence and was limited in its ability to deliver non-blocking throughput for end-user traffic. Thus, rather than serving a functional purpose, the three-tier architecture was born from a need to hide product deficiencies.

Still, many vendors preferred the three-tier architecture as it encouraged users to purchase substantially more network devices. By building products capable of line-rate routing and switching with full service enablement, vendors could allow enterprises to collapse the network from three layers to two. This presents certain vendors with a business dilemma since by collapsing the network into two-tiers, enterprises require fewer products and have the ability to lower their overall expenditure on network equipment.

**Simplifying the Network Through a Two-Tier Architecture**

The concept of the two-tier network architecture is derived from the IT organization’s inherent desire to simplify its infrastructure. The end goal is to build a network for convergence—one that has the extensibility to support a variety of new applications in a highly available and secure fashion. While the two-tier architecture represents a simplification of previous designs, it does not represent a compromise in terms of quality, availability, security or management. As the name indicates, the two-tier architecture is a collapsing of layers into intelligent core and unified access (see Figure 2).

**Unified Access**

The edge of the enterprise network has evolved substantially over the past five years. Historically, users accessed the network through hubs—a shared medium incapable of dedicating bandwidth or offering any additional services. Today, not only can the edge scale to meet the bandwidth needs of any user, it can offer both wired and wireless access alternatives.

**Universal Port**

The universal port takes away the guess work from matching Ethernet ports with the function of the endpoint. The combination of Gigabit Ethernet and PoE into a high-density form factor results in a universal port—an ideal connection point for any mix of IP telephones, wireless APs or PCs. The universal port responds to the proliferation of networked devices by offering IT organizations growth without compromise. The switch delivers the power required by each individual port without the need for tedious upgrades to power supplies or compromises on how devices can be connected and powered. At the root of the two-tier architecture is the ability to collapse the access and distribution layers. This is achieved by eliminating the need to groom traffic as it passes from access to core. Performance without compromise in the access layer is essential to providing the scalability required to collapse layers and Extreme Networks® has designed its access products to provide line-rate switching across all ports at all speeds—no compromises.

A key feature of the universal port is Extreme Networks’ AccessAdapt™ technology. This innovative feature is embedded into access layer switches and is capable of determining the function of the connected device. Armed with this information, the switch can automatically and appropriately configure the connecting device and enact certain policies as dictated by the administrator. For example, using AccessAdapt, the switch could automatically assign a specific virtual LAN (VLAN) and Quality of Service (QoS) parameters to traffic originating from an IP telephone or a wireless AP connected to the universal port. In doing this, the switch eliminates the need for a network administrator to manually intervene to assign specific VLAN tags or QoS rules. The connected device takes its personality directly from the port. An IT administrator can relocate a wireless AP from one part of the building to another without worrying about reconfiguration. AccessAdapt automatically recognizes the AP and delivers the appropriate configuration information.

© 2006 Extreme Networks, Inc. All rights reserved.

A Two-Tier Architecture for Converged Networks—Page 2
AccessAdapt simplifies moves, additions and changes and can alleviate much of the complexity in administering usage policies across wired and wireless, and voice and data networks.

**Voice-Class Availability**

A network is only as available as its weakest link and high availability is critical in the new flexible access layer. Converged communications has raised the bar in terms of the level of uptime and IT organizations expect their network to provide the same level of availability as traditional PBX and voice standards. Historically, the access layer has taken a best effort approach to availability. Today, IT organizations must insist that new access layer products deliver a level of availability on par (if not better) than traditional telephony products. Extreme Networks has delivered a product portfolio with a high level of design redundancy at the component, system, and Operating System (OS) levels. All components are provisioned with n+1 redundancy including management modules and switch fabrics. Furthermore, Extreme Networks has innovated in the area of resiliency protocols to offer Ethernet Automatic Protection Switching (EAPS) RFC 3619 for sub 50 millisecond network layer failover for consistent and predictable recovery behavior regardless of where link failures occur. Finally, the ExtremeXOS™ modular OS provides users with the flexibility to conduct upgrades (or planned downtime) in real-time without the need to power down or reboot. The need for voice-class availability spans the breadth of the network and the access and core layer features become interdependent to provide the utmost in resiliency.

**Access Security**

IT organizations are faced with an onslaught of new security threats including unauthorized users, unauthorized access to resources, infected laptops, and Day-Zero threats. Extreme Networks has pioneered intelligent network access security service to help ensure only authorized and compliant users and devices gain network access. Extreme Networks is able to authenticate a user or device and enforce predetermined policies based on the authenticity of the entity. The network then works with industry partners from the Trusted Computing Group, to perform an integrity check and determine the “security health” of the authenticated device by verifying that this device carries no infection and poses no threat to the rest of the network. Only authorized users with healthy devices are allowed on the corporate network while unauthorized users with unhealthy devices are quarantined and cured (see Figure 3). Additionally, access layer switches have been “hardened” to mitigate some of the risk of attack and to withstand harmful behavior directed at the switch itself. Security features across the core and access layers must mesh to guarantee the highest level of network integrity. Extreme Networks security framework is designed with flexibility in mind and control can be handled at the access or core layers depending on the IT organization’s requirements and preferences.

![Figure 3: Action Policies Based on Authentication and Integrity](image)

**Intelligent Core**

In the two-tier architecture, the core is the aggregation point and the anchor of the network. The core must provide enough horsepower to switch and route packets with ease while also enforcing policies and delivering intelligent services.

**Network Determinism**

As the work horse of the network, the core must be capable of delivering consistency and quality of connection. Latency and throughput must remain constant irrespective of application type. Applications and different device types introduce variability into the network. By acting in a deterministic fashion, the core preempts this variability and provides a higher QoS for all applications. Extreme Networks achieves this functionality through significant provisioning of hardware and software buffers, large routing tables and a mesh architecture that increases scalability and redundancy without increasing complexity or cost. Furthermore, the dual homing of uplinks into the core combined with the ability of links to operate in standby mode allows for greater flexibility in the way in which the network core aggregates traffic of varying types (e.g. data center, end-user).

**Carrier-Class Availability**

The mission critical status of the network has risen dramatically over the years as more and more business functions become inextricably tied to network availability. Extreme Networks extends its focus on delivering a network capable of exceeding the availability requirements of voice and other mission-critical applications from the access layer into the core. At first glance it is easy to view carrier-class availability as a measure of uptime—typically relying on the well known five 9s scale (e.g. 99.999% uptime). However, such numbers are often difficult to measure and validate. It is generally unclear whether these numbers refer to individual switch performance, network system performance or application performance. Operations teams frequently lack a solid understanding of how to
measure such performance. A preferable approach to quantifying network availability is to focus on the time it takes for the network and applications to return to full operational capability.

Within the context of an overall high availability strategy, network architects must consider all facets of switch/router performance from the component to the system level. The collapsing of network layers simplifies the network and thus promotes high availability. Extreme Networks has demonstrated its understanding of high availability requirements by offering the EAPS protocol. In addition to sub 50 milli-second failover, EAPS offers quick recovery at Layer 2—obviating the need for any re-convergence of routing protocols at Layer 3—and provides scalable network segmentation and fault isolation. By collapsing network tiers into core and access, Extreme Networks is able to more effectively ensure that high availability is a service delivered across all layers of the network. While some environments favor complete device level redundancy (e.g. data centers), IT organizations can simplify the remainder of the network—favoring lower costs, while maintaining a high level of uptime.

Core Security

Security becomes an important issue in the core due to the possibility of malicious traffic affecting the aggregate. The network core and access layers must work cohesively to ensure the broadest level of defense against malicious activity. Layer 3 Virtual Switching is a unique offering from Extreme Networks that leverages existing firewalls to isolate traffic flows at Layer 3 based on predetermined policies—a feature that mirrors the capabilities of the intelligent network access in the access layer. IT organizations can establish various access policies based on employee function, line of business or any other predetermined grouping. In addition to the Layer 3 Virtual Switching capability, Extreme Networks also offers CLEAR-Flow—the ability to inspect traffic and gather information which can then be passed to third party security appliances for further action. CLEAR-Flow builds on the access layer's ability to regulate traffic flows using granular ACLs, but also allows the network to respond to Day-Zero attacks by quarantining suspect traffic. CLEAR-Flow relies on external appliances for additional levels of security (e.g. IDS/IPS), freeing the network core to perform its primary function—delivering scalable bandwidth and advanced services to the entire enterprise network. Thus, instead of trying to integrate security directly into the chassis through bolt on modules, Extreme Networks leverages CLEAR-Flow to integrate "cutting edge" functionality from leading security technology vendors.

Modular Operating System

The network OS has evolved to be one of the most complex parts of the entire network. As certain vendors’ product offerings have evolved over time, the OS has taken on a life of its own—often time splitting into various strains and code bases. Extreme Networks has again taken an innovative approach to ensure the simplicity of its system. The key characteristic of the ExtremeXOS is its modularity. Prior to modularity, network operators were forced to reboot the entire OS to recover from process failures. A reboot was also required to add patches or new features to the system. With the advent of modularity, the system supports hitless software upgrades and maintains dual images to allow network technicians to “fail back” to the former versions of code. Furthermore, the software can isolate specific areas or faults to allow for additional maintenance without impacting the operation of other software modules. ExtremeXOS spans core and access layers decreasing the need for the administrator to learn and support multiple versions.

Why Now? What Has Changed?

Organizations resist change. As a result, there has to be a good reason for enterprises to veer from the incumbent position. Up to this point we have discussed the reasons enterprises architected a three-tier network. We have also outlined the components that make up the two-tier architecture. However, we have yet to discuss what has changed in the industry to make this shift possible. The combination of advancements in the following areas has paved the way for overall network simplification.

Gigabit and 10 Gigabit Ethernet

The initial standard for Gigabit Ethernet revolutionized the enterprise networking market. It gave birth to a plethora of new equipment manufacturers eager to offer customers greater network scalability at a lower cost. Since the ratification of the 10 Gigabit Ethernet standard, adoption has remained limited. The majority of enterprises have yet to invest substantially in 10 Gigabit Ethernet—largely due to a lack of immediate need. However, as vendors continue to increase economies of scale, price points are dropping to a point where it becomes cost-effective for average enterprises to deploy the technology. By deploying 10 Gigabit Ethernet links between the network access and core, IT organizations can scale the access layer without worry of contention. These 10 Gigabit Ethernet links allow enterprises to remove the distribution layer as both core and access switches have enough capacity to aggregate traffic.

Wire-Speed Access Layer

Incumbent vendors have had limited success in developing access layer switches capable of switching at wire-speed with a high-density of Gigabit Ethernet ports. This lack of horsepower was a key reason many vendors advocated a three-tier architecture. Extreme Networks delivers access layer switches that are non-oversubscribed—passing packets at wire-speed on all ports.
This level of performance allows network architects to shift their focus from limiting network contention to the support of more advanced IP applications such as converged communications. With high-performance access switches the need to groom traffic across multiple layers is no longer necessary.

High-Density PoE

Still relatively young feature in the networking portfolio, PoE has the promise of substantially decreasing the cost required to deploy a converged infrastructure. IT organizations have the flexibility to power any mix of IP telephones, wireless APs and IP video or surveillance end points. Previously, IT organizations were forced to buy specific switches or mid-span products capable of injecting power onto the wire. With the Extreme Networks universal port concept, this additional step is eliminated and the enterprise is left with an infrastructure that provides the greatest degree of flexibility and investment protection.

Active Network Security

Once considered part of the problem, the network has emerged as the key enterprise tool in detecting and responding to security threats. The integration of security functionality into the three-tier architecture has been complex and costly to manage. Security policies must be implemented and maintained across three layers and a multitude of devices—potentially increasing the risk of security holes through oversight and poor processes. By simplifying the network into two-tiers, the number of security zones can be decreased to a more manageable number. IT organizations can leverage technologies like Intelligent Network Access and host integrity services to ensure a secure access layer. Extreme Networks offers Layer 3 Virtual Switching and CLEAR-Flow as security tools to help guarantee the integrity of critical data within the network core. Both access and core security can be unified through the Extreme Networks EPICenter® management framework to provide IT organizations with a unified view of security and compliance levels across the organization.

Limitations of a Two-Tier Approach

This paper must recognize that a two-tier network architecture may not be appropriate for every enterprise. Some enterprises may be limited by physical or organizational constraints. A two-tier network design is ideally suited for enterprises with Greenfield environments or with sufficient space and modularity within the building to handle the consolidation and changes necessary to migrate from a three-tier approach. Enterprises with long distances between core and access may find it more cost-effective to include additional network layers to ensure reach of traffic flows. An example of this may be a large manufacturing campus with distributed production locations. In other cases, organizations that occupy historical buildings with older cable plants or restrictions on physical infrastructure changes may also be limited in their ability to cleanly migrate to a two-tier design. While a two-tier design should decrease the amount of space required for the physical housing of switches, some building layouts may not have the flexibility of providing space where it is required.

As a general rule, enterprises with a physical separation between the data center or access layer and the core that is greater than 100 meters for copper runs and 300 meters for multi-mode fiber, could be faced with the relatively more expensive option of using higher powered optics to cover the greater distances. This additional cost should be weighed carefully against the cost of supporting additional network layers. Fundamentally, the largest issues prohibiting a two-tier architecture are distance, age of cable plants and the flexibility of the building structure. Assuming none of these are of major concern, the enterprise is best served by collapsing layers and simplifying overall network design.

Benefits of a Two-Tier Approach

So far this paper has identified several key benefits of migrating to a two-tier network design. Enterprises benefit from a lower network acquisition cost by requiring fewer switches. Installation and maintenance costs are decreased due to the added simplicity of the two-tier design. A simplified network improves the IT organization’s ability to innovate at the application layer and deliver next generation IP applications such as IP Telephony with quality and consistency.

When designing a network, IT organizations should remember the four principles of quality connections, continuous uptime, maximum security and compliance and simplicity of management and operations. It is good practice to use these four criteria when evaluating competitive network designs and products.

The best way to understand the true benefits of each of these principles is to evaluate their function in a true enterprise example. Let’s focus on a large financial institution undertaking serious application and infrastructure projects. Suppose this company has evaluated an IP Telephony solution and is now ready to commence a broad roll-out of IP telephones. In addition, the IT organization, after being inundated with requests, has decided to deploy a Wi-Fi network at the headquarters location.

The benefits of the Extreme Networks architecture shine in this scenario. The concept of quality connections ensures that the network adjusts its services to meet the requirements of each application.
In the case of an IP telephone, the network will immediately recognize the device as a telephone, provide power, assign it to the appropriate VLAN and verify that the telephone has all the configuration information required to operate effectively. Once the telephone has been identified, the network can also assign policies for QoS. By delivering low latency, low jitter and predictable performance, the network is ready for converged applications. In the case of the wireless deployment, the network responds in a similar fashion. There is automatic recognition of wireless APs followed by the provisioning of power and requisite configuration and identity information. In addition, the AP is immediately brought into the established security policies of the business—helping to ensure the utmost in integrity. This ability to differentiate and tailor services based on the endpoint or application is at the heart of the quality connections concept.

Let’s continue with our financial corporation. The migration to IP Telephony and the addition of wireless means the business reliance on the network is greater than ever. The cost of downtown continues to rise with estimates at the high-end reaching $6.4 million/hour (see Figure 4). Extreme Networks considers continuous uptime to be an intrinsic network design principle. The simplification of network design via a two-tier architecture favors a more streamlined two-tier architecture. As companies are faced with the pressures of supporting emerging applications like IP Telephony and wireless networking, the network must be adequately extensible to facilitate this process. By evaluating network designs based on the four principles of quality connections, continuous uptime, security and compliance, and simplicity of management and operations, IT organizations will realize the value that a consolidation of network layers brings.

In addition to the benefits of these four pillars, the two-tier architecture decreases the total cost of network ownership—both in terms of capital and operating expenses. By collapsing network layers, the IT organization needs fewer products with which to run the network. Fewer products mean lower costs of capital, implementation and training. Additionally, fewer products also mean less management—both in terms of capital and operating expenses. By collapsing network layers, the IT organization needs fewer products with which to run the network. Fewer products mean lower costs of capital, implementation and training. Additionally, fewer products also mean less management—both in terms of capital and operating expenses.

The simplification of network design also allows network administrators to decrease the MTTR by facilitating quicker fault isolation and remedy. Additionally, EAPS provides the sub 50 millisecond failover our financial customer needs to guarantee the optimal disruption is decreased. The simplification of network design via a two-tier architecture favors a more streamlined two-tier architecture. As companies are faced with the pressures of supporting emerging applications like IP Telephony and wireless networking, the network must be adequately extensible to facilitate this process. By evaluating network designs based on the four principles of quality connections, continuous uptime, security and compliance, and simplicity of management and operations, IT organizations will realize the value that a consolidation of network layers brings.

With such complex infrastructure projects, our financial company is conscious of the human resources required to operate such a network and seeks a simple management solution. Network management has advanced substantially over the past five years. Through its EPICenter platform, Extreme Networks offers a single portal from which network administrators may control configuration, performance monitoring, policy and fault management. As previously disparate networks converge (voice, data, wired and wireless), so too has Extreme Networks view of management. EPICenter provides tight integration of IP Telephony and Extreme Networks wireless LAN product portfolios. In this way, network administrators can converge network management across wireless, wire-line, voice and data networks.

In this paper we have sought to explain the benefits of migrating from a three-tier network architecture to a more streamlined two-tier architecture. As companies are faced with the pressures of supporting emerging applications like IP Telephony and wireless networking, the network must be adequately extensible to facilitate this process. By evaluating network designs based on the four principles of quality connections, continuous uptime, security and compliance, and simplicity of management and operations, IT organizations will realize the value that a consolidation of network layers brings.

Conclusion

In this paper we have sought to explain the benefits of migrating from a three-tier network architecture to a more streamlined two-tier architecture. As companies are faced with the pressures of supporting emerging applications like IP Telephony and wireless networking, the network must be adequately extensible to facilitate this process. By evaluating network designs based on the four principles of quality connections, continuous uptime, security and compliance, and simplicity of management and operations, IT organizations will realize the value that a consolidation of network layers brings.
The timeliness of this architectural shift can be attributed to the advancement of network technology in several key areas. However, change for the sake of technology alone is not logical. Instead, the true benefits of a simplification of architecture can be seen in the numbers. Enterprises embracing such a strategy are certain to realize substantial reductions in both capital and operational costs. In today’s world of tightened purse strings, lowering network Total Cost of Ownership while maintaining levels of service is the bottom line that ultimately matters the most.

**About the Author: Chris Kozup**

Chris Kozup is a management consultant focusing on the strategic applications of information technology. Previously, Mr. Kozup was program director at the META Group where he provided strategic analysis on campus/local-area network and metropolitan-area network infrastructure and services. Specific areas of coverage included: high-speed networking, including switching and routing products, Wi-Fi, wireless security, and convergence (voice, video, data).